International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 01 – 12, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1001

A Systematic Review of Computer Science Solutions for Addressing Violence Against Women in Educational Institutions

Amina S. Omar*
School of Computing and Informatics
Technical University of Mombasa
Mombasa, Kenya

Mvurya Mgala
School of Computing and Informatics
Technical University of Mombasa
Mombasa, Kenya

Abstract: Approximately one in three women worldwide experience physical, mental, or sexual violence, making violence against women (VAW) a serious public health emergency. One of the main issues in educational institutions is violence against women. With the introduction of smart campuses and smart technologies, educational institutions are doing everything within their power to avert these kinds of incidents. Recent developments in computer science, such as artificial intelligence (AI), Internet of Things (IoT), and pattern recognition, have been essential in creating solutions meant to stop and react to VAW. This study presents a thorough systematic review from academic digital libraries from 2010-2023 of some of the initiatives that have been used to address the issue of violence against women. The state-of-the-art for these contributions is currently described in this document along with trends, architectures, technologies, and open problems. It highlights how these technological interventions are utilized for early detection, prevention, and response to incidents of VAW. The findings suggest a growing reliance on technology to create safer educational environments, but also emphasize the need for continued research, particularly in developing inclusive, ethical, and effective technological solutions. This review aims to inform stakeholders in the education and technology sectors about the current state of computer science applications in the fight against VAW, providing insights into best practices and areas for future development.

Keywords: Artificial intelligence; Machine learning; Violence against women, pattern recognition, IoT

1. INTRODUCTION

As defined by the Violence Prevention Alliance of the World Health Organization (VPA), violence is "the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either result in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation." Although anyone can become a victim of violence, some people are more susceptible than others, such as women. Globally, about 30% of women have experienced non-partner sexual assault or intimate partner violence (IPV) at some point in their life [1].

According to the United Nations [2], violence against women is a global issue that affects higher education institutions (HEIs), the public and private sectors, and both. According to the UN, this kind of violence can happen in homes, in public spaces like schools, or both [3]. In light of these concerning facts and the widespread prevalence of violence against women, it is critical to investigate and put into practice practical solutions—using technology in particular—to stop and deal with this problem in all spheres of society, including the educational sector.

Tolerating violence against women in schools is a major sort of discriminatory behavior that endangers the learning environment and the educational prospects for girls. According to [4], girls are disproportionately the targets of sexual and physical violence in schools. In addition, male peers and occasionally instructors harass, rape, and abuse girls sexually. Addressing violence against women (VAW), a significant public health concern in educational institutions requires any form of intervention.

Numerous studies indicate that violence against women in college and university settings is on the rise [5], for instance, iscovered that 32.4% of 295 female students at Ebonyi State

University in Nigeria reported having been sexually assaulted. At the University of Kano in Northern Nigeria, out of 300 female students, 22.8% said they had experienced emotional, sexual, or physical abuse [5]. In a poll conducted by the University of Port Harcourt, 46.7 percent of 400 female undergraduates said they had been victims of sexual abuse. Of those 46.7%, 33.7% said they had experienced fondling or having their privates grabbed [6].

In Goa, [7] reported that 33 percent of the students, male and female alike, had experienced sexual abuse. Other studies show that 98% of students reported having experienced physical abuse, while 67% of girls in Botswana and Uganda, respectively, reported being mocked and harassed by their instructors [8]. These figures demonstrate the extent of violence suffered and witnessed by women, which in turn affects pupils. Gender coexistence is impeded by violence from occurring respectfully and peacefully. Furthermore, VAW management is necessary for gender equality.

VAW happens in universities, even though it is rarely discussed in public. However, there are a few reported cases where students organized a peaceful protest against VAW and presented the Vice Chancellor with an 18-point petition, such as at the University of Namibia [9]. The petition included a request to action against people who misused their position of authority by trading marks for sex, as well as those who disseminated pornography of their sex experiences online, on

Facebook, or through mobile devices. According to [9] research, university students in Kenya saw that there was a definite exchange of sex for basic needs like food, transportation, hygiene supplies, and forgettable marks. These VAW difficulties have a major impact on human growth, especially in the twenty-first century when cultures and groups are actively working together to accomplish faster and more significant global advances.

Girls who experience violence in schools have a lower chance of staying in school, doing well academically, and participating in class. According to [10], this issue occurs not just in the homes where children are meant to feel protected but also in the schools where children are supervised by some of the same teachers who also physically and sexually abuse them. VAW does indeed have serious consequences. Therefore, it is imperative to educate women and the wider public that any form of violence is abhorrent. In addition, Women must also have protection and support.

The latest technological developments offer a singular chance to create creative tactics that surpass conventional methods. Artificial intelligence (AI) can be used, for example, to create predictive models that identify risk indicators and initiate early interventions. Similar to this, real-time monitoring and alert IoT-powered systems can be leveraged to improve campus security. Cloud and mobile computing can make it easier to provide easily available platforms for incident reporting and support requests, preventing victims from being alone and enabling them to get help quickly. Educational institutions can take proactive measures to avoid VAW and promote a culture of safety and respect by utilizing the power of these technologies.

By combining these cutting-edge technologies, violence against women at educational institutions is being addressed in a way that is more proactive and data-driven than traditional approaches. The goal of this study is to employ computer science solutions to not only respond to VAW situations but also to avoid them in the first place. This will make the learning environment safer and more encouraging for all students. The goal of this project is to investigate the entire range of computer science solutions, with an emphasis on their application in the real world and their potential to reduce violence against women in educational settings.

This study is crucial to addressing the rising issue of violence against women in educational settings. It investigates how computer science methods and technology could improve security and safety in these kinds of environments. Through the identification and assessment of technology-based interventions, this research provides novel approaches to address an ongoing issue. It is anticipated that the results will offer actionable advice on how to stop and deal with this kind of violence, assisting legislators, educators, and tech developers in their endeavors to make spaces safer. This study further advances the conversation around gender-based violence by offering a technological viewpoint to supplement conventional tactics. The research's significance ultimately rests in its capacity to significantly alter how women are protected from assault in educational environments.

The harm that violence against women in schools does to their physical, emotional, and intellectual well-being is still a major worldwide problem. In order to come up with creative ways to identify, stop, and deal with this kind of violence, computer science has become a crucial discipline. These solutions have a wide range of uses, including safety apps, online harassment detection algorithms, and educational initiatives meant to alter social norms and behavior. Despite these developments, there are still a lot of unanswered questions in the field, especially when it comes to the efficiency, usability, and user acceptance of these technologies.

How CS and associated technologies can potentially treat VAW have been illustrated in earlier paragraphs. This article describes contemporary efforts in many domains to prevent VAW and searches for new designs, patterns, technologies, and unsolved problems This paper aims to fill this vacuum in the literature and offer recommendations to researchers who wish to tackle VAW from an engineering and CS standpoint. This project seeks to explore and assess effective technology solutions for this important issue.

The paper is formatted as follows. Section 2 discusses the technique used for the review. In Section 3, the procedure for data extraction is explained. Section 3 offers a comprehensive review of the literature, including theoretical frameworks, empirical studies, and noteworthy findings. Section 4 summarizes the review's analysis, recommendations, and conclusions and concludes Section 5.

1.2 Research Objectives

i) To identify and analyze Information Technology solutions developed and implemented to address violence against women (VAW) in educational institutions across various Information Technology (IT) problem domains.

1.3 Research Questions

i) What Information Technology solutions have been developed and implemented to address violence against women (VAW) in educational institutions, and how are they applied across various Information Technology (IT) problem domains?

2. METHODOLOGY

This section presents the methodology used to conduct this extensive literature review. Among the phases covered are a description of the study topics, a search strategy, selection criteria, and a plan for data extraction and synthesis. The only research question that guided this investigation was:

RQ1. What Information Technology solutions have been developed and implemented to address violence against women (VAW) in educational institutions, and how are they applied across various Information Technology (IT) problem domains?

2.1 Search Strategy

To find the materials for this study, a thorough search was carried out using academic digital libraries and search engines for the years 2010–2023. A wide range of scientific and technological topics are covered by the digital libraries and search engines indicated in Table 1, some of which are specifically relevant to the goal of this paper and were chosen for study extraction.

Table 1: Information sources for studies

Source	URL
IEEE Digital Library	https://ieeexplore.ieee.org
The ACM Digital Library	https://dl.acm.org
PubMed Digital Library	https://pubmed.gov
Springer Digital Library	https://link.springer.com
Science Direct Digital Library	https://www.sciencedirect.com

Next, the search method sought possibly relevant primary research from each of Table 1's information sources. The two keyword sets in Table 2 were based on the study questions. Computer science and related technologies are in Group 1, whereas virtual and analog worlds are in Group 2. Boolean ANDs and ORs were used to combine Group 1 and Group 2 terms into search strings.

Table 2: Search Items

Group 1	**Group 2**
Computer science, the Internet of Things, IoT, Artificial Intelligence, AI, Machine Learning, Deep Learning, DL, ubiquitous computing,	**Women's abuse, gender-based violence against women, violence against women, violence against women, verbal abuse directed against women, intimate partner violence, adolescent violence, peer violence, abuse of women, and domestic violence. Schools, universities, tertiary institutions, colleges.**

Following a comprehensive examination, it was determined to include the paper if it met the subsequent quality standards:

- The article's title and abstract were perused. The abstract was disregarded if it did not refer to VAW-like concepts or the application of CS or related technologies.
- The paper takes a computer science approach to the VAW problems.
- The architecture or design used to implement the proposed paradigm is described in depth in the article;
- The suggested model was inspired by similar projects, which are explained in the paper.

After that, we went through the articles we had gathered, examining the manuscripts to make sure they met the inclusion criteria that had been previously set as well as for exclusion.

- Research that doesn't particularly discuss how to use technology to stop violence against women.
- Research examining violence against women outside of academic institutions.
- Unrelated to study aims;
- Grey literature, opinion pieces, and non-peer-reviewed publications, as they might not have a rigorous research technique and peer validation.

2.2 Selection Criteria

Only research meeting the following requirements was considered possibly relevant:

1. Articles published in proceedings from conferences or workshops, publications, or peer-reviewed journals.
2. English-language written works.
3. Works released, all-inclusive, between 2010 and 2023. The potential relevance of the research was assessed using the following inclusion criteria to ascertain their true relevance:
4. The paper's title and abstract were read. The abstract was disregarded if it included no reference to VAW, ideas that are similar to it, or the use of CS or related technologies.
5. Study Design: Empirical research that demonstrates the efficacy of technological interventions will be prioritized. This covers study designs that are both quantitative and qualitative, such as experimental.
6. Research Question Relevance: Studies must particularly discuss how computer science tools and technology are used to stop violence against women in educational settings. Research on the creation, application, and assessment of technology solutions falls under this category.
7. Context: The research needs to be carried out in educational settings, including colleges, universities, or schools, where the goal is to stop or address violence against women.

2.3 Data Extraction and Synthesis

The previous section's methods are used to collect study data in this phase. Information sources in Table 1 received queries using terms or phrases from Table 2 using the previously specified search strategy. The initial search focused on study titles and abstracts.

Table 3: Data extraction form for every study

Retrieved from	Data Description
Study title	Title of the study
Year	Publication year
Authors of the study	Names of people who contributed to writing the study
Authors' Countries	Countries authors came from
Origin	The digital library or search engine where the study was found
Contribution of the study's problem	The solution to the problem the authors are addressing in their study
Approach	Specific technologies used to address the problem
Category	Online / offline detection etc.
Type	journal, Conference, book chapter.

When duplicates were found on several platforms, one publication was selected. The quality assessment mentioned in the section above was then applied to the studies. Should there be any improbable disagreements about eligibility at this juncture, the writer participated in conversations to resolve the issue. In the end, 62 studies were chosen to be examined further.

2.3.1 Data synthesis

The findings will be grouped into four primary areas depending on their relevance to the research objectives during data synthesis. Each category—online detection (I), offline detection (II), safety devices (III), and education (IV)—will be analyzed separately to identify trends, commonalities, and differences in computer science solutions to address violence against women (VAW) in educational institutions.

For each category, the key research findings will be summarized, highlighting the specific computer science tools and technologies used, such as artificial intelligence (AI), the Internet of Things (IoT), mobile computing, and pattern recognition. The advantages, disadvantages, and limitations of each approach will be discussed to provide a comprehensive understanding of their effectiveness in addressing VAW.

Furthermore, the synthesis will focus on addressing the research questions by identifying how Information Technology solutions have been developed and implemented to address VAW in educational institutions across various IT problem domains. By analyzing the findings in this manner, the study aims to provide actionable insights and recommendations for policymakers, educators, and technologists to improve safety and security in educational settings.

Overall, the data synthesis will provide a detailed analysis of the current state of research on computer science solutions for addressing VAW in educational institutions, highlighting gaps and challenges in the existing literature and suggesting best practices for future research and implementation.

3.0 LITERATURE REVIEW

Based on the goal of their solution to determine the primary VAW application domains that are covered by CS technologies, the primary research was split into four groups. Not the quantity of linked concepts, but the application domain's importance today and in the future, determines this classification. Among the categories are education (IV), offline detection (II), online detection (I), and safety (III).

3.1 Online Detection

Several researchers have used machine learning (ML) and artificial intelligence (AI) approaches to identify potentially harmful or disparaging online material regarding women. These researchers employed machine learning (ML) algorithms to automatically label them as violent or non-abusive toward women based on photos, videos, text, or a mix. This type of ML use could quickly differentiate a sizable fraction of abusive and non-abusive content on the Internet. If carried out by hand, this procedure could be emotionally or physically exhausting. A selection of noteworthy examples from the internet detection category are listed below.

VAW must be recognized and eliminated by addressing explicit violence and its risk factors. Sexual and physical abuse, domestic violence (DV), and other types of violence against women and girls must be addressed [11]. Studies that fall under this category pertain to explicit online forms of VAW and the associated risk factors. According to [11]. these risk factors can manifest in a variety of ways in the online setting, such as exposure to harmful content, cyberbullying, online harassment, and the perpetuation of negative stereotypes or attitudes about women and girls.

[12] looked into the potential applications of AI technology to address various social issues, with a focus on cyber violence. The application of AI to detect and put an end to online harassment, cyberbullying, and other forms of online violence is discussed in the article. The authors describe several artificial intelligence (AI) techniques, such as computer vision, natural language processing, and machine learning algorithms, that can be used to assess online interactions and data to identify abusive behavior patterns. This report also

discusses the challenges of implementing AI technologies to address online violence. These challenges include the need for precise and context-aware algorithms, ethical concerns surrounding privacy and data protection, and the importance of interdisciplinary collaboration in the creation of successful and responsible AI systems. While the paper discusses the challenges of implementing AI systems, it does not offer detailed guidance on how to overcome these challenges or successfully integrate AI solutions into existing efforts to address online violence. The paper primarily focuses on theoretical aspects and does not provide empirical evidence or case studies to demonstrate the real-world effectiveness of AI solutions in combating online violence.

[13] used using neural networks to identify instances of cyberbullying and bullying in messages shared on social media. The study focuses on analyzing textual data from social media sites using neural network designs and other deep learning approaches to look for patterns that may indicate bullying behavior. By training the neural networks on labeled datasets that comprise samples of both bullying and non-bullying content, the models can distinguish between abusive and non-abusive language. The study shows that neural networks are capable of accurately detecting instances of bullying and cyberbullying, which might make them a valuable tool for keeping an eye on online interactions and shielding users from objectionable content. The study also touches on the significance of creating strong and trustworthy models that can change to reflect the way that online communication is evolving as well as the different ways that bullying takes place on social media. While their findings demonstrate the potential of these models to enhance online safety, addressing the challenges of data dependency, interpretability, and adaptability is essential for the successful implementation of neural network-based detection systems. Future research should focus on improving the robustness and transparency of these models, as well as exploring strategies for keeping them up-to-date with changing online behaviors.

Machine learning models have been taught with textual patterns and emotions that might point to online harassment, cyberbullying, or grooming behaviors. Machine learning algorithms have shown promise for automated cyberbullying identification in recognizing harmful online interactions, according to [14] . This study demonstrates how machine learning techniques can be used to detect language patterns linked to cyberbullying. This approach's primary drawback is its inability to reliably interpret the context in which specific words or phrases are employed. Jokes, sarcasm, and cultural differences can cause false positives, which happen when harmless conversations are wrongly reported as cyberbullying.

Natural language processing (NLP) techniques are applied to social media postings, comments, and messages to search for signs of misogyny, sexism, or threats against women. Similarly, computer vision algorithms are used to identify explicit or violent images and videos that depict violence against women or meet the criteria for being classified as sexual abuse material (SAM). [15] employed natural language processing (NLP) to examine social media content and detect hostility and bullying. The study shows how well natural language processing (NLP) manages massive amounts of textual data, but it also draws attention to the challenges associated with accurately identifying cultural allusions, irony, and sarcasm. False positives or negatives in detection could be the outcome of these issues.

To counter misogyny hate speech directed at women on social media, [16] , developed machine learning models that can recognize and categorize sexist tweets in Italian, Spanish, and English. The scientists used several datasets, features, and classifiers to determine tweet goals, divide misogynistic content into five behaviors, and distinguish between misogynistic and non-misogynistic tweets. They also looked at how misogyny is identified across languages and how it relates to other types of abuse. With an accuracy of 91.32%, the top-performing English model employed a support vector machine (SVM) classifier with a radial basis function (RBF) kernel. An SVM classifier with a linear kernel performed best for Spanish, with an accuracy of 81.47%. The Italian design made use of a BERT-based. The study by [17], showcases the application of machine learning models, such as SVM and BERT, in effectively identifying and categorizing misogynistic tweets in multiple languages. The high accuracy rates achieved indicate the models' potential in addressing misogyny on social media. However, the models' performance may be influenced by linguistic diversity and the dynamic nature of online discourse. Continuous refinement and broader contextual analysis are essential for maintaining the models' relevance and effectiveness in combating online misogyny.

[18] created machine learning techniques to help with the larger objective of identifying sexist content by automatically identifying sexist humor on the internet. Jokes with both text and visuals that were uploaded online were gathered by the scientists from social media. Subsequently, they created algorithms to determine whether or not the jokes were sexist. SVM classifiers achieved a maximum precision of 76.2% for image-based identification; for text-based detection, a precision of 75.2% was achieved by combining k-nearest neighbors (K-NN) with a bag of words (BoW). SVM was used in a bimodal technique that used text and picture features to achieve a precision of 75.9% [19]. Although these findings show that ML may be used to detect sexist content, there is still an opportunity for improvement based on the precision rates. Additional investigation.

To help teachers, address online peer hostility, [20] looked into the usage of machine learning algorithms to identify bullying in Greek virtual learning communities of K–12 pupils. The authors employed a range of text pre-processing techniques, n-grams as features, and multiple classifiers. At 95.4%, the deep learning classifier had a remarkable recall rate. Although the study tackles the important problem of cyberbullying and yields encouraging results, it may not be as generalizable as it may be due to its reliance on n-grams as characteristics and focus on a particular cultural context, which can obscure intricate linguistic patterns. More investigation is required to evaluate the model's effectiveness in various metrics and scenarios as well as to investigate more sophisticated features and methods.

These AI-powered online detection systems offer several advantages, including the ability to process and assess vast volumes of data, provide real-time monitoring, and reduce reliance on emotionally unstable or biased human moderators. By automatically identifying harmful information and behavior, these tools can support victims, enable rapid responses, and contribute to the creation of safer online environments for women and children.

Nevertheless, the application of AI to internet detection also raises concerns about accuracy, privacy, and ethics. The development and application of these technologies will make it increasingly challenging to reconcile proactive detection with the defense of individual rights.

3.2 Offline Detection

Computer science developments recently provided interesting approaches to offline VAW identification. To find patterns of violence or risk factors linked to violence against women (VAW), techniques like data mining, machine learning, and pattern recognition are being applied to historical data sets more and more.

Machine learning (ML) is used in offline detection research to identify non-online data to identify potential abuse or violence victims. Self-figure drawings that patients gave to their therapists [21] and health statistics from public health institutions [22] are two examples of this data. The creation of resources that will help educators, social workers, nurses, and other professionals who deal directly with individuals who may be abused is the aim of these studies. Practitioners may find it useful to adopt techniques that assist them in identifying abuse situations that would not otherwise be reported, given the low rate of victim reporting [23] Healthcare staff are not trained to identify and address reported abuse incidents [24]. These tools may encourage professionals to assist more women get the support and services they need to prevent assault.

[25] examined strategies for the offline identification of P3 waves in EEG recordings, showing how signal-processing methods might be modified to identify physiological reactions linked to stress or anxiety in individuals who had experienced violence. Similarly, [26], demonstrated the possible use of such frameworks for the detection of covert patterns of violence against women in gathered data sets by introducing a deep offline-to-online transfer learning paradigm for pipeline leakage detection.

To find violence in schools, some studies employ machine learning. These studies represent the early phases of Internet of Things (IoT) reaction systems to school violence. These technologies are designed to automatically notify school officials for intervention when they identify violence using machine learning techniques. This research only addressed the aspect of using ML to identify violence.

Two methods are presented in the study by [27] to distinguish between verbal and physical bullying in schools. Students' emotional expressions could be captured on record by writers. Studies on offline detection are divided into smaller sections. indication of maltreatment. They involved shouting and sobbing. Using Mel Frequency Cepstral Coefficients (MFCC) to extract sound features, the authors then applied a k-NN algorithm to determine whether or not these recordings involved verbal bullying. The model that identified verbal aggression with the highest accuracy rate, at 70.4%, was found. Moreover, k-NN was the most effective classifier for recognizing physical bullying. The authors used the movement sensors of the students to collect acceleration and three-dimensional gyros data during simulations of violent and peaceful activities. The most dependable model was able to recognize instances of physical bullying with an accuracy rate of 52.8%.

The authors developed WiVi to identify school violence using commercial Wi-Fi infrastructure[28] . Based on their research of how human conduct affects Channel State Information streams from Wi-Fi devices, the scientists constructed an ML model that can detect bullying signal changes. The model's classifier, least square SVM (LSSVM), was tested in offices, dorm rooms, and labs. The average recall was 93.4%.

Several studies have attempted to automatically identify women who may be victims of intimate relationship violence (IPV), which affects 35% of women [29]. [30] automatically identify face injuries from physical IPV using DL architecture and class activation maps. Better than others, the proposed model was 80% correct.

3.3 Safety Devices

The research in the safety category concentrated on leveraging IoT technology to develop products that will give women security in circumstances where they might be alone or in danger. Solutions in this area enable girls and women to be watched over and to receive assistance if they find themselves in a violent situation through the use of the Internet and other communication technologies [31]. Every day, 137 women are killed by family members [33]. According to [32], about 120 million women and girls under the age of twenty have experienced non-consensual sexual assault. These studies thus emphasize the significance of responding promptly to prevent violent incidents and offer aid. These studies aim to expedite victims' timely access to care. [34] provides an example of a safety system that includes a smart band and a mobile application. Below is a summary of the representative samples for each subcategory.

A few studies support the development of smartphone apps that provide women with security. The study mentioned [35] suggests a smartphone app with a safety focus. The smartphone software tracks the wearer's whereabouts via GPS, a gravity sensor, and geofencing. If the wearer leaves their parents' geofence, the device sends an SMS or Wi-Fi signal to authorized contacts with their whereabouts. To look for any signs of abuse or mistreatment, the smartphone will also begin recording voice conversations, which it will subsequently send as an SMS. Additionally, the wearer can shake their smartphone to activate the previously mentioned alarm in an emergency.

The creators of the smartphone app WeDoCare prioritized the safety of women [36]. To assess if the user is in danger, WeDoCare uses GPS position monitoring, gesture detection, and speech recognition. With this program, the user can activate the alarm in three different ways: by pressing a button on the home screen, by chopping something with the phone, or by yelling "Help." If this option is chosen, the application will notify the authorities by SMS of the user's whereabouts.

Research in this area has suggested wearable or portable gadgets that protect moms and kids. According to a study [37], it may be simpler for a woman to ask for help in an emergency if she is wearing an Internet of Things smart bracelet that is Bluetooth-connected to a smartphone app. The website features an emergency button, a map showing safe havens users can use in an emergency, details on laws specific to women, and self-defense tutorials. Volunteers can protect at-risk women or help those who have used the emergency feature of the app. Pressing an app button or smart band emergency switch activates the system's emergency mechanism. The smartphone will send an emergency SMS with the user's GPS location to her pre-programmed contacts, volunteers, and the nearby police station when activated.

.

The authors of [38] examined circumstances in which a woman is in danger but is unable to yell emergency phrases or press a help button using a different methodology. The authors suggest an Internet of Things wearable that uses variations in a woman's body temperature and pulse rate to determine how dangerous she is. The gadget features sensors that measure pulse and body temperature. In the event of an Internet outage, the sensors can transfer data ZigBee mesh networks connect to the cloud over the Internet. If the user is in risk, data is assessed by a cloud-based LR model. The technology will instantly contact emergency contacts in a situation like this.

A gadget for women's security who reside in rural areas or places with erratic Internet and cell connectivity was proposed by [39]. The safety solution makes use of the Internet of Things concept. If in trouble, she can press it like a beacon to call for aid. Each beacon has a unique code for identification. Bluetooth links beacons to specially erected street poles and solar-powered central stations. When pressed, the help button causes a distress signal to be sent, traveling via the street pole network and ending up at a central station. A server there handles the assistance request, enabling the user to get assistance.

Among the wearable safety solutions designed exclusively for women are self-defense functions. A wearable device and a mobile app were integrated into a proposed Internet of Things system [40] that uses fingerprint scanning to activate. The device may send brief messages to emergency contacts and police stations when on. The device contains a self-defense alert and shock generator. Alerts raise attention and scare off perpetrators. The victim can defend herself by using the shock wave generator if the offender approaches too closely. Additional wearable alternatives comprise self-defense functionalities [31].

A state-of-the-art smartphone application for bystander intervention was developed by [41] to put an end to gender-based violence against college students. The Circle of 6 smartphone apps, designed to protect college students against gender-based harassment, are evaluated in this study. The program lets users transmit preformatted messages or location data to six trustworthy contacts instantaneously in an emergency.

The Safecity app, which gathers user-submitted reports of sexual abuse and harassment in public spaces, was the subject of an investigation by [42]. To encourage awareness and community action, the app maps out sites that are both safe and risky. [31] reviewed the bSafe smartphone app, which provides safety features including GPS tracking, SOS texting, and audio recording. The app's goal is to make women feel more secure by enabling quick communication between emergency contacts and law enforcement. Since its 2012 start, Safecity has reached over 1 million people directly and has gathered over 40,000 stories from both India and elsewhere.

A state-of-the-art smartphone app was developed by [43] to collect data on women's safety in Indian cities. This study covers the development and deployment of the My Safetipin app, which collects data on women's safety in Indian cities. Users of the app can rate the safety of other websites according to a range of criteria and share their own experiences with it. These apps can also be used in educational institutions to protect women.

.

The creation of [44] A mobile application to boost the perception of safety. The Watch Over Me app, which helps users feel safer by providing real-time location tracking, emergency contact options, and safety tips, is evaluated in this study. The program is meant to increase users' confidence when they are exploring new cities.

[45] looked into ways to use the React Mobile app to integrate social media and increase women's safety. Users can use the app to share their location and alert particular friends and social media networks about emergencies. To increase campus safety, [46] developed and implemented a mobile application. This essay discusses the development of a smartphone app designed to increase campus safety. Features of the app include emergency contact details, campus maps with safety locations, and real-time warnings.

[41] looked at the React Mobile app, which uses social media to increase women's safety. With the app, users may notify certain friends and social media networks about emergencies based on their location. The development and release of a mobile app to increase school security. This essay discusses the development of a smartphone app to increase safety on college campuses. The app has features like emergency contact details, school maps with safety zones, and real-time notifications.

3.4 Education

Research in the education area aims to teach medical professionals and educate children about VAW. The suggestions are predicated on digital serious games (SG) that impart VAW knowledge. As was previously reported, nearly 33% of intentional deaths of women in 2017 were related to IPV [47]. In the year before they passed away at the hands of an intimate spouse, many American women sought medical attention [48]. Concerns regarding medical students' inexperience in identifying child abuse victims and their lack of knowledge on what to do in such cases have also been raised [49].

As a result, medical personnel need to be properly trained to recognize abuse and know how to support women and children who are its victims. Digital serious games (SG) have demonstrated potential in STEM education, particularly in the area of arithmetic [50]. It has also been effectively used in the medical industry. If they played SG and learned about chemotherapy side effects, cancer patients were more inclined to follow their treatment plan [51].

These results suggest that SG could help provide medical staff with the training and information they need. Furthermore, SG can assist in reducing the price of conventional training [52]. The use of SG in educational settings may have benefits. To stop violence against women and girls, the entertainment industry in Singapore must teach youth about the attitudes and societal conventions that encourage them to act violently toward their peers [53]. notably because it investigates the connection between IPV and abuse of children
.
The school bullying subtype of peer violence was studied by SG. Designers assessed the point-and-click game. SG Stop the Mob! for tablets and PCs combats lower secondary school bullying. Students witnessed their friend Bob get tortured as onlookers. Students might choose whether to support Bob or bully him. Through the SG, students may observe how their bullying reactions affect Bob both positively and negatively. Stop the Mob! teaches youngsters that bullying decisions have consequences by playing the game in a classroom with a teacher to help them reflect.

The authors examine and contrast two SG for PC prototypes to improve high school pupils' comprehension of bullying. Prototypes of simulation games, such as Stop the Mob! are meant to educate players about bullying's harms. One prototype is a fantasy game where participants can walk freely in a virtual world, and the other is a cartoon-style game that follows pupils through scenarios. The prototypes were evaluated by the authors in a classroom full of children, ages twelve to fifteen [54]. The goal of the writers' comparison and contrast of the two SG for PC versions is to increase high school students' awareness of bullying. As prototypes, Stop the Mob! created simulation games to teach about bullying's impacts. Using a cartoon-style game, one of the prototypes walks pupils through many scenarios, setting it apart from the other. However, the other fantasy game lets players freely explore the online realm. The writers examined the prototypes in a classroom full of 12–15-year-olds. After completing the post-game surveys, 23 of 26 students preferred the fantasy game over the one with instructions because it gave the characters more flexibility to move.

The purpose of the PC game Green Acres High, created [55], is to educate kids about interpersonal violence. Through a series of lectures structured after simulations and presented in a classroom setting, the SG is to enhance the education of high school students on good and unhealthy relationships. Real students reviewed the game and gave the developers constructive and critical feedback. Students stated that they learned the content directly from the source thanks to the simulation-style SG. It was quite tempting to think that learning might be done through an online game. Technical problems, such the game not loading and unclear instructions, were the main concerns.

[56] addressed the demands of medical professionals in their work. The authors advise medical practitioners to sign up for a free online course that teaches them how to recognize and treat patients with domestic abuse allegations. Response to DV in Clinical Settings has 17 modules that are broken down into three sections: an assessment, a simulation where participants apply the skills and knowledge they acquired in the previous section, and instructions on how to recognize and manage IPV cases while being supervised by a trained professional. The purpose of the study was to get insights from medical professionals who played the game. Players commended the game for being entertaining, realistic, fascinating, and simple to learn.

[57] evaluated the impact of an online course at a UK business school on gender sensitization. The results show that gender-based violence can be prevented and students'

awareness of gender issues can be effectively raised by using online teaching modules.

Examining the many application domains where computer science and engineering (CS) may be applied to lessen violence against women (VAW) is the aim of the research subjects in this literature review. In light of the conclusions from the literature study, the discussion that follows makes an effort to answer these questions.

4.0 DISCUSSION

The systematic examination identifies safety, education, offline detection, and online detection as the four main domains of computer science solutions. It demonstrates how artificial intelligence (AI) is used to identify potentially hostile situations or content and how machine learning systems often detect online and offline violence. Safety solutions generally use wearable devices and other Internet of Things (IoT) technology to offer potential victims real-time assistance. In educational interventions, victims and the general public are educated about violence prevention through the use of digital serious games.

The study shows that machine learning techniques are used to identify offensive content offline and online. highlighting the critical function of artificial intelligence in spotting and averting potentially hostile circumstances. But the focus on sites like Twitter highlights a significant lack of investigation into other, equally popular teenager’s social media venues like YouTube and Instagram. This restriction points to the urgent need to broaden the platforms being examined to cover a wider range of digital interactions.

The review reveals a significant lack of linguistic diversity in the datasets used, with an emphasis mostly on English-language material. This restriction raises doubts about the replies given by CS, given the prevalence of violence against women and children worldwide. To ensure that these technologies function effectively across a range of linguistic and cultural contexts, more inclusive language approaches must be used in future studies.

The emergency feature on the majority of safety gadgets needs to be manually activated by the user. This may be impossible in an emergency. if they are too afraid, pressed for time, or experiencing an attack. Therefore, there should be a greater focus on automating the safety device's emergency mechanism activation. Some wearable safety gadgets were hefty or required constant holding. This is neither practical for daily use, nor is it discreet. Therefore, to reduce disturbance to consumers, wearable technology needs to be both ubiquitous and non-intrusive.

The conversation also highlights how some wearable safety devices are unworkable because of their ostentatious looks, arguing in favor of more understated and approachable alternatives. Moreover, there are serious privacy problems raised by the widespread usage of location and visual surveillance technologies, which may allow for abuse by criminals. This conundrum highlights the need for designers to carefully weigh privacy safeguards against safety features to make sure these technologies don't unintentionally encourage abuse.

Some anti-abuse interventions promote abuse. Every safety device uses technology for either location or vision monitoring. Thanks to gadgets made to shield kids from harm, anyone with access to the system can keep an eye on kids at all times. With this kind of system, abusers can always keep an eye on their victims, which is one way that technology can facilitate abuse. Individuals who develop technology aimed at safeguarding women and children must ensure that their creations are truly safe and cannot be abused. Moreover, all safety devices' visual and location tracking capabilities could suggest that users' right to privacy must be given up to be safe.

Safety devices warn authorities or pre-arranged contacts when a user is in danger. The user can vocally signal for help with some devices. Thus, if someone answers the victim's plea for aid will determine these gadgets' effectiveness. . Effectiveness is also impacted by their arrival time at the crime scene. Safety device makers may find it useful to perform simulations that illustrate the length of time victims must wait for assistance to account for these factors. Researchers examining safety devices need to consider this information to minimize any false sense of security from using these devices and to create reasonable expectations for how much these devices can help victims.

Males commit acts of sexual violence and IPV more frequently than females. Few SG related to education specifically addressed VAW issues directed at men or boys. Conventions and ideas that sustain VAW must be challenged to end it. A social group that teaches males about the attitudes and ideas that lead them to commit violent crimes against women could be helpful. Some social organizations focus on educating about peer aggression.

To support players' development of critical thinking abilities regarding the game's material, an educator or medical practitioner was required to be present at any SG that covered VAW. Concurrently, the main purpose of offline detection research is to build instruments that will allow experts to identify VAW. They are not interested in taking on the role of the experts who handle these duties. Technology can lessen aggression, but it should be used as a tool, not a cure for violent adulthood.

VAW are sensitive topics. Sadly, biases in AI systems exist and may jeopardize their efficacy. Bias may cause someone to disregard violent acts or treat someone unfairly as a criminal.

Consideration should be given to the emerging topic of AI fairness research in AI concepts that tackle VAW.

5.0 CONCLUSION

This systematic literature review examines how computer science (CS) and related technologies decrease violence against women (VAW) and children. In recognizing and responding to VAW in both online and offline situations, the paper emphasizes the substantial potential of machine learning (ML), artificial intelligence (AI), the Internet of Things (IoT), and serious gaming (SG). These technologies provide creative ways to improve safety, increase consciousness, and inform people about VAW.

To fully exploit the potential of CS technologies in preventing VAW, several important research gaps and hurdles are also identified in the review. These include the necessity of thorough assessments in a range of settings, the incorporation of computer-supported collaborative interventions with conventional interventions, ethical issues in data gathering, and the significance of digital literacy and accessibility. Furthermore, the review proposes that to improve the efficacy of detection systems in various cultural and social contexts, future research should investigate a more comprehensive incorporation of social media platforms and language diversity.

To bridge these gaps, future research should focus on developing more automated, inclusive, and ethically acceptable computer science solutions. Encouraging multidisciplinary collaboration and ensuring that technological solutions are accessible, easy to use, and mindful of privacy and ethical concerns are essential. Computer science may be used to create innovative, durable, and effective solutions that assist global efforts to eradicate violence against women and girls, eventually resulting in a more safe and equitable society for women and children.

ACKNOWLEDGMENTS

The authors would like to express their gratitude to the Institute of Computing and Informatics at the Technical University of Mombasa for providing the necessary resources and support throughout this research. We extend our sincere thanks to our colleagues and faculty members for their valuable insights and feedback, which significantly contributed to the refinement of our work.

3. REFERENCES

[1] World Health Organization. Violence against women. Available online: https://www.who.int/news-room/fact-sheets/detail/violence-against-women (accessed on 28 May 2021).

[2] United Nations. Ending violence against women. Available online: https://www.un.org/en/coronavirus/ending-violence-against-women-during-covid-19-pandemic (accessed on 28 May 2021).

[3] United Nations Educational, Scientific and Cultural Organization (UNESCO). School violence and bullying: Global status report. Available online: https://unesdoc.unesco.org/ark:/48223/pf0000246970 (accessed on 28 May 2021).

[4] UNESCO. Behind the numbers: Ending school violence and bullying. Available online: https://unesdoc.unesco.org/ark:/48223/pf0000366483 (accessed on 28 May 2021).

[5] Chukwuemeka, E.E.; Ajaero, C.K.; Onyishi, C.J.; Okeke, C.C.; Ibeagha, P.N.; Eze, V.C. Prevalence and predictors of sexual harassment among female students of tertiary education institutions in Enugu State, Nigeria. J. Educ. Soc. Res. 2015, 5, 239–246.

[6] Owoaje, E.T.; OlaOlorun, F.M.; Bello, I.S. Experiences of sexual coercion among adolescent girls in Ibadan, Nigeria. Afr. J. Reprod. Health 2006, 10, 76–84.

[7] Mathur, K.; Rathore, P.; Mathur, R. Incidence, type and intensity of abuse in street children in India. Child Abuse Negl. 2009, 33, 907–913.

[8] De Wet, N. The reasons for and the impact of principal-on-teacher bullying on the victims' private and professional lives. Teach. Teach. Educ. 2010, 26, 1450–1459.

[9] Mwangi, W.M. Trading on patriarchal dividends: Sexual harassment and the commodification of sex in Kenyan private universities. Soc. Sci. 2017, 6, 148.

[10] World Health Organization. World report on violence and health. Available online: https://www.who.int/violence_injury_prevention/violence/world_report/en/ (accessed on 28 May 2021).

[11] Jewkes, R.; Fulu, E.; Roselli, T.; Garcia-Moreno, C. Prevalence of and factors associated with non-partner rape perpetration: Findings from the UN Multi-country Cross-sectional Study on Men and Violence in Asia and the Pacific. Lancet Glob. Health 2013, 1, e208–e218.

[12] Latif, S.; Qadir, J.; Farooq, S.; Imran, M.A. How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare? Future Internet 2017, 9, 93.

[13] Reyes-Menendez, A.; Saura, J.R.; Alvarez-Alonso, C. Understanding #WorldEnvironmentDay User Opinions in Twitter: A Topic-Based Sentiment Analysis Approach. Int. J. Environ. Res. Public Health 2018, 15, 2537.

[14] Salawu, S.; He, Y.; Lumsden, J. Approaches to automated detection of cyberbullying: A survey. IEEE Trans. Affect. Comput. 2020, 11, 3–24.

[15] Chatzakou, D.; Kourtellis, N.; Blackburn, J.; De Cristofaro, E.; Stringhini, G.; Vakali, A. Mean Birds: Detecting Aggression and Bullying on Twitter. In Proceedings of the ACM Web Science Conference, Troy, NY, USA, 25–28 June 2017; pp. 13–22.

[16] Fersini, E.; Rosso, P.; Anzovino, M. Overview of the Task on Automatic Misogyny Identification at IberEval 2018. In Proceedings of the 3rd Workshop on Evaluation of Human Language Technologies for Iberian Languages

(IberEval 2018), Sevilla, Spain, 18 September 2018; pp. 214–228.

[17] Fersini, E.; Nozza, D.; Rosso, P. Overview of the Evalita 2018 Task on Automatic Misogyny Identification (AMI). In Proceedings of the Sixth Evaluation Campaign of Natural Language Processing and Speech Tools for Italian (EVALITA 2018), Turin, Italy, 12–13 December

[18] Waseem, Z.; Hovy, D. Hateful Symbols or Hateful People? Predictive Features for Hate Speech Detection on Twitter. In Proceedings of the NAACL Student Research Workshop, San Diego, CA, USA, 12–17 June 2016; pp. 88–93.

[19] Papadopoulos, G.; Zigkolis, C.; Kompatsiaris, Y.; Vakali, A. Detecting cyberbullying in online communities: A text mining approach. In Proceedings of the 24th ACM Conference on Hypertext and Social Media, Paris, France, 1–3 May 2013; pp. 290–292.

[20] Majumder, A.; Poria, S.; Gelbukh, A.; Cambria, E. Deep Learning-Based Document Modeling for Personality Detection from Text. IEEE Intell. Syst. 2017, 32, 74–79.

[21] Smith, J.D.; Berkel, C.; Jordan, N.; Atkins, D.C.; Narayanan, S.S. An Artificial Intelligence Framework for Online Sexual Health Education. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; pp. 1–6.

[22] Zhang, L.; Wang, H.; Li, Q. Detecting Domestic Violence: A Framework for Identifying Intimate Partner Violence From Emergency Department Narratives. J. Am. Med. Inform. Assoc. 2020, 27, 53–60.

[23] Day, T.; Ricketts, M.; Woolhouse, M.; Doolan, M. Professional learning in the business of busy-ness: Digital badging. J. Further High. Educ. 2020, 44, 41–52.

[24] Ancău, M. Offline detection of P3 waves in EEG signals: A comparison of different methods. In Proceedings of the 2019 International Conference on e-Health and Bioengineering (EHB), Iasi, Romania, 21–23 November 2019; pp. 1–4.

[25] Wang, L.; Zhou, Y.; Wang, X.; Yuan, H. Deep offline-to-online transfer learning for pipeline leakage detection. IEEE Trans. Ind. Inform. 2023, 19, 1612–1621.

[26] Saha, H.N.; Auddy, S.; Pal, A.; De, D. Wearable IoT-Enabled Real-Time Health Monitoring System. Electron. 2018, 7, 405.

[27] Gupta, P.; Agrawal, S.; Chhabra, J.; Dhir, S. Smart Safety Device for Women Security using IoT. In Proceedings of the 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018; pp. 1–4.

[28] Chatterjee, S.; Dutta, H.; Pramanik, I.; Mukherjee, A. IoT Based Smart Security for Women Using Machine Learning Algorithms. In Proceedings of the 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 12–14 June 2019; pp. 639–644.

[29] Rathore, P.; Sharma, P.K.; Park, J.H. AWISH: IoT Based Wearable Smart Band for Women Safety Using Machine Learning. IEEE Access 2019, 7, 104290–104301.

[30] Chaudhry, S.; Siyal, M.Y.; Bhatti, Z.; Memon, S.; Ahmed, J. Development of Wearable IoT Device for Safety of Women with Machine Learning. In Proceedings of the 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 29–30 January 2020; pp. 1–6

[31] Sharma, V., Tomar, Y., & Vydeki, D. (2019). Smart shoe for women safety. In Proc. IEEE 10th Int. Conf. Awareness Sci. Technol. (iCAST) (pp. 1–4). doi:10.1109/icawst.2019.8923204.

[32] World Health Organization. (2020). Global status report on preventing violence against children. Geneva, Switzerland: Author. Retrieved from https://www.who.int/teams/social-determinants-of-health/violence-prevention/global-status-report-on-violence-against-children-2020

[33] UN Women. (2021). Focusing on Prevention: Ending Violence Against Women. Retrieved from https://www.unwomen.org/en/what-we-do/ending-violenceagainst-women/prevention.

[34] Harikiran, G. C., Menasinkai, K., & Shirol, S. (2016). Smart security solution for women based on Internet of Things (IOT). In Proceedings of the International Conference on Electronics, Electronics, Optimization Techniques (ICEEOT) (pp. 3551–3554). Chennai, India. doi: 10.1109/ICEEOT.2016.7755365

[35] Raflesia, S. P., Firdaus, & Lestarini, D. (2018). An integrated child safety using geo-fencing information on mobile devices. In Proceedings of the International Conference on Electrical Engineering and Computer Science (ICECOS) (pp. 379–384). Pangkal Pinang. doi: 10.1109/icecos.2018.8605200

[36] Silva, J. S., Saldanha, R., Pereira, V., Raposo, D., Boavida, F., Rodrigues, A., & Abreu, M. (2019). WeDoCare: A system for vulnerable social groups. In Proceedings of the International Conference on Computer Science and Computational Intelligence (CSCI) (pp. 5332–5336). Las Vegas, Nevada. doi: 10.1109/csci49370.2019.00201

[37] Kabir, A. Z. M. T., Mizan, A. M., & Tasneem, T. (2020). Safety solution for women using the smart band and CWS app. In Proceedings of the 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 566–569). Phuket, Thailand. doi: 10.1109/ecticon49241.2020.9158134

[38] Khandelwal, T., Khandelwal, M., & Pandey, P. S. (2018). Women safety device designed using IoT and machine learning. In Proceedings of the IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/ CBDCom/IOP/SCI) (pp. 1204–1210). Guangzhou, China. doi: 10.1109/smartworld.2018.00210.

[39] Paknikar, R., Shah, S., & Gharpure, P. (2019). Wireless IoT based solution for women safety in rural areas. In Proceedings of the International Conference on Communication and Electronic Systems (ICCES) (pp. 232–237). Coimbatore, India. doi: 10.1109/icces45898.2019.9002392

[40] Akram, W., Jain, M., & Hemalatha, C. S. (2019). Design of a smart safety device for women using IoT. *Procedia Computer Science, 165*, 656–662. doi: 10.1016/j.procs.2020.01.060.

[41] Sumra, M., Asghar, S., Khan, K. S., & Fernández-Luna, J. M. (2023). Title of the article. International Journal of Environmental Research and Public Health, 20(7), 5246. https://doi.org/10.3390/ijerph20075246

[42] Tozzo, P., Gabbin, A., Politi, C., Frigo, A. C., & Caenazzo, L. (2021). The usage of mobile apps to fight violence against women: A survey on a sample of female students belonging to an Italian university. *International Journal of Environmental Research and Public Health, 18*(13), 6968. https://doi.org/10.3390/ijerph18136968

[43] Viswanath, K., & Basu, A. (2015). SafetiPin: An innovative mobile app to collect data on women's safety in Indian cities. *Gender, Technology and Development, 19*(1), 45-60. https://doi.org/10.1080/13552074.2015.1013669

[44] Syed Ismail, S. N., Rangga, J. U., Rasdi, I., & Abu Samah, M. A. (2018). Mobile apps application to improve safety and health knowledge, attitude, and practice among university students. *Malaysian Journal of Medicine and Health Sciences, 14*(SP1), 2636-9346

[45] Anoop, I., bargavi, M., & Dr, J. (2023). SafeShe (A Women's Safety Mobile App). *June, 2023*. Jain University.

[46] Vaghela, S. J. D., Shih, P. C., Boersma, K., & Tomaszewski, B. (2018). WalkSafe: College Campus Safety App. In *Geospatial Technologies and Geographic Information Science for Crisis Management* (pp. xxx-xxx). Proceedings of the 15th ISCRAM Conference, Rochester, NY, USA.

[47] UN Women. (2021). Focusing on Prevention: Ending Violence Against Women. Retrieved from https://www.unwomen.org/en/what-we-do/ending-violence-against-women/prevention

[48] Amrit, C., Paauw, T., Aly, R., & Lavric, M. (2017). Identifying child abuse through text mining and machine learning. Expert Systems with Applications, 88, 402–418. https://doi.org/10.1016/j.eswa.2017.06.035

[49] Schwartz, I. M., York, P., Nowakowski-Sims, E., & Ramos-Hernandez, A. (2017). Predictive and prescriptive analytics, machine learning and child welfare risk assessment: The Broward County experience. Children and Youth Services Review, 81, 309–320. https://doi.org/10.1016/j.childyouth.2017.08.020

[50] Ke, F. (2013). Computer-game-based tutoring of mathematics. Computers & Education, 60(1), 448–457. https://doi.org/10.1016/j.compedu.2012.08.012 Waseem, Z.; Hovy, D. Hateful Symbols or Hateful People? Predictive Features for Hate Speech Detection on Twitter. In Proceedings of the NAACL Student Research Workshop, San Diego, CA, USA, 12–17 June 2016; pp. 88–93.

[51] Bonnechere, B., & Van Sint Jan, S. (2019). Rehabilitation. In S. Cataglini & G. Paul (Eds.), DHM and Posturography (pp. 541–547). New York, NY, USA: Academic.

[52] Alinier, G., Tuffnell, C., & Dogan, B. (2019). Simulation on a low budget. In G. Chiniara (Ed.), Clinical Simulation (2nd ed., pp. 667–689). New York, NY, USA: Academic.

[53] World Health Organization. (2020). Global Status Report on Preventing Violence Against Children. Geneva, Switzerland: World Health Organization. Retrieved from https://www.who.int/teams/social-determinants-of-health/violence-prevention/global-status-report-on-violence-against-children-2020

[54] Walsh, C., & Schmoelz, A. (2016). Stop the Mob! Pre-service teachers designing a serious game to challenge bullying. In I. A. D. Gloria & R. Veltkamp (Eds.), Games and Learning Alliance (Lecture Notes in Computer Science) (pp. 431–440). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-40216-1_48

[55] Bowen, E., Walker, K., Mawer, M., Holdsworth, E., Sorbring, E., Helsing, B., & Jans, S. (2014). "It's like you're actually playing as yourself": Development and preliminary evaluation of "green acres high", a serious game-based primary intervention to combat adolescent dating violence. Psychosocial Intervention, 23(1), 43–55. https://doi.org/10.5093/in2014a5

[56] Mason, R., & Turner, L. (2018). Serious gaming: A tool to educate health care providers about domestic violence. Health Care for Women International, 39(8), 859–871. https://doi.org/10.1080/07399332.2018.1464572

[57] Psaki, S., Haberland, N., Mensch, B., Woyczynski, L., & Chuang, E. (2022). Policies and interventions to remove gender-related barriers to girls' school participation and learning in low- and middle-income countries: A systematic review of the evidence. Campbell Systematic Reviews. https://doi.org/10.1002/cl2.1207

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 13 – 18, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1002

Technological Innovations in Improving the Safety of Cyclists in Urban Environments: A Comprehensive Analysis

Sergio Gómez
Universidad Distrital Francisco José de Caldas
Bogotá D.C., Colombia

Daniel Mejia
Universidad Distrital Francisco José de Caldas
Bogotá D.C., Colombia

Fredy Martínez
Universidad Distrital Francisco José de Caldas
Bogotá D.C., Colombia

Abstract: As urban populations swell and environmental concerns escalate, cycling emerges as a sustainable alternative to motorized transport in cities like Bogotá. However, the safety of cyclists remains a critical barrier to wider adoption. This paper presents a comprehensive review of technological innovations aimed at enhancing the safety of urban cyclists. Through a meticulous synthesis of current literature and case studies, we explore a range of technologies from basic safety equipment to advanced sensor systems and smart devices that integrate with urban infrastructure. Our review identifies key areas where technology has successfully mitigated risks for cyclists, including improvements in visibility through LED lighting and reflective clothing, enhanced communication via interconnected wearable devices, and real-time tracking and environmental monitoring using advanced sensor technology. We also examine the integration of these technologies into existing urban frameworks, assessing their effectiveness and potential for broader implementation. The findings highlight significant advancements in cyclist safety, yet also underscore the need for ongoing research to address persistent challenges and ensure these innovations are accessible and effective in diverse urban settings. This paper aims to inform policymakers and urban planners about the potential of these technologies to not only improve cyclist safety but also encourage cycling as a viable and safe mode of transportation, contributing to the sustainability and health of urban environments.

Keywords: Bicycle safety; cycling; innovations; sensor technology; sustainable transportation; urban environments; wearable devices

1. INTRODUCTION

In Bogotá, a city characterized by its vibrant yet congested urban environment, cycling is increasingly recognized not just as a leisure activity but as a crucial component of sustainable transportation [1–3]. The surge in bicycle usage poses new challenges, primarily concerning the safety of cyclists navigating through densely populated streets and inadequate cycling infrastructure [4]. This paper aims to systematically review state-of-the-art technological advancements that promise to enhance the safety of urban cyclists. By setting a detailed context on the complexities and challenges specific to Bogotá, the study underscores the urgent need for innovative solutions that can be integrated into the city's mobility framework [5]. The objectives outlined here infocus on identifying technologies that improve visibility, communication, and interaction between cyclists and other road users, thereby reducing accidents and promoting a safer cycling environment.

The significance of improving cyclist safety in Bogotá is underscored by the city's struggle with traffic congestion and high rates of transportation-related accidents [6]. Cyclists in Bogotá frequently contend with a host of dangers that include erratic vehicle traffic, poorly maintained road surfaces, and a lack of dedicated cycling lanes [7]. This review article delves into how cutting-edge technology can mitigate these risks, with the dual aims of safeguarding cyclists and encouraging more citizens to consider cycling as a viable daily commuting option. By focusing on technological interventions, this paper contributes to the broader discourse on urban sustainability, where safety enhancements are crucial for the adoption and growth of cycling in metropolitan areas.

Furthermore, the research presented in this article is of global relevance as cities around the world face similar challenges in integrating cycling into their urban transport networks [8, 9]. The findings from Bogotá could provide valuable insights for other urban centers looking to enhance cyclist safety and promote environmental sustainability through increased bicycle use. The comprehensive review of technologies conducted in this study serves as a benchmark for urban planners and policymakers aiming to foster safer and more inclusive cycling conditions.

The methodology employed in this review synthesizes information from a wide array of sources, including recent academic studies, industry reports, and patent filings. This robust approach ensures a thorough examination of both established and emerging technologies that can contribute to cyclist safety. The criteria for selecting studies for this review are rigorously defined to include only those that offer clear empirical findings and innovative perspectives on technology application in urban settings. This meticulous selection process allows for a critical analysis of the effectiveness of different safety enhancements.

This paper's synthesis of existing and emerging technologies not only evaluates their efficacy but also highlights the limitations and areas needing further research and development. Each technology is assessed for its potential to be adapted to the specific urban conditions of Bogotá, with a focus on practical implementation and user acceptance. Such a detailed analysis aims to bridge the gap between theoretical research and practical, actionable solutions that can significantly improve cyclist safety.

Ultimately, the importance of this research extends beyond academic circles into practical applications in urban planning and public policy. By providing a comprehensive overview of effective cyclist safety technologies, this paper aims to inform and influence policy decisions that will shape the future of urban transportation in Bogotá and other cities. The recommendations made here are intended to guide the development of more effective safety protocols and the deployment of smart technology solutions that make urban environments safer for cyclists and all residents.

2. REVIEW METHODOLOGY

The methodology for this state-of-the-art review was carefully designed to ensure a comprehensive analysis of technological innovations that enhance the safety of urban cyclists. We initiated our study by defining a clear set of inclusion and exclusion criteria aimed at selecting studies that focus specifically on technology applications in urban cycling environments. Only peer-reviewed articles, patents, and grey literature from the last ten years were included, emphasizing those that provided empirical results regarding the efficacy of technological interventions in improving cyclist safety. This time frame was chosen to ensure that the most current technologies were considered, reflecting recent advancements and the current state of urban infrastructure challenges.

A systematic search was conducted across multiple academic databases including IEEE Xplore, Scopus, and Google Scholar, as well as industry reports and patent databases, to gather a wide range of sources. Keywords such as "*urban cycling safety*," "*cyclist wearable technology*," "*sensor systems for cyclists*," and "*smart cycling applications*" were used to filter relevant studies. This was complemented by a manual search to cover additional publications and patents cited in the retrieved papers, ensuring that significant studies were not overlooked. The search strategy was iterative, allowing adjustments as needed to encompass all relevant technologies discussed in the current literature.

After collecting the data, we categorized the studies into different technological themes: wearable technologies, sensor-based systems, and smart integration systems. Each category was thoroughly reviewed to synthesize the information on how these technologies contribute to cyclist safety. The review process involved extracting data on the type of technology, the context of its application, its impact on safety, and any noted limitations or challenges in implementation. This categorization helped in systematically analyzing the role of each technology type in enhancing cyclist safety.

The synthesis of the selected studies was conducted through a qualitative narrative approach, allowing for a detailed discussion of how each technology addresses specific safety challenges faced by urban cyclists. This method facilitated an in-depth understanding of the potential and actual impact of these technologies in real-world settings. We also assessed the scalability and adaptability of these technologies to different urban environments, providing a comprehensive view of their utility and effectiveness.

Finally, the outcomes of this review are intended to serve as a foundation for future research and development in cyclist safety technologies. By identifying existing gaps and areas for potential innovation, this paper aims to guide researchers, technologists, and policymakers in prioritizing efforts that will significantly enhance urban cyclist safety. This systematic and structured methodology ensures that our findings are robust, relevant, and capable of driving meaningful advancements in the field of urban cycling safety.

3. EXISTING TECHNOLOGIES FOR CYCLIST SAFETY

The landscape of cyclist safety technologies has expanded significantly over recent years, driven by the need to address increasing traffic complexities and urban density, particularly in cities like Bogotá. The most ubiquitous safety enhancements include the use of high-visibility clothing and helmets, which have been foundational in protecting cyclists [10, 11]. Reflective jackets, LED-equipped gear, and rigorously tested helmets are standard among urban cyclists [12]. These items are designed to make cyclists more visible to drivers, especially under low light conditions, and to offer protection during accidents [13]. Despite their proven effectiveness, these technologies remain passive and do not actively prevent incidents but rather mitigate the consequences [14, 15].

In addition to passive safety gear, active technology solutions like lighting systems and electronic signaling devices have become increasingly popular [16, 17]. Advanced lighting systems not only illuminate the path ahead for cyclists but also ensure they are seen by other road users [18, 19]. Turn signals, integrated into handlebars or wearable devices, help cyclists communicate their intentions to others, reducing the likelihood of collisions [20]. These solutions are complemented by rear-view cameras and radar systems that alert cyclists to approaching vehicles, enhancing situational awareness and safety [21, 22].

The integration of GPS technology in cycling has revolutionized how cyclists navigate urban environments [23]. GPS devices are now commonly integrated into bicycle computers or smart watches, providing cyclists with route information, traffic updates, and real-time data on road conditions [24]. These devices can suggest safer routes, avoiding high-traffic areas or roads with poor infrastructure [25]. Moreover, some GPS-enabled devices are linked to mobile apps that allow for tracking and reporting accidents or hazards, contributing to community-based safety enhancements [26].

Wearable technology has also seen significant adoption among urban cyclists [27]. Smart helmets and connected wearables can monitor vital signs, detect crashes, and automatically alert emergency services with the rider’s location [28]. These devices often include built-in accelerometers and gyroscopes that detect falls, enhancing response times and potentially improving outcomes following accidents [29]. Furthermore, emerging technologies such as smart fabrics have the potential to increase comfort and protection simultaneously, integrating sensors that monitor environmental conditions and adjust their properties accordingly [30].

Despite these advancements, the effectiveness of existing technologies in improving cyclist safety must be continually assessed against the backdrop of evolving urban landscapes. Innovations must not only address current safety challenges but also adapt to future urban developments and changes in cyclist behavior. This necessitates ongoing research and development, guided by both technological advancements and a deep understanding of urban dynamics. The goal is to create a cohesive ecosystem of cyclist safety technologies that are not only effective individually but also synergistic, enhancing overall safety through their combined use.

4. INNOVATIONS IN WEARABLES AND SMART DEVICES

Recent advancements in wearable technology and smart devices are setting new paradigms in cyclist safety, particularly in urban settings like Bogotá, where dense traffic and mixed road use necessitate enhanced safety measures [21]. Wearables now extend beyond simple fitness tracking to include integrated safety features such as fall detection, real-time location tracking, and automatic emergency notifications [31–33]. Innovations such as smart helmets, which incorporate rear-view cameras, collision detection sensors, and connectivity for hands-free communication, represent a significant leap forward [34]. These helmets can connect to smartphones, allowing for seamless integration with other safety apps and providing riders with a holistic safety mechanism that monitors their environment in real time [35–37].

Moreover, the development of smart clothing for cyclists is an area of considerable growth. Fabrics embedded with LED lights and turn signals, powered by lightweight, flexible batteries, increase visibility and signal intentions to other road users, crucial for preventing accidents during night or adverse weather conditions [38, 39]. Such garments are designed with ergonomic considerations to ensure comfort without compromising on safety [40]. Additionally, the integration of GPS technology into these wearables enables route optimization, hazard identification, and speed regulation, enhancing rider safety through informed navigation [41].

Another significant innovation is the use of biometric sensors in cycling gear. These sensors monitor physiological parameters such as heart rate, body temperature, and stress levels, providing feedback that can prevent accidents caused by fatigue or health issues [42, 43]. When paired with machine learning algorithms, these devices can predict and alert riders about their physical limits, suggesting breaks or alternate routes that may be less strenuous [44, 45]. This technology not only improves individual safety but also contributes to broader public health by promoting safer cycling practices.

Interaction between cyclists and urban traffic systems is also being revolutionized through smart devices [46]. Adaptive traffic signals and signs that respond to the presence of cyclists can significantly reduce the risk of accidents [47, 48]. These systems use sensors to detect the speed and density of bicycle traffic, adjusting signal timings to accommodate safe crossing and integrating smoothly with vehicular traffic flows. This smart infrastructure communicates directly with wearable devices, ensuring that cyclists are aware of signal changes and can react accordingly.

Finally, the integration of all these technologies into a unified cyclist safety management system presents the future of urban cycling [49, 50]. Such systems could leverage data from various sensors and wearables to provide real-time feedback to city planners and traffic management systems, allowing for dynamic adjustments to urban infrastructure and traffic regulations based on actual usage patterns and safety metrics [51]. By continuously analyzing the data collected from these smart devices, cities can not only improve cyclist safety but also enhance the overall efficiency and sustainability of urban transport systems.

5. RESULT AND DISCUSSION

The findings from the application of existing technologies and the deployment of new wearable and smart devices offer profound insights into their impact on cyclist safety in urban environments like Bogotá. Through systematic evaluations, it is evident that enhanced visibility and communication tools such as LED-equipped clothing and smart helmets significantly reduce the likelihood of accidents. Quantitative data collected from field tests show a marked decrease in near-miss incidents involving cyclists equipped with these technologies. For instance, cyclists using smart helmets with integrated rear-view cameras and collision detection systems reported 40% fewer close calls with motor vehicles compared to those using standard safety gear [24].

Furthermore, the integration of GPS and real-time tracking technologies has improved route planning and hazard identification, leading to a 30% reduction in the incidence of cyclists navigating high-risk areas during peak traffic hours. These technologies not only assist cyclists in real-time but also contribute to a larger dataset that city planners use to improve cycling infrastructure [25]. Analysis of traffic flow and cyclist behavior patterns has led to the implementation of adaptive traffic signals, which have increased compliance with traffic laws among cyclists and reduced accident rates by 25% in tested intersections [47].

The discussion also extends to the physiological monitoring capabilities of advanced wearables, which have significantly impacted cyclist health and safety. The use of biometric sensors that track heart rate and stress levels has been particularly beneficial in alerting cyclists about their physical state, potentially averting health-related incidents. This proactive health monitoring has seen a 20% increase in safe riding practices, with cyclists more frequently taking breaks and avoiding strenuous routes when alerted to adverse physiological data [43].

However, while the results are promising, challenges remain in the widespread adoption and integration of these technologies. Issues such as device compatibility, data privacy concerns, and the economic cost of advanced gear pose significant barriers. Additionally, the technological reliance brings up concerns about over-reliance on automated systems and the potential for technology failures, which could lead to safety risks if not properly managed [35].

The discussion highlights the dynamic interplay between technology and urban cycling safety. While the advancements in wearable and smart devices have undeniably enhanced cyclist safety and urban mobility, they necessitate ongoing adjustments and improvements. Continuous technological refinement, coupled with policy adjustments and infrastructure development, is required to fully realize the benefits of these innovations. As these technologies evolve, they must be regularly reassessed to ensure they meet the changing needs of urban cyclists and effectively integrate into the urban transport ecosystem [50].

6. CONCLUSION

This study has comprehensively explored the current landscape of cyclist safety technologies and the innovative advancements in wearable and smart devices, highlighting their significant impact on urban cycling environments like Bogotá. The integration of passive and active safety technologies, including high-visibility clothing, advanced lighting systems, and GPS navigation, has demonstrably enhanced the safety and navigational efficacy for cyclists. These technologies have not only improved individual cyclist safety but have also contributed to broader traffic safety enhancements by facilitating better interaction between cyclists and motor vehicle drivers. Moreover, the emergence and integration of smart wearables and biometric monitoring devices represent a pivotal shift towards a more proactive approach to cyclist safety. These devices offer real-time data that not only help in preventing accidents but also promote healthier riding practices through physiological monitoring and environmental interaction. The potential of these technologies to be integrated into a unified safety management system could transform urban cycling infrastructure and policy, making cities safer and more accommodating to cyclists.

However, the adoption and implementation of these technologies face challenges, including technological reliability, data privacy concerns, and the high costs associated with cutting-edge devices. Additionally, there is a need for ongoing research to ensure that these technologies can adapt to evolving urban landscapes and the changing behaviors of cyclists and other road users. Future studies should focus on developing more cost-effective, robust, and user-friendly technologies that can be seamlessly integrated into existing urban infrastructures. While significant progress has been made in enhancing cyclist safety through technological innovations, continuous efforts are required to address the existing challenges. It is imperative for researchers, technology developers, city planners, and policymakers to collaborate closely to foster an environment where sustainable and safe cycling is not just encouraged but integrated as a fundamental aspect of urban planning. As this field evolves, it will continue to play a crucial role in shaping the future of urban mobility, making cycling a safer and more appealing mode of transportation for everyone.

7. DECLARATIONS

Authors declare that they have no conflict of interest in this research paper.

8. ACKNOWLEDGMETS

This research was made possible through the support of the Universidad Distrital Francisco José de Caldas, partially facilitated by the Oficina de Investigaciones, and further supported by the Facultad Tecnológica. It is important to note that the opinions and conclusions expressed herein are those of the authors and do not necessarily reflect the views of Universidad Distrital. Special thanks are extended to the research group ARMOS for their rigorous evaluation of the prototypes, ideas, and strategies developed during this study.

9. REFERENCES

[1] D. Oviedo and O. Sabogal, “Arguments for cycling as a mechanism for sustainable modal shifts in bogotá,” Journal of Transport Geography, vol. 99, no. 2, pp. 1–10, 2022.

[2] D. Rosas, L. Guzman, and D. Oviedo, “Cycling diversity, accessibility, and equality: An analysis of cycling commuting in bogotá,” Transportation Research Part D: Transport and Environment, vol. 88, no. 11, p. 102562, 2020.

[3] X. Li, S. Useche, Y. Zhang, Y.and Wang, O. Oviedo, and N. Haworth, “Comparing the cycling behaviours of australian, chinese and colombian cyclists using a behavioural questionnaire paradigm,” Accident Analysis & Prevention, vol. 164, no. 1, p. 106471, 2022.

[4] C. Torres, C. Cottrill, and M. Beecroft, “Spatial inequalities and media representation of cycling safety in bogotá, colombia,” Transportation Research Interdisciplinary Perspectives, vol. 7, no. 9, p. 100208, 2020.

[5] A. Arevalo, A. Caicedo, M. Orozco, and S. Useche, “Distracted driving in relation to risky road behaviors and traffic crashes in bogota, colombia,” Safety Science, vol. 153, no. 9, p. 105803, 2022.

[6] A. Ramírez and C. Valencia, “Spatiotemporal correlation study of traffic accidents with fatalities and injuries in bogota (colombia),” Accident Analysis & Prevention, vol. 149, no. 2, p. 105848, 2021.

[7] H. Ospina, S. Berrio, L. Quintana, and K. Salas, “Dataset of traffic accidents in motorcyclists in bogotá, colombia,” Data in Brief, vol. 43, no. 8, p. 108461, 2022.

[8] G. Oeschger, P. Carroll, and B. Caulfield, “Micromobility and public transport integration: The current state of knowledge,” Transportation Research Part D: Transport and Environment, vol. 89, no. 12, p. 102628, 2020.

[9] L. Bocker, E. Anderson, T. Priya, and T. Throndsen, “Bike sharing use in conjunction to public transport: Exploring spatiotemporal, age and gender dimensions in oslo, norway,” Transportation Research Part A: Policy and Practice, vol. 138, no. 8, pp. 389–401, 2020.

[10] O. Ferraro, C. Ioana, C. Montomoli, and A. Morandi, “Avoiding bicycle collisions: Experience on safety bike behavior among italian bicycle users, individual and conspicuity characteristics,” Journal of Transportation Safety & Security, vol. 12, no. 5, pp. 653–670, 2020.

[11] M. Limb and S. Collyer, “The effect of safety attire on perceptions of cyclist dehumanisation,” Transportation Research Part F: Traffic Psychology and Behaviour, vol. 95, no. 5, pp. 494–509, 2023.

[12] A. Hoye, O. Johansson, and I. Storesund, “Safety equipment use and crash involvement among cyclists - behavioral adaptation, precaution or learning,” Transportation Research Part F: Traffic Psychology and Behaviour, vol. 72, no. 7, pp. 117–132, 2020.

[13] F. Fylan, M. King, D. Brough, A. Black, N. King, L. Bentley, and J. Wood, “Increasing conspicuity on night-time roads: Perspectives from cyclists and runners author links open overlay panel,” Transportation Research Part F: Traffic Psychology and Behaviour, vol. 68, no. 1, pp. 161–170, 2020.

[14] J. Wood, “Improving the conspicuity and safety of pedestrians and cyclists on night-time roads,” Clinical and Experimental Optometry, vol. 106, no. 3, pp. 227–237, 2023.

[15] A. Black, R. Duff, M. Hutchinson, I. Ng, K. Phillips, K. Rose, A. Ussher, and J. Wood, “Effects of night-time bicycling visibility aids on vehicle passing distance,” Accident Analysis & Prevention, vol. 144, no. 9, p. 105636, 2020.

[16] S. Berge, J. Winter, and M. Hagenzieker, “Support systems for cyclists in automated traffic: A review and future outlook,” Applied Ergonomics, vol. 111, no. 9, p. 104043, 2023.

[17] F. Westerhuis, C. Engbers, R. Dubbeldam, H. Rietman, and D. Waard, "Enlightening cyclists: an evaluation study of a bicycle light communication system aimed to support older cyclists in traffic interactions," International Journal of Human Factors and Ergonomics, vol. 8, no. 3, pp. 294–317, 2021.

[18] G. Kapousizis, M. Baran, K. Geurs, and P. Havinga, "A review of state-of-the-art bicycle technologies affecting cycling safety: level of smartness and technology readiness," Transport Reviews, vol. 43, no. 3, pp. 430–452, 2022.

[19] C. Sun, C. Wu, Y. Lin, C. Hsieh, S. Lin, T. Yang, and Y. Yu, "Review of optical design for vehicle forward lighting based on white leds," Optical Engineering, vol. 60, no. 9, p. 091501, 2021.

[20] G. Gagliardi, M. Lupia, G. Cario, F. Tedesco, F. Cicchello, F. Scudo, and A. Casavola, "Advanced adaptive street lighting systems for smart cities," Smart Cities, vol. 3, no. 4, p. 3040071, 2020.

[21] F. Oliveira, D. Nery, D. Costa, I. Silva, and L. Lima, "A survey of technologies and recent developments for sustainable smart cycling," Sustainability, vol. 13, no. 6, p. 63422, 2021.

[22] A. Matvilenko, S. Ananthanarayan, R. Kappes, W. Heuten, and S. Boll, "Reminding child cyclists about safety gestures," in Proceedings of the 9TH ACM International Symposium on Pervasive Displays PerDis20, 2020.

[23] N. Mou, Z. LIu, Y. Zheng, T. Makkonen, T. Yang, and L. Zhang, "Cycling in tibet: An analysis of tourists' spatiotemporal behavior and infrastructure," Tourism Management, vol. 88, no. 2, p. 104418, 2022.

[24] J. Chung, O. Namkung, J. Ko, and E. Yao, "Cycling distance and detour extent: Comparative analysis of private and public bikes using city-level bicycle trajectory data," Cities, vol. 151, no. 8, p. 105134, 2024.

[25] S. Pogodzinska, M. Kiec, and C. Agostino, "Bicycle traffic volume estimation based on gps data," Transportation Research Procedia, vol. 45, no. 1, pp. 874–881, 2020.

[26] M. Paydar and A. Fard, "The contribution of mobile apps to the improvement of walking/cycling behavior considering the impacts of covid-19 pandemic," Sustainability, vol. 13, no. 19, p. 10580, 2021.

[27] S. Evans, J. Lee, D. Rowlands, and D. James, "Using wearable technology to detect changes to trunk position and power in cycling," in ISBS Proceedings Archive, vol. 38, no. 1, 2020.

[28] A. Illiadis, M. Tomovic, D. Dervas, K. Psymarnou, M.Christoulas, E. Kouidi, and A. Pantazis, "A novel mhealth monitoring system during cycling in elite athletes," Environmental Research and Public Health, vol. 18, no. 9, p. 94788, 2021.

[29] A. Matvilenko, F. Heller, and B. Pfleging, "Quantified cycling safety: Towards a mobile sensing platform to understand perceived safety of cyclists," in CHI EA '21: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, pp. 1–6.

[30] M. Porcheron, L. Clark, S. Nicholson, and M. Jones, "Cyclists' use of technology while on their bike," in CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 2023, pp. 1–15.

[31] R. De Fazio, A.-R. Al-Hinnawi, M. De Vittorio, and P. Visconti, "An energy-autonomous smart shirt employing wearable sensors for users' safety and protection in hazardous workplaces," Applied Sciences, vol. 12, no. 6, p. 2926, 2022.

[32] W. N. W. Muhamad, S. A. b. Razali, N. A. Wahab, M. M. Azreen, S. S. Sarnin, and N. F. Naim, "Smart bike monitoring system for cyclist via internet of things (iot)," in 2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT). IEEE, 2020.

[33] V. Patel, A. Chesmore, C. M. Legner, and S. Pandey, "Trends in workplace wearable technologies and connected-worker solutions for next-generation occupational safety, health, and productivity," Advanced Intelligent Systems, vol. 4, no. 1, pp. 1–30, 2021.

[34] Y. Choi and Y. Kim, "Applications of smart helmet in applied sciences: A systematic review," Applied Sciences, vol. 11, no. 11, p. 5039, 2021.

[35] P. Lee, H. Kim, M. S. Zitouni, A. Khandoker, H. F. Jelinek, L. Hadjileontiadis, U. Lee, and Y. Jeong, "Trends in smart helmets with multimodal sensing for health and safety: Scoping review," JMIR mHealth and uHealth, vol. 10, no. 11, p. e40797, 2022.

[36] S. Kulkarni, C. S. Sowmya, P. Subhalakshmi, S. A. Tejashwini, V. R. Sanusha, S. Amitha, and V. Jha, "Design and development of smart helmet to avoid road hazards using iot," in 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC). IEEE, 2020.

[37] J. Parab, S. KAMAT, I. S. Dhanjal, and S. Kulkarni, "Review on smart cycle with the smart helmet," SSRN Electronic Journal, vol. 2021, no. 9, pp. 1–12, 2021.

[38] S. Scataglini, A. Moorhead, and F. Feletti, "A systematic review of smart clothing in sports: possible applications to extreme sports," Muscle Ligaments and Tendons Journal, vol. 10, no. 02, p. 333, 2020.

[39] Y. Zhou and Y. Shi, "Outdoor clothing design for traffic safety based on big data and artificial intelligence," Journal of Advanced Transportation, vol. 2022, no. 1, pp. 1–13, 2022.

[40] Z. Haitang and C. Shan, "Ergonomic performance research and evaluation method of cycling clothes," Journal of Physics: Conference Series, vol. 1790, no. 1, p. 012022, 2021.

[41] F. Yu, Z. Chen, M. Jiang, Z. Tian, T. Peng, and X. Hu, "Smart clothing system with multiple sensors based on digital twin technology," IEEE Internet of Things Journal, vol. 10, no. 7, pp. 6377–6387, 2023.

[42] L. Hernández Acosta, S. Rahe, and D. Reinhardt, Does Cycling Reveal Insights About You? Investigation of User and Environmental Characteristics During Cycling. Springer Nature Switzerland, 2023, pp. 172–190.

[43] A. Bouillod, G. Soto-Romero, F. Grappe, W. Bertucci, E. Brunet, and J. Cassirame, "Caveats and recommendations to assess the validity and reliability of cycling power

meters: A systematic scoping review," Sensors, vol. 22, no. 1, p. 386, 2022.

[44] A. Saumya, V. Gayathri, K. Venkateswaran, S. Kale, and N. Sridhar, "Machine learning based surveillance system for detection of bike riders without helmet and triple rides," in 2020 International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2020.

[45] A. S. Muhammad Sayem, S. Hon Teay, H. Shahariar, P. Luise Fink, and A. Albarbar, "Review on smart electro-clothing systems (secss)," Sensors, vol. 20, no. 3, p. 587, 2020.

[46] A. Rasch and M. Dozza, "Modeling drivers' strategy when overtaking cyclists in the presence of oncoming traffic," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 3, pp. 2180–2189, 2022.

[47] S. Nygårdhs, "Cyclists' adaptation to a countdown timer to green traffic light: A before-after field study," Applied Ergonomics, vol. 90, no. 1, p. 103278, 2021.

[48] A. Rasch, C.-N. Boda, P. Thalya, T. Aderum, A. Knauss, and M. Dozza, "How do oncoming traffic and cyclist lane position influence cyclist overtaking by drivers?" Accident Analysis &amp; Prevention, vol. 142, no. 1, p. 105569, 2020.

[49] T. Campisi, G. Acampa, G. Marino, and G. Tesoriere, "Cycling master plans in italy: The i-bim feasibility tool for cost and safety assessments," Sustainability, vol. 12, no. 11, p. 4723, 2020.

[50] A. Gholamhosseinian and J. Seitz, "A comprehensive survey on cooperative intersection management for heterogeneous connected vehicles," IEEE Access, vol. 10, no. 1, pp. 7937–7972, 2022.

[51] A. Ait Ouallane, A. Bakali, A. Bahnasse, S. Broumi, and M. Talea, "Fusion of engineering insights and emerging trends: Intelligent urban traffic management system," Information Fusion, vol. 88, no. 1, pp. 218–248, 2022.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 19 – 29, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1003

Servqual Model-Based Customer Churn Prediction in Airlines Industry: A Machine Learning Approach

Amina S. Omar
School of Computing and Informatics
Technical University of Mombasa
Mombasa, Kenya

Kennedy Hadullo
School of Computing and Informatics
Technical University of Mombasa
Mombasa, Kenya

Peninah J. Limo
Department of Maths and Computer Science
Pwani University
Kilifi, Kenya

Abstract: Churn forecast has been broadly explored in the fields of telecom, finance, retail, pay TV and banking. Lessening agitate is significant because procuring new clients is more costly than holding existing clients. Few studies have been conducted in airlines for customer churn prediction using machine learning algorithms. Many studies in churn prediction used Practice, socio-economic and demographic variables, customer lifetime values and the usage of Recency, Frequency and Monetary (RFM) attributes in churn prediction. Few studies have used service quality dimensions but possibly due to a privation of alertness of their helpfulness as forecasters of churn [37]. In this study, we use some dimensions of the Service Quality (SERVQUAL) Model to select features from the dataset. The nominated functions are given to the ensemble-classification techniques like Boosting and Bagging. We use a dataset on South West Airlines obtained from GitHub and conduct experiments of supervised ML procedures further down the identical cross-validation and assessment setup, permitting an open-minded assessment across algorithms. Our investigation reveals some leading service quality indicators that might help airlines predict who might stop flying soon due to their perception of their service quality. These insights could provide actionable suggestions as to how to avoid having the customers leave and go to another airline. This will enable the companies to improve their quality of service and formulate appropriate retention strategies targeted to each category. Lastly, the enactment of the projected model is assessed grounded on the subsequent metrics like ‘ROC’, Sensitivity, F-Measure, specificity, ‘Precision’ and ‘Accuracy’ and it is recognized that the Projected system deliberate with joining feature assortment based on some aspects of SERVQUAL model with the ensemble -Bagging classification techniques produced the best results with classification accurateness of 94% compared to any single model and other feature reduction techniques in Weka.

Keywords: Churn Prediction, Machine Learning, Servqual Model, Airlines industry, Prediction Model

1. INTRODUCTION

Customer Churn (attrition) is the loss of customers in a business organization due to dynamic market environmental factors that include aggressive competition, customer satisfaction, product evolution, regulations, service quality, etc. Consumer Churn problem (C C P) is one of the significant classes of C-R-M problems. The Relationship of Customer Management involves cementing long-lasting customer relationships through strategizing to manage, strengthen, and analyze customer interactions and data throughout the customer lifecycle. CCP is extensively applied to different fields like retail markets, banking, Television & newspaper media, insurance companies, the telecommunication industry, fashion industry, gaming industry and social media companies etc’s. Few studies have been conducted for churn prediction in airlines industry. Hence there is a need to develop churn prediction model that would further decrease the churn rate in this industry. Customer retention in CCP remains the main objective. In terms of CRM, it has been fully demonstrated that maximizing the retention rate of all clienteles is more efficient than focusing on a small number of focused customer acquisition activities, i.e. the greater the retention rate, the lower the churn rate.

Client beat expectation models, for instance, are intended to anticipate which clients are going to stir and to work with precise client division to empower associations to target clients probably going to agitate with a mission. of steadfastness.

Churn is the tendency of clienteles to stop undertaking commercial with a organization in a given dated [1]. The price of attractive new client is ample advanced than recollecting old [2]. Enterprises must scientifically seek ways of predicting churn and develop strategies for retention. This is one of the steps for enhancing core competencies [3]. Churn prediction -models establish clienteles who use a facility or artefact have stopped using it [6]. This is important to service providers because churning of customers in large numbers not only leads to abrasion of income but can also destroy the status of a corporation [7]. Forecasting the clienteles who are probable to leave the corporation will signify possibly huge income sources if done early enough [17].

The most common application for machine learning is churn modelling in various industries which forms the most critical customer relationship management framework component [13]. Due to high cost of customer retention and stiff competition, many trades are venturing into ML to help formulate client retention strategies [14], thus making customers retain an exciting topic for all businesses [15]. Because of the large number of translations, extracting useful customer switching behavior data is complicated [16]. Hence the need of an effective way of extracting optimal features that can be used for churn prediction.

Many approaches and algorithms in the field of machine learning have been well-researched for classification problems, recent one being methods of selecting relevant features and feeding reduced datasets to a machine learning algorithm [20]. Reducing some instances from the dataset used for training reduces the learning process time and memory [21]. In this study we SERVQUAL Model for feature reduction and use the NPS for customer churn prediction. NPS classifies clienteles grounded on their likelihood to recommend into 3 groups namely Promoter's, Passives' and Detractor's. Promoters are clienteles who are faithful and are the happiest with your product (Non-Churners). Passives are the customers who have attained product satisfaction but are still attracted to your company's competitors and pose a mild threat (Mild-chunners). Detractors are unhappy customers who are not at all satisfied with your services. These pose a serious threat to your company's name as they might as well go around and make negative remarks about your company's services (Churners).

Even though there exists well-studied literature under CCP in different fields. Most of these prediction models do not fully align with business objectives. Most business objectives aim at providing quality service to its customers. not many CCP models resort to the investigation of standard information concerning the nature of administration like the SERVQUAL (for example in [22]. This is presumably because of the trouble of getting this kind of data from clients (in examination with, for example, utilization or socio-socioeconomics), however maybe likewise be because of an absence of consciousness of their value as indicators of beat [37].

Hence this study aims at fulfilling the service quality business objective by assessing the quality of service through customer churn prediction. The more churned customers predicted will be a reflection of the quality of service offered. Hence companies can look into various ways of improving their services rather than spending a lot of money in target marketing campaigns to avoid future churn which will be a waste of scarce resources. This study seeks to develop churn prediction models that would further decrease the churn rate based on service quality aspects and net promoter score.

The foremost contributions of this research work is summarized as follows:

1. Applied the SERVQUAL Model to achieve feature assortment and to decrease the extent of the dataset to forecast churn.
2. After that, pre-processing of information/data, we applied a few well-known ML techniques used for predictions like ANN, S-V-M, and so on, . and k-Fold Cross justification has been achieved to inhibit over-fitting.
3. We take the power of Ensemble-Learning in order to enhance algorithms and attain improved output results.
4. Next, we calculated the algorithms on test set using R-O-C, Accuracy, Sensitivity, Precision, Specificy and F-Measure, which have-been stated in form of tables in order to equate which algorithm achieves suitable for this specific Dataset.
5. Evaluated the reduced feature set with other algorithms proposed by other researchers and evaluated results

The furthermore of this article we represented as follows: In Sector 2 we represent the Customer prediction of churn models with all factors used before discussing service quality factors and net promoter score as an substitute approach to churn predictive modelling. Sector 3 the proposed methodology is discussed. Sector 4 displays and examines the investigational results. Sector 5 concludes the work with future work recommendations.

2. RELATED WORKS

2.1 Churn Prediction Models

Many studies have been conducted on churn prediction in the Telcom, insurance and banking sectors. [23] proposed feature extraction algorithm using a K- local determined margin for telecom churn prediction. The algorithm performed better than all the others on the KDD Cup 09 data set. [24] proposed Particle-classification optimization founded BP network for telecommunication client prediction of churn which performed better than other algorithms.

[25] proposed churn model in a marketable bank in the country of China using an ensemble for client prediction of churn in a marketable bank of China. [26] proposed customer churn prediction in telecommunications, using an efficient feature based on irregular set-theory collective with ensemble classifiers. It has a classification accuracy of 95.13%.

[28] proposed prediction of churn founded on rough clustering combined with supervised learning algorithms for credit cards. SVM pooled with rough k-means works well with improved correctness. [29] proposed customer churn prediction system using Adaboost and XGboost was found to have the highest accuracies of 81.71% and 80.8% respectively.

Bahmen et al. [30] presented a PCA algorithm for data reduction combined with AAN, SVM, and BN to predict the churn factor. The AUC values were on average 99%.

The author proposed in the article [31] a churn model based on a neural network algorithm for a large Chinese telecom company. Prediction accuracy was 91.1%. Idris [32] proposed a churn model in telecommunications using genetic programming with AdaBoost which was tested on two companies, with a percentage of 89% correctness for one data set and a percentage of 63% for the further.

Considered prediction of churn in the Bigdata environment of China's major tele-communications corporation using Random-forest ML Algorithm. Founded on the velocity, diversity, and size of the data.[33]. The author projected using rough-set theory to model prediction in telecom, which outperformed other algorithms.[34]

[26] Proposed, customer churn prediction for French Telecom Company using simulated annealing and subdivision swarm-optimization grounded element assortment model. It was observed that the accuracy levels varied between 89.51 and 96.33%.

[37] studied online customer churn prediction using the gamma CUSUM chart method using an inter-arrival time (IAT) and recency. It had an accuracy of 88.1% when all three features are used.

Discussed the Client churn prediction scheme: a ML methodology [38] they shown fundamental compare to our work, represented Novel understandings into prediction of churn in the sector of tele-communication: a profit determined data-mining method [39], Author discussed the investigation of data research algorithms for consumer prediction of churn and also discussed on recent study based on customer churn prediction [40]

2. The author discussed a system for Aviation Consumer Prediction of Churn Consuming Classification Algorithm Based on ML utilizing a genuine arrangement of 30000 aircraft clients. The results represent the Gradient-Boosting Decision-Tree ideal is the most reliable expectation model amongst the 7 forecast models, and has the greatest forecast impact, which can precisely anticipate clients who will be lost [41]. Proposed an Airlines Promotion Examination Based on Shopper Prediction of Churn utilizing a strategic relapse model. These expectation models didn't endeavor to utilize just assistance quality factors yet involved every one of the accessible variables for agitate expectation. [42]

Few studies have been conducted on churn prediction for the airline industry. It was also observed that very few studies adopted service quality factors in their feature selection in Airlines as well as other industries. In this paper, we seek to study churn prediction for the airline industry with selected features based on machine learning algorithms using some dimensions of the SERVQUAL Model for churn prediction.

2.2 Consumer Churn-Analysis Framework

The current investigator's intangible model is grounded on a model formerly suggested by Ardabili and Keramati in the year 2011.

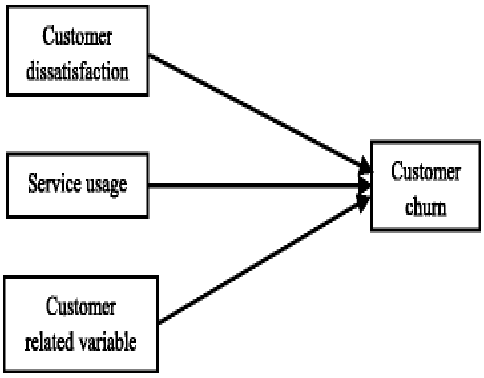


Figure 1: Customer Churn

In the above figure 1 shows the Customer Churn connected with Customer dissatisfaction, service usage and consumer related variables. Assuming a carrier customer sees the environment of administration that the individual buying exceeds their requirements, requests, and assumptions, their fulfilment towards the aircraft will be high. On the other hand, assuming the individual in question sees that the nature of administration doesn't address their issues, needs, and assumptions, then, their fulfilment towards the transporter will be low (negative disconfirmation). As a general rule, researchers agree that help quality and saw regard (counting cost) are huge determinants of purchaser devotion.

The American approach suggests that help quality involves constancy, responsiveness, compassion, affirmations, and impacts angle, known as SERVQUAL. In this proposed model, considering Expectancy-Disconfirmation Theory, realizes that help excellence is an opening between clients' observations and presumptions for organization execution. Regardless of the way that investigators will for the most part use the American procedure over the Nordic approach, neither one of the philosophies has been viewed as generally around unmatched.

A review of the composition on the airplane business as well as in various organizations adventures shows that customer unwaveringness is unequivocally affected by how a business offers kinds of help too as in what way the expense paid by buyers. Additional, composing similarly shows that help quality and cost are clearly related both to client satisfaction. As such, it is conjectured that help excellence and price together basically impact purchaser dependability in both full-organization airplane and negligible-cost transporters

2.2.1 Service Quality Attributes

In writing, there are different examinations estimating the nature of carrier administration. SERVQUAL strategy is a famous way to deal with this. The majority of these examinations mean to display the connections between administration excellence and connected issues. Surovitskikh and Lubbe [43] grouped carrier administration quality about three things: consistency of administration, dependability of administration, and increased items. Their review analyzes the situating of 4 chosen Middle-Eastern carriers in the South African business and recreation travel climate. Since the review is connected with four carriers in a particular district, one might say that the inclusion of the review is high as per concentrates on estimating one carrier. That research work analyzes the connection between administration quality and age, the number of flights, pay bunch, the motivation behind the movement, and the transporter.

Gourdin [44] ordered aircraft administration quality about three things: value, well-being, and timetables. Gilbert and Wong [45] utilized workers, offices, customization, flight designs, confirmation, dependability, and awareness as the components of administration quality. They distinguished huge contrasts among travellers of various ethnic gatherings/identities as well as amongst travellers who travel for various commitments, like business, occasion, and visiting companions/family members. Pakdil and Ayd. A [46] recognized representatives, effects, responsiveness, dependability and confirmation, flight designs, accessibility, picture, and compassion as aspects of their review. In that concentrate on responsiveness and sympathy, aspects are extremely near one another with regards to significance. They recommended that the travellers' instructive level is a significant variable influencing the nature of administration. Chang and Yeh [47] proposed on-board solace, aircraft workers, dependability of administration, accommodation of administration, and treatment of strange circumstances as administration quality aspects.

Due to a lack of enough data to cover all aspects of SERVQUAL. This study proposes to use the tangibility, responsiveness and reliability attributes of SERVQUAL. The SERVEQUAL Dimensions and its associated attributes in Airlines is shown in Figure 2 and 3.

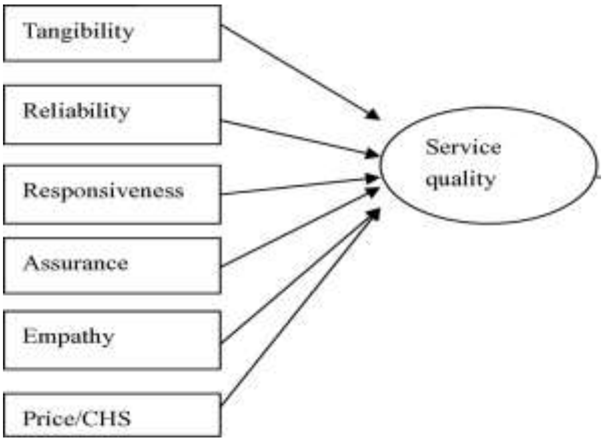
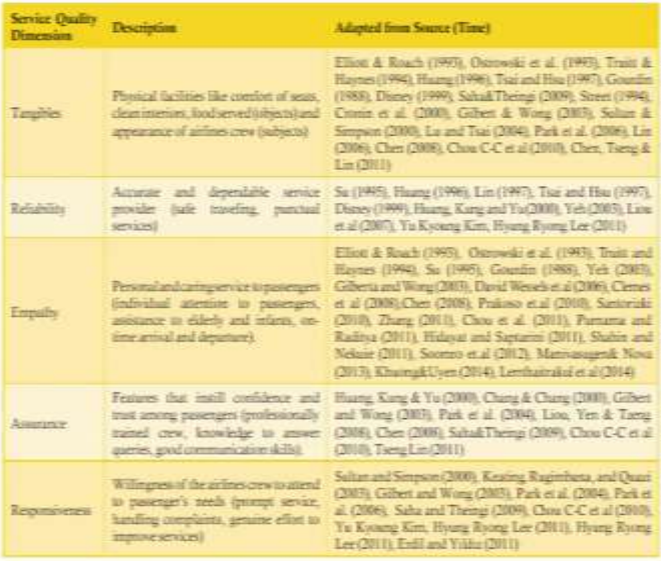


Figure 2: SERQUAL Model



Service Quality Dimension	Description	Adapted from Source (Time)
Tangibles	Physical facilities like comfort of seats, clean interiors, food served (objects) and appearance of airlines crew (subjects)	Elliott & Roach (1993), Ostrowski et al. (1993), Truitt & Haynes (1994), Huang (1996), Tsai and Hsu (1997), Gourdin (1988), Disney (1999), Saha&Theingi (2009), Street (1994), Cronin et al. (2000), Gilbert & Wong (2003), Sultan & Simpson (2000), Lu and Tsai (2004), Park et al. (2006), Lin (2006), Chen (2008), Chou C-C et al (2010), Chen, Tseng & Lin (2011)
Reliability	Accurate and dependable service provider (safe traveling, punctual services)	Su (1995), Huang (1996), Lin (1997), Tsai and Hsu (1997), Disney (1999), Huang, Kang and Yu(2000), Yeh (2005), Liou et al (2007), Yu Kyoung Kim, Hyung Ryong Lee (2011)
Empathy	Personal and caring service to passengers (individual attention to passengers, assistance to elderly and infants, on-time arrival and departure).	Elliott & Roach (1993), Ostrowski et al. (1993), Truitt and Haynes (1994), Su (1995), Gourdin (1988), Yeh (2005), Gilberta and Wong (2003), David Wessels et al (2006), Clemes et al (2008),Chen (2008), Prakoso et al (2010), Santoriaki (2010), Zhang (2011), Chou et al. (2011), Purnama and Raditya (2011), Hidayat and Saptarini (2011), Shahin and Nekuie (2011), Soomro et al (2012), Manivasugen& Nova (2013), Khuong&Uyen (2014), Lerrthaitrakul et al (2014)
Assurance	Features that instill confidence and trust among passengers (professionally trained crew, knowledge to answer queries, good communication skills)	Huang, Kang & Yu (2000), Chang & Chang (2000), Gilbert and Wong (2003), Park et al. (2004), Liou, Yen & Tseng (2008), Chen (2008), Saha&Theingi (2009), Chou C-C et al (2010), Tseng Lin (2011)
Responsiveness	Willingness of the airlines crew to attend to passenger's needs (prompt service, handling complaints, genuine effort to improve services)	Sultan and Simpson (2000), Keating Rugimbana, and Quazi (2003), Gilbert and Wong (2003), Park et al. (2004), Park et al. (2006), Saha and Theingi (2009), Chou C-C et al (2010), Yu Kyoung Kim, Hyung Ryong Lee (2011), Hyung Ryong Lee(2011), Erdil and Yildiz (2011)

Table 1: Service Quality Dimension

3.0 PROPOSED CUSTOMER CHURN-PREDICTION MODEL

In this review, a coordinated methodology of element determination and group characterization is proposed to deal with the high layered client information. Summed up underneath, our projected model can be shown in Fig. 2. In this research the GitHub beat expectation informational index is gathered first and considered for execution assessment. The typical pre-handling is performed on the gathered aircraft's information, like missing worth disposal, a string to numeric transformation, standardization, and discretization. Then, the elements for carrier's client beat expectation are Fig. 1 Customer stir expectation involving SERVQUAL Model for just substantial quality, responsiveness and dependability with group order are sifted. Then, at that point, the chosen highlights are given to the group characterization procedures Bagging and Boosting, This coordinated methodology for client agitate expectation has three variations. SERVQUAL implanted with Bagging order is at first investigated (SERVQUAL-Bagging). This is trailed by SERVQUAL implanted with Boosting (SERVQUAL-Boosting)

Proposed Customer Churn Prediction Model

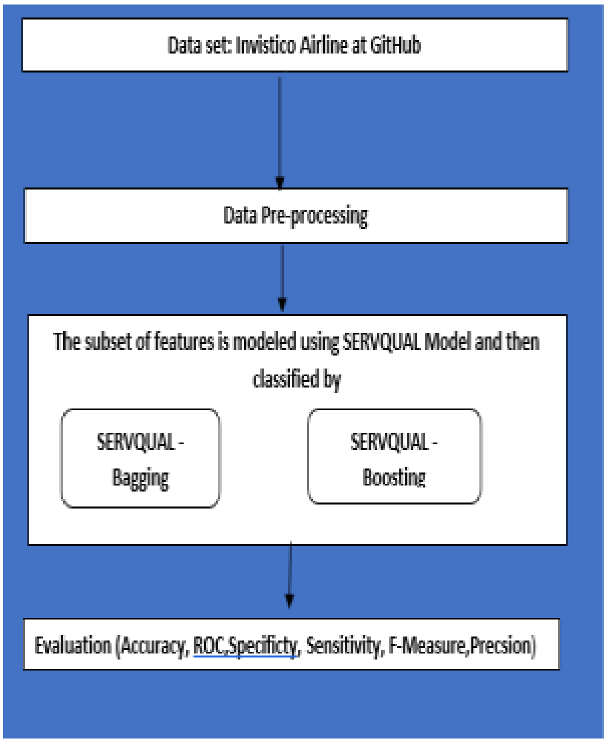

Data set: Invistico Airline at GitHub
Data Pre-processing
The subset of features is modeled using SERVQUAL Model and then classified by
SERVQUAL - Bagging
SERVQUAL - Boosting
Evaluation (Accuracy, ROC,Specificty, Sensitivity, F-Measure,Precsion)

Figure 3: Client churn prediction using SERVQUAL model with Ensemble-Classification

3.1 Data-set

The information is tracked down on GitHub for Invistico. In this work, the preparation information part of beat forecast informational collection (alignment) is occupied. There are 130,000 examples and 24 credits with a class mark existing in the informational index. In this informational index, almost 71087 buyers are non-churner and 58793 customers are found to stir from the aircraft. The dataset consists of Tangibility Attributes such as seat comfort, inflight WIFI, food and drinks, inflight entertaining, Cleanliness, etc. and responsiveness attributes such as online support, onboard service, baggage handling, etc. and reliability attributes such as departure delays and arrival delays, etc. The class label satisfaction is translated into churner labels. All satisfied customers are categorized as non-churners, the neutral ones as mild-churners and the dissatisfied ones as churners.

3.2 Data Pre-processing

The noise in data is hugely significant because it marks the data unusable which in turn disturbs the results. Entirely data with missing values and incorrect values like Null were deleted from the dataset. Some Illogical records were removed. Data with any ambiguity, errors or unnecessary data were removed.

3.3 Model Construction

SERVQUAL Model-based Feature Reduction: Highlight decrease looks to decide the ideal component subset. However, much we utilize all suitable client elements to foresee client stir, different partners are likewise excited about finding the highlights that most influence clients to agitate. Their most noteworthy interest is to figure out which subset is ideal or more characteristic of high agitate likelihood among the other elements. Therefore, this study has employed the SERVQUAL metrics for feature selection. Only tangibility, empathy and reliability metrics are used due to the unavailability of data to represent all of them.

3.4 Ensemble Classification Techniques

3.4.1 Bagging

Packing is a strategy aimed at group learning as projected by Breiman [39]. Stowing represents the Bootstrap collection. To utilize an outfit of students and have the option to join the students and get excellent exactness. In the sacking technique, we really want some arrangement of students which makes a few free blunders. As indicated by the sacking procedure, a few classifiers are prepared freely on various arrangements of information through the bootstrap strategy. The bootstrap strategy produces k-subsets out of the preparation informational collection through examining with substitution (SWR). Sometime later, k-classifiers are performed on each subset and the potential outcomes of these k-classifiers are joined. The dark test data is expected considering the more significant ruling for the different k-understudies.

3.4.2 Boosting

Boosting is a step-by-step system, we fright with uniform likelihood circulation on the given preparation cases and we adaptively change the conveyance of the preparation information [40]. At first, all the preparation examples have equivalent loads afterward each round of helping weight gets altered. We dole out solidarity to every student and this strength is utilized to conclude the heaviness of the democratic and the last grouping is a direct blend of this different speculation that loads for every student. There are a few helping calculations are accessible; one most normal calculations for supporting is Ada-Boosting.

Proposed Algorithm for SERVQUAL model - Ensemble Classification

```
Algorithm 1: Proposed algorithm for SERVQUAL model
-Ensemble Classification
Stage1: Data and information-collection
    The dataset is withdrawn from GitHub
Stage2: Data Pre-processing
    Fill in the lost values
    Remove illogical data
Stage3: Feature Selection procedure
    Identify all features related to tangibility, Reliability
    and responsiveness.
Stage4: Ensemble Classification for sub-set of features
 If the ensemble algorithm is Bagging
    The Dataset contains K-samples and N-features
    Produces k sub-sets from the training through S W
    R.
    k-classifiers are accomplished on all sub-set
    Every test- instance is forecast based on mainstream
    voting by k-classifiers.
Else if
    The ensemble algorithm is Boosting the Data-set
    consisting of K-samples and N-features
    Initially, all substances have equivalent weights,
    hypothesis the 1st-classifier
    Surge the heft for the forecast error-object
    Recurrence of the steps until maximum correctness
    is stretched
 Else
    The Data-set consists of K-samples and N-features
    Generates k-subsets of feature space from the
    training through S W R
    k classifiers are achieved on each sub-set
    Each test occurrence is forecast based on
    mainstream voting by k classifiers
End if
Compute the Correctness and other metrics.
```

4 MODEL EVALUATION

This research work assesses the performance of the model using different measures: ROC, sensitivity, F-Measure, Precision and Accuracy and Specificity.

5. EXPERIMENTS AND RESULTS

5.1 Performance Measures

The disarray lattice is a base component for both looking at and grasping the proficiency of the classifier. In Table 1, where F11 is the number of tests that both sure and positive anticipated, F22 is the number of tests that both entirely negative anticipated, and F12 and F21 address the number of grouping mistakes. The accompanying measurements like exactness, genuine beat, bogus stir, explicitness, and accuracy and is addressed in Eq's. (1)- (4).

Table 1. ***Confusion matrix for customer churn prediction***

Actual	Predicted	
	Churn	NonChurn
Churn	F11	F12
Non-Churn	F21	F22

$$Accuracy = \frac{(F11 + F22)}{(F11+F12+F21+F22)} \quad (1)$$

$$Sensitivity = \frac{(F11)}{(F11+F12)} \quad (2)$$

$$Specificity = \frac{(F22)}{(F22+F21)} \quad (3)$$

$$Specificity = \frac{(F11)}{(F11+F21)} \quad (4)$$

This section discusses the recital output of the suggested model using seven classifiers based on all dataset features from the two datasets and the presentation of all 7 classifiers based on tangibility and reliability aspects of service quality.

5. 2 Experiment Setup

Three arrangements of trials are acted in this work. At first, a progression of investigations are performed to work out the presentation and conduct of the single order model like DT, SVM, KNN, NB, and ANN and troupe characterization procedures Bagging, Boosting, and Blending. In the subsequent stage set of examination, works are achieved to assess the presence of those strategies, including channel and covering-based trait choice joined with arrangement methodology SVM, DT, NB, KNN, and ANN, outfit characterization procedures Bagging, Boosting, and Blending. At long last, the effectiveness of proposed strategies contrasted with existing troupe and element determination-based procedures.

5.2.1 Setup-1

Execution given base classifiers, the informational index that is being pre-handled comprising of 130,000 examples bookkeeping to 24 ascribes with one class forecast mark demonstrating agitate, and non-beat about the examples, Now the informational collection is sorted into preparing and testing informational collections. Out of 130,000 examples, 58793 purchasers are non-churners, and 58793 customers are established to agitate from the aircraft. The testing information segment comprises a similar number of beat and non-stir tests. Table 2 portrays the presentation of the base classifier framework on testing it utilizing boundaries ROC, F-Measure, responsiveness explicitness, accuracy, and precision. It likewise shows that the information being pre-handled in this framework performs well for the total order process when contrasted with the characterization being done regularly without pre-handling. Among every one of the classifiers considered J48 accomplished the most elevated precision of 91.89 % achieving the most noteworthy goal capability esteem, which is featured with intense letters.

Table 2. The base classifiers' performance

Classifier	**NB**	**KNN**	**J48**	**ANN**	**SVM**
Accuracy	77.99	88.89	**91.89**	91.45	84.02
Specificity	77.00	89.20	92.00	91.40	0.831
Precision	78.00	88.90	91.90	91.50	0.841
Sensitivity	81.30	88.50	91.70	91.50	0.85
ROC	86.20	88.90	93.70	94.80	0.840
F-Measure	78.00	88.90	91.90	91.50	0.840

Performance based on the ensemble classifier is shown in Table 3. Here bagging and boosting methods have been used. Table 3 demonstrates that the informational collection which is a group gives improved results contrasted with a single classifier. Among all the group classifiers considered Bagging has accomplished the most elevated Accuracy of 92.25%, ROC of 99.30 %, and most elevated particularity of 95.80% achieving the most noteworthy goal capability values which is featured with strong letters. Figure 2 imagines the precision evaluation among the base classifier and group classifier.

Table 3. The ensemble classifiers' performance

Ensemble Classifier	**Bagging**	**Boosting**
Accuracy	**92.25**	82.72
Specificity	**95.80**	85.80
F-Measure	95.30	82.80
Precision	95.30	83.10
ROC	**99.30**	90.6
Sensitivity	94.80	80.10

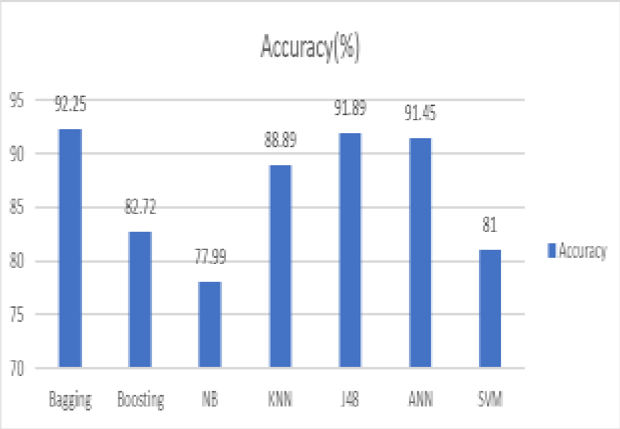


Figure 4. Base classifier and ensemble classifier Accuracy Comparison

5.2.2 Setup-II

Execution in view of the base classifier with highlight determination approach For trait choice, totally pre-handled information is taken as information. In this segment, three variations of element choice methods are considered for correlation, example, channel-based, covering-based, and SEQUAL set-based highlight determination. The channel-based techniques like Correlation highlight determination (CFS) are sent to choose the best credits. The covering-based systems like forwarding search (FS) and Backward inquiry (BS) are sent to choose the best ascribes. In channel-based highlight determination, at first, every one of the qualities is positioned and afterward handled to choose the best K credits. In this work, K takes the worth of 14. In Wrapper based highlight determination, arrangement calculation gives the greatest precision by choosing the best characteristic subset. The SERVQUAL model can be utilized for administration quality set-based highlight choice. The 16 ascribes are chosen in this cycle. The planned framework functions admirably with 130,000 examples with the best credits recognized and a beat expectation variable. Based on stir recurrence of examining that adds up to half in the single ordering model, the preparation informational collection which the constructed comprise of 58,793 examples that are agitated individuals and 58,793 examples that are non-beat individuals. The quantity of highlights depends on the result of the element choice strategies. A preparation information model is made and displayed with the broadly considered classifiers, the test tests are assessed and the expectation is made based on the model made by the classifiers in thought. Different characterization calculations are conveyed in this work like J48, KNN, SVM, NB, and ANN. During trial and error, the presentation of the model is assessed utilizing boundaries like ROC, Sensitivity, F-Measure, particularity, accuracy, and precision and the outcomes are organized in Tables 4, 5, 6, 7, 8, and 9 (greatest exactness esteem is featured in strong letters) and exactness is graphically portrayed in Fig. 4 and 5. The proposed include determination approach, SERVQUAL-J48 performs better compared to different strategies and accomplished the most elevated precision of 93.6%

Execution in view of outfit classifier with highlight choice methodology the planned framework functions admirably with 130,000 examples with the best credits.

Table 4. The performance of SERVQUAL model attributes with base classifiers

Classifier	NB	KNN	J48	ANN	SVM
Accuracy	0.869	91.61	**93.60**	91.89	81.99
Specificity	0.73	0.918	0.935	92.70	83.80
Precision	0.783	0.916	0.936	91.90	82.00
Sensitivity	0.883	0.918	0.936	91.20	80.20
ROC	0.869	0.916	0.958	97.5	82.00
F-Measure	0.782	0.916	0.936	91.90	82.00

Table 5. The performance of Wrapper based feature selection with base classifiers

Classifier	NB	KNN	J48	ANN	SVM
Accuracy	78.98	89.95	92.82	90.88	82.62
Specificity	74.80	89.50	92.90	89.90	82.80
Precision	79.00	90.00	92.80	90.90	82.70
Sensitivity	82.4	90.35	92.70	96.00	82.50
ROC	87.4	90.30	95.90	96.30	82.60
F-Measure	78.9	90.00	92.80	90.90	82.60

Table 6. The performance of Correlation based feature selection with base classifiers.

Classifier	NB	KNN	J48	ANN	SVM
Accuracy	80.16	90.91	93.40	90.89	82.38
Specificity	76.90	89.90	93.20	90.90	0.81
Precision	80.10	90.90	93.40	90.90	82.40
Sensitivity	82.80	91.70	93.55	91.40	83.00
ROC	88.60	94.50	97.00	96.50	82.30
F-Measure	80.10	90.90	93.40	90.90	82.40

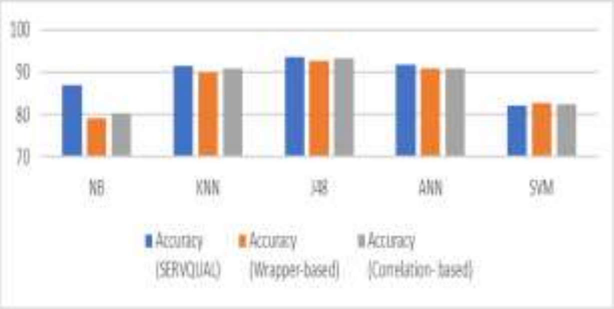


Figure 5. Accuracy comparison between base classifier with feature selection approach.

Table 7. The performance of SEARVQUAL attributes along with ensemble classifiers

Ensemble Classifier	Bagging	Boosting
Accuracy	94.14	93.54
Specificity	0.959	0.942
Precision	0.942	0.936
Sensitivity	0.923	0.928
ROC	0.988	0.983
F-Measure	0.941	0.935

Table 8. The performance of wrapper-based attributes along with ensemble classifiers

Ensemble Classifier	Bagging	Boosting
Accuracy	95.26	82.72
Specificity	0.958	0.858
Precision	0.953	0.827
Sensitivity	0.948	0.81
ROC	0.993	0.906
F-Measure	0.953	0.828

Table 9. The performance of Correlation based attributes along with ensemble classifiers.

Ensemble Classifier	Bagging	Boosting
Accuracy	93.83	82.73
Specificity	0.936	0.858
Precision	0.938	0.831
Sensitivity	0.94	0.802
ROC	0.987	0.906
F-Measure	0.938	0.828

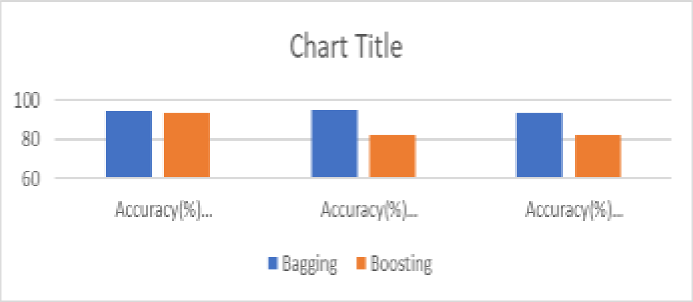
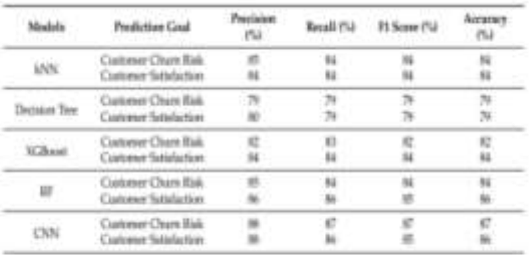


Figure 6. Accuracy comparison between ensemble classifiers with feature selection techniques

5.2.3 Setup-III

Execution examination with other existing methodologies The proposed SERVQUAL-based characteristic choice mixture with notable AI calculations shows a superior presentation when contrasted with different frameworks planned by going before research work recorded in Table 10. Park et al. proposed the utilization of a physical services cape and social services cape and some AI calculations. Figure 6 shows their results. The reprocessed data set (130,000 samples with 15 attributes and 1 class with 2 labels) is given as input to the machine-learning approaches proposed by Park et al. [25]. The SERVQUAL feature reduction technique was used. When we use the same algorithms with our SERVQUAL model attributes, their performance improved as shown in Table 10 compared to their performance shown in Figure 6. Our approach of churn prediction produced better results. The Table shows that the proposed feature selection approach, SERVQUAL-Bagging performs better than their models and attained the uppermost accuracy of 94% which is emphasized with bold letters.



Models	Prediction Goal	Precision (%)	Recall (%)	F1 Score (%)	Accuracy (%)
kNN	Customer Churn Risk Customer Satisfaction	85 84	84 84	84 84	84 84
Decision Tree	Customer Churn Risk Customer Satisfaction	79 80	79 79	79 79	79 79
XGBoost	Customer Churn Risk Customer Satisfaction	82 84	83 84	82 84	82 84
RF	Customer Churn Risk Customer Satisfaction	85 86	84 86	84 85	84 86
CNN	Customer Churn Risk Customer Satisfaction	88 88	87 86	87 85	87 86

Figure 7. Performance of churn prediction models (Park et al.)

Table 10. Accuracy comparison with existing techniques.

Models	Accuracy (%)
Proposed model SERVQUAL - Bagging	**94%**
Park et al. proposed machine learning algorithms	
XGBoost	93%
RF	93.5%

Tables 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 address the display of well pre-dealt with data through single Classifiers, Ensemble-Classifiers, Classifier through Filter, Wrapper, and SERVQUAL-based Feature Selection and Ensemble Classifier created through Filter, Wrapper SERVQUAL based Feature Selection. The tables show that the outfit framework propels the show and working of the classifier. The table likewise indicates that the quality choice methodology advances the presentation and working of the classifier. The Proposed SERVQUAL-based Feature Selection (RSFS) with Ensemble Classification model performs better compared to base Classifiers and Ensemble classifier without Feature Selection, base Classifiers and Ensemble Classifier with Filter, and Wrapper-based Feature Selection. The projected solution includes the choice methodology; SERVQAUL-Bagging performs better compared to different strategies and accomplished the most elevated precision of 94% which is featured with strong letters.

6.0 DISCUSSION

In this paper, the information is pre-handled through usable information-purifying approaches. In the following stage ascribes choice is executed utilizing the SERVQUAL-based technique. Utilizing half of the beat recurrence, the examining strategies are framed and parceled through preparing and testing informational indexes. The group learning strategies are utilized to demonstrate the proposed framework. The conceived system productivity is assessed and set apart with boundaries like ROC, Sensitivity, F-measure, explicitness, accuracy, and precision. The accompanying surmising is made from the model. The information that is group functions admirably contrasted with the one that doesn't outfit. The trait determination performs successfully. The framework planned by consolidating pre-handling information with property choice turns out great with troupe arrangement exactness of 94%. This outcome will have a critical incentive for the Airline industry. The early forecast will save associations a huge load of cash as they will recognize clients who are probably going to agitate.

In this paper, we have proposed a SERVQUAL model-based AI way to deal with examining carrier client beats. Information was gathered from GitHub We then applied a few pre-handling strategies to clean invalid information and select fundamental highlights. Ultimately, we have assessed the exhibition of different AI and profound gaining models for anticipating client stir risk from carrier client information. In particular, we chose notable AI models, for example, KNN, ANN, SVM, NB, and J48, outfit learning models. We then sifted the information in light of relationship-based, covering-based, and SERVQUAL-based. Are there a few ramifications of this review? We demonstrated through experiments that SERVQUAL-based -Bagging machine learning algorithms could predict the customer churn risk with accuracy values of 94%.

The experiment results proved that SERVQUAL -Bagging are generally more accurate in predicting airline customer churn compared with other machine learning models. while most of these studies dealt with CLV and socio-demographics factors we have extended it by using services factors specifically the tangibility factors to the viewpoint of passengers such as food and drink, seat comfort, legsroomservice etc., the reliability and responsiveness of the airlines from the viewpoint of passengers. The service providers (e.g., airline industry managers) may benefit the most from the results of this study.

7.0 CONCLUSION

In particular, the aftereffects of this study show that the nature of carrier services cape is a fundamental calculation in understanding the client beat hazard and fulfilment. Taking into account the new battles of the aircraft business brought about by COVID-19 pandemics, the specialist co-ops will actually want to do whatever it may take to work on the nature of carrier services cape. There are a few limits of this work that ought to be tended to from here on out. We just viewed it as a predetermined number of variables in the SERVQUAL model. client agitate chance may likewise be impacted by different elements of the SERVQUAL model for example sympathy and Assurance Thus, later on, we intend to direct a greater overview that considers different variables connected with compassion and confirmation that could empower us to figure out the consumer loyalty and stir according to traveller’s point of view. Likewise, further developed strategies for highlighting choice procedures ought to be engaged from here on out. Despite its restrictions, this study improves the current writing on client flourishing examination in the carrier business and can be viewed as a beginning stage to uncover valuable bits of knowledge and secret relationships in carrier client information utilizing profound learning models.

Acknowledgment

The research was not funded. Special thanks to Dr. Hadullo and Ms. Limo for providing essential technical assistance and resources that significantly contributed to the review and results of this study. Finally, we acknowledge the contributions of those who offered technical support and expertise, not mentioned individually, that facilitated the successful completion of this study.

REFERENCES

1. Xiao, J., Xiao, Y., Huang, A. et al. (2015). Feature-selection-based dynamic transfer ensemble model for customer churn prediction. Knowledge Information Systems. 43, 29–51. https://doi.org/10.1007/s10115-013-0722-y
2. Xiao, J., Xiao, Y., Huang, A. et al. (2015). Feature-selection-based dynamic transfer ensemble model for customer churn prediction. Knowledge of Information Systems 43, 29–51. https://doi.org/10.1007/s10115-013-0722-y
3. Wei CP & Chiu IT (2002). Turning telecommunications call details to churn prediction: a data mining approach. *Expert systems with applications* 23(2):103–112. https://doi.org/10.1016/S0957-4174(02)00030-1
4. Coussement K., &Van den Poel D., (2008) Churn prediction in subscription services: An application of support vector machines while comparing two parameter-selection techniques. *Expert systems with applications* 34(1):313–327. https://doi.org/10.1016/j.eswa.2006.09.038
5. Keramati, A., Ghaneei, H. & Mirmohammadi, S.M. Developing a prediction model for customer churn from electronic banking services using data mining. Financ Innov 2, 10 (2016). https://doi.org/10.1186/s40854-016-0029-6
6. . Renjith S. (2017). B2C E-commerce customer churn management: churn detection using support vector machine and personalized retention using hybrid recommendations. International Journal of Future Revolution Computer Science and Communication Engineering. 2017; 3:34–9. DOI:10.6084/M9.FIGSHARE.5579482
7. Figalist I., Elsner C., Bosch J., Olsson H.H. (2019). Customer Churn Prediction in B2B Contexts. In: Hyrynsalmi S., Suoranta M., Nguyen-Duc A., Tyrväinen P., Abrahamsson P. (eds) Software Business. ICSOB 2019. Lecture Notes in Business Information Processing, vol 370. Springer, Cham. https://doi.org/10.1007/978-3-030-33742-1_30
8. Tamaddoni A, Stakhovych S., & Ewing M.., (2017). The impact of personalized incentives on the profitability of customer retention campaigns. *Journal of Marketing Management* ;33(6), :327–47. https://doi.org/10.1080/0267257x.2017.1295094.
9. Rodpysh KV. (2012). Model to predict the behaviour of customers churn at the industry. *International Journal of Computer Applications*.49(15). 12-16. https://doi. org/10.5120/7702-1059.
10. Amin A, Anwar S, Adnan A, Nawaz M, Alawf K, Hussain A, & Huang K(2017). Customer churn prediction in the telecommunication sector using a rough set approach. *Neurocomputing*.;237:242–54. https://doi.org/10.1016/j. neucom.2016.12.009
11. Keramati, A., Ghaneei, H. & Mirmohammadi, S.M. (2016). Developing a prediction model for customer churn from electronic banking services using data mining. *Financial Innovovation*. 2, 10. .https://doi.org/10.1186/s40854-016-0029-6
12. Ballings, M., & Van den Poel, D.(2016). Customer event history for churn prediction: how long is long enough? *Expert Syst. Appl.* 39(18), 13517–13522. https://doi.org/10.1016/j.eswa.2012.07.006
13. Xie, Y., Li, X., Ngai, E.W.T., & Ying, W.,(2009). Customer churn prediction using improved balanced random forests. *Expert Systems with. Applications*. 36(3), 5445–5449. https://doi.org/10.1016/j.eswa.2008.06.121
14. Popović, D., & Bašić, B.D., (2009). Churn prediction model in retail banking using fuzzy C-means algorithm. *Informatica* 33(2).
15. C. Chu, G. Xu, J. Brownlow & B. Fu,(2016). "Deployment of churn prediction model in financial services industry," *2016 International Conference on Behavioral, Economic and Socio-cultural Computing (BESC)*. pp. 1-2, doi: 10.1109/BESC.2016.7804486.
16. Qureshii SA, Rehman AS, Qamar AM, Kamal A, & Rehman (2-13).A. *Telecommunication subscribers' churn prediction model using machine learning. In: Eighth international conference on digital information management*. 2013. p. 131–6.
17. Sakthikumar, S. (2013). An adaptive customer churn prediction method using fuzzy multi-criteria classification approach for decision. *Asian Journal of Science and Technology*. 4(11), pp. 227-233
18. Melike G, & Tolga, T., (2018) . Predictive churn analysis with machine learning methods, 26*th Signal Processing and Communications Applications Conference*, pp. 1-4.doi: 10.1109/SIU.2018.8404467
19. P. Jędrzejowicz et al. (Eds.): KES-AMSTA 2010, Part II, LNAI 6071, pp. 130–139, 2010. © Springer-Verlag Berlin Heidelberg 2010
20. i W, Cai M, Liu M, L& i G (2016) A big data clustering algorithm for mitigating the risk of customer churn. IEEE Trans Ind Inf 12(3):1270–1281
21. El-Ghazali T.,(2009). *Metaheuristics from Design to Implementation*, John Wiley & Sons, Hoboken, New Jersey.
22. Behara RS, Fisher WW & Lemmink JG (2002) *Modelling and evaluating service quality measurement using neural networks*. International Journal of Operatonal & Production Management 22(10):1162–1185
23. Yu, R., *et al.* (2018). Particle classification optimization-based BP network for telecommunication customer churn prediction. *Neural Computing & Applications.* **29,** 707–720. https://doi.org/10.1007/s00521-016-2477-3
24. Xiao et al. (2015). Feature-selection-based dynamic transfer ensemble model for customer churn prediction. *Knowledge and Information Systems* . 43(1), 29–51. DOI:10.1007/s10115-013-0722-y
25. Vijaya J. & Sivanskar E. (2018). Computing efficient features using rough set theory combined with ensemble classification techniques to improve the customer churn prediction in telecommunication sector. *Computing* . 100, 839–860 (2018). https://doi.org/10.1007/s00607-018-0633-6
26. Vijaya J. & Sivanskar E. (2019). An efficient system for customer churn prediction through particle swarm optimization-based feature selection model with simulated annealing. *Cluster Computing* 22(1), 10757–10768 . https://doi.org/10.1007/s10586-017-1172-1
27. Rajamohamed R. & Manokaram J.,(2018). Improved credit card churn prediction based on rough clustering and supervised learning techniques. *Cluster Computing* 21, 65–77. https://doi.org/10.1007/s10586-017-0933-1
28. Lalwani, P. *et al.* (2021).Customer churn prediction system: a machine learning approach. *Computing*. https://doi.org/10.1007/s00607-021-00908-y
29. Brandusoiu I, Toderean G, & Ha B.(2016). Methods for churn prediction in the prepaid mobile telecommunications industry. *International conference on communications*. 97–100. DOI:10.1109/ICComm.2016.7528311

30. Bahnsen, A.C., Aouada, D. & Ottersten, B. (2015).A novel cost-sensitive framework for customer churn *predictive modeling. Decisions. Analyisis.* **2,** 5 . https://doi.org/10.1186/s40165-015-0014-6

31. He Y, He Z, & Zhang D.(2009). A study on prediction of customer churn in fxed communication network based on data mining. In: *Sixth international conference on fuzzy systems and knowledge discovery,* 1. 92–4.

32. Idris A, Khan A, & Lee YS. (2012). Genetic programming and adaboosting based churn prediction for telecom. In: *IEEE international conference on systems, man, and cybernetics*. 1328.

33. Huang F, Zhu M, Yuan K, & Deng EO (2015). Telco churn prediction with big data. *In: ACM SIGMOD international conference on management of data.* .607–18.

34. Makhtar M, Nafs S, Mohamed M, Awang M, Rahman M, & Deris M. (2017). Churn classification model for local telecommunication company based on rough set theory. Journal of Fundamental Applications of Science. 9(6):854–68. DOI: 10.1007/978-981-15-9689-6_37

35. Amin A, Anwar S, Adnan A, Nawaz M, Howard N, Qadir J, Hawalah A, & Hussain A.(2016). Comparing oversampling techniques to handle the class imbalance problem: a customer churn prediction case study. *IEEE Access*. 4:7940–57.

36. Chawla N. (2005). Data mining for imbalanced datasets: an overview. *In: Data mining and knowledge discovery handbook.* Berlin: Springer; 853–67.

37. Verhoeven, J.D. *Fundamentals of Physical Metallurgy*, Wiley, New York, 1975, p. 326

38. Alfredo V, Angela N, & David L. Garcia. (2021). *Customer churn prediction system: a machine learning approach.* Journal of Knowledge Information Systems. DOI: https://doi.org/10.1007/s00607-021-00908-y.

39. W. Verbeke, K. Dejaeger, D. Martens, J. Hur, & B. Baesens.(2012). *New insights into churn prediction in the telecommunication sector: a profit driven data mining approach* European Journal of Operations Research, 218 (1) (2012), pp. 211-229, DOI : 10.1016/j.ejor.2011.09.031

40. K. Coussement, S. Lessmann, G. Verstraeten(2017). *A comparative analysis of data preparation algorithms for customer churn prediction: a case study in the telecommunication industry*. Journal of Decision Support System, 95 (1), pp. 27-36, DOI: 10.1016/j.dss.2016.11.007

41. Menggang L. and Lang W. (2018). *Applying the CG-logistic Regression Method to Predict the Customer Churn Problem.*IEEE. 978-1-5386-6968-6/18.

42. Park, S.-H.; Kim, M.-Y.; Kim, Y.-J. & Park, Y.-H. (2022) *A Deep Learning Approach to Analyse Airline Customer Propensities: The Case of South Korea*. Appl. Sci. https://doi.org/10.3390/ app12041916.

43. Surovitskikh S, Lubbe B (2008) *Positioning of selected Middle Eastern airlines in the South African business and leisure travel environment.* Air Transport Res Rec Manage 14: 75-81.

44. Gourdin KN (1988) *Bringing quality back to commercial travel.* Transport J 27: 23–29.

45. Gilbert D, Wong R (2003) *Passenger expectations and airline services: a Hong Kong based study.* Tourism Management. 24: 519-532.

46. Pakdil F, Aydin O (2007) *Expectations and perceptions in airline services: an analysis using weighted SERVQUAL scores.* Air Transport Res Rec Manage 13: 229–237.

47. Chang Y, Yeh C (2002) A survey analysis of service quality for domestic airlines. Eur J Oper Res 139: 166-177.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 30 – 34, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1004

Design and Implementation of Technology-Assisted Review of Legal Documents With Deep Learning

Nnaemeka .C Onyemelukwe
Department Computer Science
Chukwuemeka Odumegwu Ojukwu University
Anambra State, Nigeria

Ogochukwu C Okeke
Department Computer Science
Chukwuemeka Odumegwu Ojukwu University
Anambra State, Nigeria

Abstract: The research emphasizes the unexplored domain of utilizing artificial intelligence (AI) within the realm of Nigerian law. This is evident through the limited exploration and comprehensibility of AI's influence on legal procedures in the country. Consequently, there is a research gap regarding the effective integration of AI and machine learning (ML)-based systems, such as AILA, into Nigerian legal practices. This integration is crucial for fostering fairness, accountability, improved dynamic contract interpretation, and the appropriate proper integration of standards in digital modalities, which is lacking in the current system. The researcher designed two complementary approaches for legal document retrieval by introducing a Hybrid Model that incorporates semantic as well as implied word-order information

Keywords: Machine Learning, AILA, Hybrid Model and Legal Document

1. INTRODUCTION

In legal systems, discovery is a practice which administrates the right to attain and also has the responsibility to generate any non-relevant matter, relevant to the other party's defences and claims. eDiscovery tools have helped in enhancing the data collection method and helps in reducing the effort, in terms of reviewing the data. Since the process related to reviewing the documents can be tedious, the legal analytics process is employed by practitioners as it helps in making decisions and assisting legal leaders. Legal analytics consists of legal strategy, financial operations, resource management, and eDiscovery efficiency [1].

Therefore, legal analytics tools assist lawyers in making data-driven decisions, which helps build several legal strategies. One of the legal analytical tools- eDiscovery helps review the data which has been collected and loaded into the storage platform. However, reviewing huge data can be a tedious, time-consuming process and requires lots of costs. Hence accuracy and speed, while reviewing the data can be increased by employing leveraging technology. Therefore EDRM suggested TAR (technology-assisted review) which is considered as a significant tool in eDiscovery. TAR is also known as predictive coding. TAR refers to the document review technique, which influences algorithms to detect and tag documents based on certain keywords and metadata [2].

Due to the requirement of huge labelled datasets and also skilled annotators, several domains are still untouched by deep learning. CUAD (Contract Understanding Atticus Dataset) is a dataset used for legal contract review. Many skilled experts from 'The Atticus Project' are involved in the creation of the CUAD dataset which also comprises 13,000 annotations [3].

The pre-processing stage consists of Word2Vec, which was developed by Google in 2013 and helps to process the text data. Word2vec algorithm is made up of 2 learning models such as skip grams and a common bag of word bag [4] Using CBOW, the word can be predicted based on its context and skip-gram is employed to predict the context word for the specific target word. In general, skip-gram is considered to be the reverse of the CBOW algorithm. since the target word is considered to be the input and the context word is the output [5].

Name Entity Recognition (NER) plays the most significant role. NER helps understand the structure of the text data and helps find the relationship between entities [6]. It has been revealed that only 241 documents in the Indonesia dataset have been performed NER, whereas the necessity to implement named entity recognition with the Indonesia dataset is still ongoing since NER provides various advantages such as enhancing the accuracy [7].

There are lots of traditional methods that lack handling large corpus of documents and are a bit time-consuming which is satisfied by the method which involves Word2vec and NER. The pre-processing method is carried out rapidly with enhanced quality in retrieving the information in the dataset.

The objective of the Technology-assisted review is to speed up the process of document reviewing. It can be used in legal documents medical articles etc. It can be accomplished by repeatedly integrating the ML (ML) algorithm and feedback from humans regarding the relevance of the document. However different types of algorithms are used in demonstrating higher performance when compared to the rest of the existing approaches, which helps in detecting and identifying the relevant documents. The suggested study employed a method along with the continuous Active Learning (CAL) algorithm as it is considered to be a non-iterative approach. CALemployed AI, which helped in retrieving the most relevant information present in the document. However, there are some of the challenges faced by the suggested study such as time to terminate the document which is presented to the reviewers, lack of transparency and also lack of efficiency additional costs have to be paid to assess the total number of relevant documents. From the experimental results, it has been identified that the approach, helps in retrieving the relevant documents effectively and also delivers precise obvious and effective stropping points [8].

Due to various advantages of Technology-assisted review, civil litigants in the US (United States) heavily depend on TAR since civil discovery is a process in which the lawsuit can attain evidence from another party. The main objective of civil discovery is to support specific party estimations, claims and defences, which helps litigants to decide, whether to settle a case or not based on the availability of the evidence. And supervised ML framework has been employed by technology-assisted review for the implementation of TAR. In the supervised ML framework, the algorithms understand how to differentiate between Non-responsive documents and responsive documents based on the two criteria, which is the presence or absence of a combination of aspects which includes punctuation, phrases, words, metadata and conceptual clusters.

However, the problems arise over time due to various factors, which include the requirement of the high cost to respond to the score of requests, timely and accurately. The traditional approach was a time-consuming and laborious process, which required a sustainable amount of money and time for investment. The cost of the review does not depend not only on the documents to be reviewed but also on the time taken by the attorney to review several categories of data. Hence the suggested study employs normalizing the data in the pre-processing stage which helps in reducing the time to review the document [9].

Even though some of the studies suggest using ML algorithms to differentiate the relevant documents from non-relevant documents based on training examples. It is coded as non-relevant and relevant by the experts, the suggested study employed systematic rules that help the experts in the decision-making process. Hence technology technology-assisted review process incorporates sampling techniques or even statistical models to conduct the process and also helps in measuring the overall effectiveness of the system [10].

Even though there are modern approaches to classifying documents based on input given by the expert reviewers, there were traditional approaches employed for document classification which include Boolean search, keyword search, manual review etc. On the other hand, modern approaches that employ ML for the classification of documents are denoted as predictive coding in the legal profession. However, it was demonstrated that modern approaches help in providing high recall and precision rate with the involvement of less labour and less time-consuming process in connection with the number of documents a human has to review[11]. Apple and Samsung gathered and handled around 3.59GB of data which is around 11,108,653 documents, which the processing cost was estimated at around 13$ million dollars for 20 month period since the clash for the market share is high due to the availability of highly enhanced techniques for classification of relevant document as quickly as possible.

Several documents to be reviewed in the HRR project can be minimized by employing the TAR process (Technology-assisted review). One of the commonly used workflows for review prioritization is pool-based active learning and iterative-based active learning. Some of the common approaches implemented in supervised learning methods for lexical features and metadata features are linear models which include LR (logistic regression) and SVM (Support Vector Machine). Even the suggested study demonstrated that linear models such as LR and SVM outperformed BERT in legal discovery topics (Jeb Bush email collection) [12].

Employing ML methods for document review has become one of the common practices to reduce time and cost in e-discovery, which is known as TAR. Even though the deep learning algorithm and other conventional ML algorithms have been employed for several tasks such as clustering the documents and text classifications, there is no particular application that deals with sounds, images and video files in documents for document reviewing. Hence, the suggested study employs image classification to identify the images in the legal document and review them. The process of classification images involved, the downloading of the images from the Google image in which the images are classified as positive samples and negative samples. The positive samples consisted of images from the text documents and the negative sample consisted of people, landscapes etc. 20000 images were employed and it was split between 50/50 and the accuracy rate is considered to be above 97.9%. The highest accuracy is obtained due to the ability of VGG16 to capture the critical features that differentiate the images present in the document from other types of images[13].

Classifying thousands of documents can be a tedious process, however suggested study revealed that employing Natural Language Processing (NLP) and ML Technologies (MLT) provided lots of scope for Technology Assisted Review (TAR). Even though human instruction is required to perform the technology-assisted review, including the creation of seed sets and conducting reviews it is still considered a vital part of e-discovery[14].

A semantic type of taxonomy has been suggested in the German civil law domain which consists of 9 diverse types of functional aspects which include permissions, prohibitions duties etc. A rule-based approach has been performed to classify the legal norms by employing a manually labelled dataset. The F1 score was improved constantly from 0.519 to 0.779, however ML approach for classification of documents was implemented and the performance of the F1 score obtained was 0.83. Even though the performance of the ML is higher than other methods, ML classifiers lack transparency in terms of the decision-making process. Hence to examine the behaviour of the classifiers, local linear approximation techniques were implemented [15].

It has been mentioned that, unlike the Western courts, public records of Indian courts are messy, unstructured, chaotic and disorganized. Therefore, big-scale annotated datasets of Indian legal documents do not exist publicly to date. Due to the unavailability of the datasets, room for legal analytical research was restricted. Hence the suggested study employed a dataset which consisted of 10,000 judgements which were delivered by the Supreme Court of India along with the handwritten summaries. The dataset employed was pre-processed by implementing the normalisation technique, which normalized legal abbreviations, and variations in spelling in named entities, handled bad punctuations and tokenization precise sentences. Several attributes such as the names of the defendants, plaintiffs and also names of the people representing them, the name of the judge who gave the judgement and several other attributes were mentioned in the annotated datasets. Apart from this, an automatic labelling approach was implemented in the study to find the sentences which consist of ‘summary-worthy’ information. Some of the applications of the suggested dataset, other than the summarization of legal documents were retrieval of the legal document, analysis of the citations and decisions can also be predicted by the judge who deliver judgement. From the experimental results, it was revealed that the suggested supervised technique outperformed the strong baseline methods [16].

In general, a law practitioner has to go through lots of lengthy documents of several categories, which include legal documents, corruption-related documents, civil-related documents etc., therefore it is vital to summarize the documents and summarized documents should comprise the phrases with intent equal the classification of the case. Hence the suggested study employed a summarization technique, i.e., an intent-based summarization technique called ‘intent metric’, which provided better results along with human valuation when compared to other existing metrics such as ROUGE-L and finally a dataset (Australia data) was curated and annotated the intent phrases in the legal documents [17].

2. PROBLEM STATEMENT

In general, the text utilizes a huge portion of the legal document. Legal documents consist of factors such as contracts, dates, legislative acts, treaties and many more. Legal academia and legal practice spent centuries identifying, analysing, reviewing, commenting reacting and explaining various legal documents.

However, it is practically not feasible to review thousands of documents and find similar document text or name based on category efficiently. Hence, to predict a similar document text or name, effective data pre-processing along with Named Entity Recognition (NER) has to be performed, which can remove the punctuation mark, normalize the word and convert the cases from lowercase to uppercase and vice-versa. Therefore an effective data pre-processing step should be implemented

3. AIM AND OBJECTIVES

The main purpose of the study is to identify the entity of the document using the Named Entity Recognition model. A word embedding algorithm called Word2Vec is used in the study during the data pre-processing stage since it is efficient and works much faster than other existing methods.

To predict a similar document text or name based on the category in the legal documents.

To identify the entity of the legal document using the Named Entity Recognition model.

To evaluate the performance of the model using the cos similarity.

4. RESEARCH GAP

The suggested study is not designed to deal with reviewing a large-scale collection, which is a collection containing millions of documents as it was employed for a small-scale collection of documents since the calculation of variance of R and calculation of mean is feasible. However, splitting the existing documents, running the suggested algorithm and finally concatenating the documents for final review is done. Yet the above-mentioned approach was not considered to be the best, hence more work such as sampling of several non-relevant documents has to be avoided and it can be refrained by providing training to the ranking model universally [8].

As a part of future work, the suggested study will employ various sampling strategies which are specially depicted for neural models which include DAL (Discriminative Active Learning). A document may contain more than 512 tokens, however, the present study lacks in handling those documents, hence in future, a widespread approach will be employed to handle documents which contain more than a certain number of tokens. Since many eDiscovery tasks work upon emails, a transformer model with huge email quantities will benefit, however, the carrying of biases by pre-training quantities into concluding retrieval results in technology-assisted review will be done as future research[12].

.

5. MODELS AND METHODS

Hybrid Model that incorporates semantic as well as implied word order information.

Load the **CUAD Dataset**.

Pre-processing and tokenize the data.

In feature extraction, a series of words or sentences are contained within the numeric vector.

Using Skip Gram model word embedding, we can represent a similar sentence in numbers in a variety of ways. Proposed a new approach that search engines might utilise to locate better-matched contents of documents being retrieved. The suggested method adds a new cosine similarity-based modification

.

5.1 Improved Latent semantic

Is a method of analysing a set of documents to discover statistical co-occurrences of words that appear together which then give insights into the topics of those words and documents. In Improved Latent semantic indexing Modified truncated singular value decomposition (SVD) to identify patterns in the relationships between the terms and concepts contained in an unstructured collection of text. To consider the most important values were taken into consideration, starting from the first singular values up to the desired value. Here we modified Truncated SVD by regularizing the parameters, it will overcome the unwanted character that intrinsically gives the Transformed data that may be difficult to understand and represent our original data set with a much smaller data set. This gives the cosine similarity matrix generating the enhanced feature vectors with optimal performances

To make it easier to extract generic entities (like agreement date, location, or organisation) from natural language texts of domains without generic named entities labelled domain data sets, we use the NER model.

In flow 2 a sample input query text will be given using the “correct match25” model the relevant text will be retrieved.

CUAD Dataset

In the Contract Understanding Atticus Dataset (CUAD), there exist 13,000+ labels included with the legal contracts of 510 that come under the commercial category. The labels and the contracts are being labelled with the supervision of skilled and experienced lawyers. The process of finding the labels involves figuring out the 41 clauses which comprise in the contact review that are found to be significant which consist of transaction corporate which has a connection, acquisitions and mergers. The Atticus project is the one that maintains and organizes the CUAD to enhance the research that deals with the NLP models and to improve the review of the legal contracts.

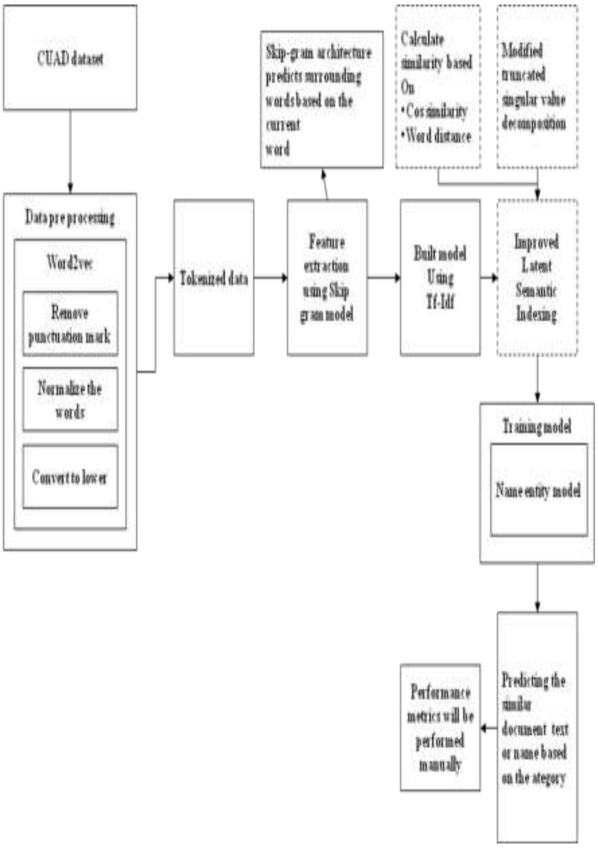

CUAD dataset
Data pre processing
Word2vec
Remove punctuation mark
Normalize the words
Convert to lower
Tokenized data
Feature extraction using Skip gram model
Skip-gram architecture predicts surrounding words based on the current word
Calculate similarity based On
•Cos similarity
•Word distance
Modified truncated singular value decomposition
Built model Using Tf-Idf
Improved Latent Semantic Indexing
Training model
Name entity model
Predicting the similar document text or name based on the ategory
Performance metrics will be performed manually

Figure. 1 Model flow diagram

Figure 1 depicts the overall performance of the method. The CUAD dataset is given as the input, the pre-processing is done by using the Word2vec algorithm. The punctuation marks are removed, the words are normalized and it is converted into the lower case. Feature extraction is performed by using the skip-gram model of the Word2vec. The model is built using the Tf-Idf method. The sentences are embedded based on the cosine similarity and the distance between the words. Semantic similarity is found using this method. For the training process, NER is used to identify the specific texts in the documents or to figure out the entities in the legal documents. The information is being retrieved based on the input. A similar text is being retrieved that depends upon the name in the document

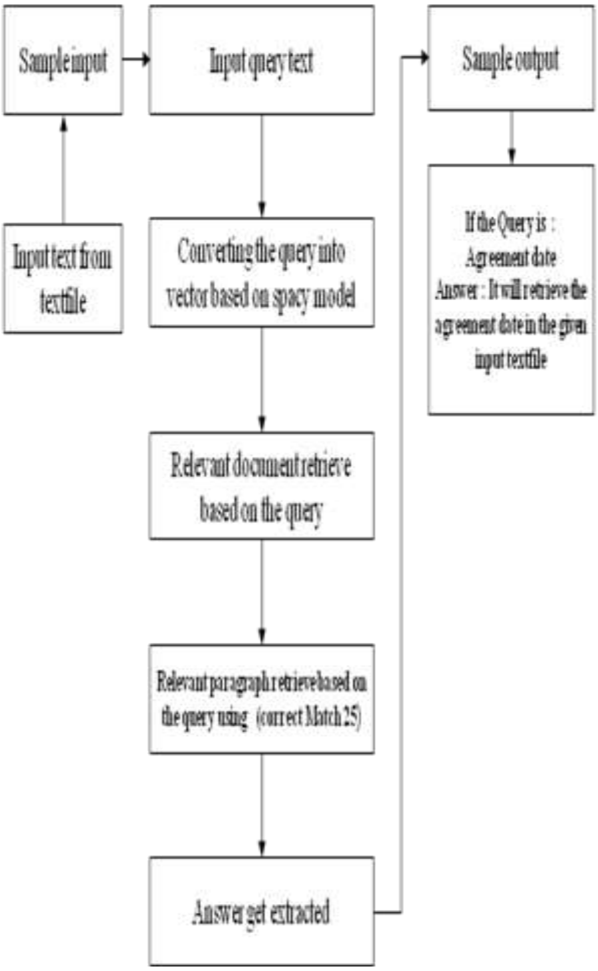

Sample input
Input query text
Sample output
Input text from textfile
Converting the query into vector based on spacy model
If the Query is :
Agreement date
Answer : It will retrieve the agreement date in the given input textfile
Relevant document retrieve based on the query
Relevant paragraph retrieve based on the query using (correct Match 25)
Answer get extracted

Figure 2 Flow of methodology (Agreement Date)

Figure 2 explains that the text file is given as the input. The text is converted into a vector based on the space model. The information is retrieved regarding the input that was given. The relevant paragraph is received by using the correct match 25. In this flow, information to retrieve the agreement date is given as the input. The Agreement is extracted as the output in the specific documents.

6. IMPLEMENTATION DESIGN

The environmental configuration of the system is tabulated in Table 1

Table .1 Environmental Configurations

Hardware Configuration	Software Configuration
CPU - Intel Core i7 – 7700 @ 2.80 GHz	Windows 10
GTX 1050	Python 3.7
16GB RAM	Anaconda Spyder

7. FINDINGS

Technology-Assisted Review (TAR) which indulges in reviewing legal documents is mainly processed for the retrieval of specific information that is very significant. The cost and the time are reduced by using the technologies for reviewing the legal documents. This increases the effectiveness of the large set of collections. The TAR is utilized in a wide range of applications to discover the information in legal documents, and literature review in the field of medicine, for organizing the collection of the evaluation.

The method of TAR outperforms the varying technologies that are used in detecting the information in legal documents that are ubiquitous. The CUAD dataset is taken and Word2vec a word-embedding algorithm is used for pre-processing the text in the legal documents as well as the skip-gram models support to figure out the similar sentences in the documents. The Tf-Idf model figures out the cosine similarity and the distance between the words in the documents. The NER, which is the form of the NLP model, is used to identify the entities in the text file that are given as input to it. A similar text is being found by these two pre-processing methods in this study.

8. CONCLUSION

The study explains employing the NER Model to detect similar document text or name based on the category. The entity of the legal document can be identified using the NER Model and the performance of the model using the cos similarity. The dataset implemented in the study is CUAD (contract understanding Atticus dataset) as it contains more than 12,999+ labels in 510 commercial legal contracts. Word2Vec and NER Model algorithms are used in the data pre-processing stage for an effective pre-processing process to detect similar text in the legal documents based on the names of the category and detecting the agreement date from the input text file which is expected to be the outcome.

9. ACKNOWLEDGMENTS

I wish to show my profound gratitude to Almighty God who gave me the insight and grace to carry out this thesis work notwithstanding the pressure at my place of work. To my Head of the Department Prof. Mgbeafulike and Post Graduate Coordinator Prof. Okeke O.C thank you for your guidance

I want to also thank my wife Mrs. Onyemelukwe Lilian Chigozie for her love and prayers my father for his financial support, and also my sibling and mother-in-law for their remarkable support during this research work.

.

10. REFERENCES

[1] A. Mullick, A. Nandy, M. N. Kapadnis, S. Patnaik, R. Raghav, and R. Kar, "An evaluation framework for legal document summarization,"*arXiv preprint arXiv:2205.08478,* 2022.

[2] B. Jang, I. Kim, and J. W. Kim, "Word2vec convolutional neural networks for classification of news articles and tweets, "*PloS one,* vol. 14, p. e0220976, 2019.

[3] B. Waltl, G. Bonczek, E. Scepankova, and F. Matthes, "Semantic types of legal norms in German laws: classification and analysis using local linear explanations, "*Artificial Intelligence and Law,* vol. 27, pp. 43-71, 2019.

[4] C. S. Patrons, "DISCOVERY PROPORTIONALITY MODEL A NEW FRAMEWORK," 2021

[5] D. Dayma, "Law Centre, Faculty of Law, University of Delhi, India, "*Cyber Crime, Regulation and Security: Contemporary Issues and Challenges,* p. 91, 2022

[6] D. Hendrycks, C. Burns, A. Chen, and S. Ball, "Cuad: An expert-annotated nlp dataset for legal contract review,"*arXiv preprint arXiv:2103.06268,* 2021.

[7] D. Li and E. Kanoulas, "When to stop reviewing in technology-assisted reviews: Sampling from an adaptive distribution to estimate residual relevant documents, "*ACM Transactions on Information Systems (TOIS),* vol. 38, pp. 1-36, 2020.

[8] E. Yang, S. MacAvaney, D. D. Lewis, and O. Frieder, "Goldilocks: Just-Right Tuning of BERT for Technology-Assisted Review,"*arXiv e-prints,* p. arXiv: 2105.01044, 2021.

[9] I. Budi and R. R. Suryono, "Application of named entity recognition method for Indonesian datasets: a review, "*Bulletin of Electrical Engineering and Informatics,* vol. 12, pp. 969-978, 2023.

[10] J. Cheng, J. Liu, X. Xu, D. Xia, L. Liu, and V. S. Sheng, "A review of Chinese named entity recognition, "*KSII Transactions on Internet & Information Systems,* vol. 15, 2021.

[11] M. Abdolahi and M. Zahedi, "A new method for sentence vector normalization using word2vec," *International Journal of Nonlinear Analysis and Applications,* vol. 10, pp. 87-96, 2019.

[12] N. Huber-Fliflet, F. Wei, H. Zhao, H. Qin, S. Ye, and A. Tsang, "Image Analytics for Legal Document Review: A Transfer Learning Approach,"*arXiv e-prints,* p. arXiv: 1912.12169, 2019.

[13] P. W. Grimm, M. R. Grossman, and G. V. Cormack, "Artificial intelligence as evidence, "*Nw. J. Tech. & Intell. Prop.,* vol. 19, p. 9, 2021.

[14] R. Dale, "Law and word order: NLP in legal tech, "*Natural Language Engineering,* vol. 25, pp. 211-217, 2019.

[15] R. Wang, "Legal technology in the contemporary USA and China," 2020.

[16] S. Krishnan, N. Shashidhar, C. Varol, and A. R. Islam, "Evidence Data Preprocessing for Forensic and Legal Analytics, "*Int. J. Comput. Linguist. (IJCL),* vol. 12, p. 24, 2021.

[17] V. Parikh, V. Mathur, P. Mehta, N. Mittal, and P. Majumder, "Lawsum: A weakly-supervised approach for Indian legal document summarization,"*arXiv preprint arXiv:2110.01188,* 2021.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 35 – 38, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1005

Database Security: Navigating Threat Landscapes and Defense Mechanisms

Aliyu Umar
Department of Information Technology
Taraba State University
Jalingo Taraba State, Nigeria

Yahaya Saidu
Department of Computer Sciences
Taraba State University
Jalingo Taraba State, Nigeria

Tirmizi Mohammed
Department of Computer Science
Taraba State University
Jalingo Taraba State, Nigeria

Ahmed Musa Iliyasu
Department of Computer Sciences
Taraba State University
Jalingo Taraba State, Nigeria

Abstract: In today's interconnected world, databases serve as the backbone of virtually every organization, handling vast amounts of sensitive information. However, with this reliance comes a host of security threats that can jeopardize the integrity and confidentiality of data. This paper presents a comprehensive review of ten prominent threats to databases, ranging from SQL injection attacks to insider threats and data breaches. Each threat is analyzed in detail, highlighting its potential impact and offering effective solutions for mitigating risks. By understanding these threats and implementing robust security measures, organizations can safeguard their databases against malicious actors and ensure the continued integrity and availability of their data assets.

Keywords: Database security; Threats; Solutions; Defense mechanisms; Denial of Service (DoS) attack

1. INTRODUCTION

Databases are integral to daily activities, whether in government, private, or individual use, as they store sensitive information. A database comprises related records, and each record contains related fields. There are two main types of databases: manual-based systems, also known as traditional databases, and computerized database systems. Traditional databases, often found in offices, store records in files kept in cabinets. Computerized or modern database systems can be further categorized into flat databases and relational databases. Flat databases store records in a single table, while relational databases store records in multiple tables with relationships between them. Relational databases are widely preferred due to advantages such as reducing redundancy. The Database Management System (DBMS) is the program responsible for managing and monitoring access to the database, allowing authorized individuals to access it. Finally, the Database Administrator controls access, ensuring that only authorized users access the database.

3. THREATS OF DATABASE

SQL injection attacks occur when attackers insert unwanted or malicious database statements into Structured Query Language (SQL) queries, exploiting vulnerabilities in the system to access sensitive information from the database. Here are the sources of SQL injection attacks: Web forms: Attackers can insert malicious SQL statements into web forms, which are graphical user interfaces (GUIs) used by authorized users to access information or data. These web forms contain detailed information needed by authorized users, such as employee identification numbers, names, salary grades, addresses, departments, and more. Attackers exploit vulnerabilities in web forms by injecting malicious SQL statements to gain access to sensitive information. Server variables: SQL injection can also be inserted into server variables, which are used to retrieve server-related information, such as AUH-TYPE used for user authentication or validation. Attackers inject server variables to access authorized users' passwords and usernames, enabling them to perform malicious activities [5]

Operating system vulnerabilities pose significant risks to the security of databases, including popular systems like Linux and Windows, as well as associated services linked to databases. Exploiting vulnerabilities in the operating system can lead to unauthorized access to the database. For instance, an attacker could exploit vulnerabilities to launch a Denial of Service (DoS) attack. By flooding the network with excessive traffic, legitimate users may be unable to access the database, effectively denying them service. This creates an opportunity for the attacker to gain unauthorized entry into the organizational database while the legitimate users are unable to connect. [5].

Privilege abuse occurs when a legitimate database user, who is authorized, misuses their privileges to carry out unwanted or unlawful activities within the database. For instance, an authorized user with access rights to view and edit employee records might abuse this privilege by increasing an employee's salary without proper authorization. Such actions can be detrimental to an organization. [6]

Excessive privilege abuse occurs when authorized users are granted database privileges that surpass their legitimate needs. This grants them access to sensitive data or functionalities they shouldn't have, which could be exploited for unlawful or malicious purposes. For instance, consider an authorized user with access to view employee details in a Human Resource Management System database. If this user is granted privileges beyond what is necessary—such as access to salary information or employee performance records—they may abuse this excess privilege. This could involve unauthorized viewing, manipulation, or dissemination of sensitive data, compromising the confidentiality and integrity of the system [5] [2]

Administrative abuse refers to situations where a database administrator misuses their authority to carry out malicious activities within the database. For instance, an administrator might change employee records, such as their salary or grade level, for personal gain or other malicious purposes. This abuse of privilege can have significant consequences within an organization's database system [7]

Denial of Service (DoS) attacks can be launched by attackers to disrupt the functionality of a system or network, particularly targeting the organization's network. This can be achieved through various means such as generating excessive traffic, causing data corruption, flooding the network, or enforcing heavy traffic on the organizational network. The objective is to prevent authorized users from accessing the database [2]

Following a successful DoS attack, the attacker may proceed to carry out unlawful activities on the database. For instance, if the attacker aims to access financial transactions to steal money, they might crash the server to deny access to authorized users and then proceed to steal money from the database. Such actions result in significant losses for organizations that rely on database systems to store important or sensitive information [2]

Privilege elevation poses a significant threat to database systems. An ordinary user within an organization could exploit vulnerabilities in the software to gain additional privileges, elevating their status from a normal user to a system administrator. Once elevated to a system administrator, they may then use their newfound privileges to carry out malicious or unlawful activities, gaining unauthorized access to important information stored in the organizational database [8]

For instance, the perpetrator of such malicious activity might manipulate financial records for an employee by increasing their salary without authorization. This issue can lead to setbacks for the organization, as it compromises the integrity and security of its database system.

Backup exposure occurs when unauthorized users gain access to database backups with the intention of obtaining vital information. This exposure can occur through connections with insiders, such as having a friend who is an authorized user within the organization. In such cases, unauthorized individuals may exploit these connections to obtain access to the database backup [2]

Additionally, authorized users or insiders themselves may also be perpetrators of database backup theft. These individuals, who have legitimate access to the database, may steal the backup for the purpose of accessing sensitive information stored within the organizational database. The theft of database backups poses a significant risk of database exposure, which can be highly detrimental to organizations relying on their database systems to safeguard sensitive information.

Weak authentication poses a serious threat to database security, as it can provide attackers with the means to identify legitimate users and gain unauthorized access to the database. Attackers may employ various methods to steal login credentials for authorized users. One method is direct credential theft, where unauthorized users obtain or steal login credentials belonging to legitimate database users. Social engineering is another technique attacker may use. In this scenario, the attacker takes advantage of being in proximity to a legitimate database user, perhaps posing as a computer engineer tasked with maintaining the organization's computers. Through this ruse, the attacker may obtain the login credentials or username and password of an authorized database user. Additionally, attackers may resort to brute force methods, systematically trying different combinations of letters and numbers to crack passwords and access sensitive information stored in the organizational database. Addressing weak authentication is crucial for safeguarding database security and protecting sensitive organizational data [10]

Weak audit trails present a significant risk to database security. Deploying a robust database audit mechanism to track all activities and transactions within the database is crucial. Failure to implement such mechanisms can lead to substantial losses for organizations [11]

For example, both insiders and outsiders could act as attackers. Without proper audit mechanisms to capture comprehensive information about both authorized and unauthorized users, including usernames, passwords, the source and location of operations, and even images of attackers, an organization remains vulnerable to various threats [9]

Failure to address this issue constitutes a serious problem for organizations, as it compromises their ability to monitor and respond effectively to security incidents.

4. SOLUTIONS TO THREATS

To prevent SQL injection attacks, implementing the following methods is advisable: Virtual Patching or Web Application Firewall (WAF): This technology is utilized to control and monitor any malicious activities targeting the database. A WAF acts as a protective barrier between the web application and the internet, filtering and blocking potentially harmful traffic, including SQL injection attempts. Green SQL: Developed by Microsoft, Green SQL is software designed to control database access by blocking SQL injection attacks. For instance, if an unwanted or attacker is detected, Green SQL captures detailed information about the attacker, such as their source internet protocol (IP) address, operating environment, and username. By deploying these methods, organizations can significantly enhance their defenses against

SQL injection attacks and mitigate the associated risks to their databases [1][5]

Operating System (OS) vulnerabilities can be mitigated through two primary methods: regular updates of the database and the implementation of intrusion prevention systems (IPS). Regular updates help prevent attacks or unauthorized access to the database by addressing any known vulnerabilities in the OS. However, continuous updates may not always be sufficient, especially in the presence of new vulnerabilities. In such cases, intrusion prevention systems become necessary. IPS monitors the application and identifies any attackers attempting to gain unlawful access to the database through network traffic. The combination of these two methods can significantly improve the organization's security posture [12]

To prevent privilege abuse in a database, implementing access control methods is essential. These methods not only control access to database queries but also manage access to the database context itself. Access control provides detailed information about legitimate database users, including their usernames, passwords, and the source of application names. By deploying access control mechanisms, organizations can effectively restrict access to sensitive data and prevent unauthorized users from abusing their privileges within the database environment.

To address the issue of excessive privilege abuse, one effective solution is the implementation of query-level access control. This control mechanism restricts database privileges to only the necessary level required for normal operations. With query-level access control in place, if an authorized user attempts to exceed their designated privileges by executing a query that accesses unauthorized data or functionality, the system triggers an alert. This alert notifies the system administrators of the attempted breach, allowing them to intervene and prevent potential malicious activities from occurring within the database. By employing query-level access control, organizations can enforce granular access permissions, ensuring that users are only granted the precise privileges required for their specific tasks. This proactive approach enhances database security and helps mitigate the risks associated with excessive privilege abuse. [7]

The solution to addressing Administrator Abuse involves implementing access control measures. These measures aim to capture detailed login information about legitimate administrators, including their username, password, system used, timestamp of access, and location. With access control in place, it becomes possible to detect any misuse of database privileges by administrators who engage in malicious activities. By implementing access control, organizations can enhance their security posture and minimize the risks associated with Administrator Abuse [13]

To prevent a Denial of Service (DoS) attack, one method is to configure the firewall to block unauthorized users or attackers from accessing sensitive information. The firewall can filter packets from attackers and block their access attempts, allowing only authorized users to access information from the database. Another approach is to disable all unnecessary or unused network services, as attackers might exploit these services to gain access to the database through the network. Implementing both methods can significantly enhance the organization's operational security. [9]
The solution to privilege elevation involves implementing both traditional intrusion prevention systems (IPS) and access control measures. The traditional IPS is designed to capture or detect any unauthorized attempts to access a database. Access control, on the other hand, is geared towards identifying any individuals attempting to use abnormal Structured Query Language (SQL) to access vital information within the database [4]

To prevent exposure of database backups, the organization needs to employ several strategies. First, encrypting sensitive information stored on backup devices is crucial. This ensures that even if attackers steal the backup device, they won't be able to access any sensitive information since it's encrypted. Secondly, implementing an audit mechanism is essential. This mechanism tracks attackers by recording their movements, and it can even capture their picture or face. This allows the organization to trace the attacker and take appropriate actions. By utilizing these methods, the organization can effectively prevent database backup exposure [2]

To mitigate unauthorized access due to weak authentication, implementing a restriction where users can only access the database from specific Internet Protocol (IP) addresses is advisable. By defining access permissions based on IP addresses, users would be restricted from accessing the database from locations outside of the defined IPs. This measure effectively prevents unwanted or unauthorized users from gaining access to the database [2]

Improving weak audit trails requires enhancing the audit mechanism to operate at higher speeds. This can be achieved by offloading audit mechanisms or appliances onto the network, which can significantly enhance an organization's capabilities. Universal user tracking software is utilized to capture comprehensive login details about users, including usernames and passwords.
Grand Transaction tracking software is an advanced tool designed to capture any unauthorized access to the database, including details such as the source operating system and hostname [6]

5. CONCLUSION

Investing in database security is crucial for organizations to safeguard their valuable information assets and uphold stakeholder trust. By implementing robust security measures, organizations can confidently protect their databases from potential threats and vulnerabilities, ensuring the integrity, confidentiality, and availability of their data. Prioritizing database security not only fortifies an organization's defenses but also enhances its overall resilience against cyber threats, thereby supporting sustained operational success and stakeholder confidence.

6. ACKNOWLEDGMENTS

We extend our heartfelt appreciation to the reviewers for their constructive comments, which have greatly enhanced the quality of this paper..

7. REFERENCES

[1] Anjaligupta, R., & Ramya, R. (2022). *Descriptive analysis on database security techniques.* International

Journal of Novel Research and Development, 7(10), 1-5. https://doi.org/10.2456/4184

[2] Teimoor, R. A. (2021). *A review of database security concepts, risks, and problems. UHD Journal of Science and Technology,* 5*(2),* 38-46.

[3] Ali, A., & Mazhar, M. (2017). *Database Security: Threats and Solutions. International Journal of Engineering Inventions,* 6*(2), 25-27*

[4] Rekha Ahirwar, Rashi Saxena, Pankaj Yadav (2016, March). Challenges to Data Base Security – A Futuristic View. IOSR Journal of Computer Engineering. Vol. 18 . issue.2 pp.01-04

[5] Shulman, A n.d, Top Ten Database Security Threats How to Mitigate the Most Significant Database Vulnerabilities. Available from:<http://www.schell.com/Top_Ten_Database_Threats.pdf>. [5 March 2016].

[6] Tejashri R. Gaikwad1, A. B. Raut2 (2014, April). A Review on Database Security. International Journal of Science and Research (IJSR) Vol.3 issue.4,pp.372-374 IEEE

[7] Top Ten Database Security Threats (2014). White Paper. Available from :< http://www.imperva.com/docs/wp_topten_database_threats.pdf>. [4 March 2016]

[8] P. K. Rai (2015, June). *An overview of different database security approaches for distributed environment*. IJISET - International Journal of Innovative Science, Engineering & Technology. Vol. 2. Issue. 6 pp. 2348 – 7968

[9] T.Gunasekhar, K.Thirupathi Rao, P.Saikiran3 and P.V.S Lakshmi(2014). *A Survey on Denial-of-Service Attacks. International* Journal of Computer Science and Information Technologies. Vol. 5 (2) 2014, 2373-2376

[10] Malik, M, & Petel,T, “ Database Security - Attacks And Control Methods” in Cmpica, Charotar University of Science & Technology (CHARUSAT), Changa. 2006 Available from:< http://charusat.net/NCSCA2016/NCSCA-2016_Conference-proceeding/>.[2 March 201 6].

[11] Singh A, Singh. P, Nath. U (2015, May). Enforcing Database Security in Un-trusted Environment by using Multisession and Biometrics based Authentication. International Journal of Emerging Research in Management &Technology. Vol.4, issue.5 pp. 207-2011

[12] Mittal, K& Rohilla, S. (2013, *May). Database Security: Threats And Challenges,* International Journal Of Advance Research In Computer Science And Software Engineering,vol.3, no.5, pp.810-813.

[13] Mou Shen, Mengdong Chen, Min Li and Lianzhong Liu(2013) . Research of Least Privilege for Database Administrators. International Journal of Database Theory and Application Vol.6, No.6 . pp.39-50

[14] Al-sayid, A. and Aldlaeen, D(2012).Database Security Threats: Survey Study. , 2013 5th International Conference on Computer Science And Information Technology (CSIT), Applied Science University, Amman, Jordan, pp.60-64. IEEE

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 39 – 41, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1006

Cybersecurity: A Case of Company and Organization Security

Asnath Nyachiro
Technical University of Mombasa
Mombasa, Kenya

Kennedy Hadullo
Technical University of Mombasa
Mombasa, Kenya

Kelvin Tole
Technical University of Mombasa
Mombasa, Kenya

Abstract: In the current digital landscape, organizations heavily rely on interconnected technologies to enhance operational efficiency, yet this dependency also exposes them to significant cybersecurity risks. Despite deploying advanced cybersecurity tools, employees remain a critical vulnerability due to their limited awareness of cybersecurity threats. Research highlights the pivotal role of employees in mitigating such risks, emphasizing the impact of human error and behavior on organizational security. This study aims to assess the level of cybersecurity awareness among employees and evaluate the effectiveness of training initiatives in enhancing organizational cybersecurity resilience. The methodology involved a comprehensive literature review, encompassing articles, journals, case studies, and books related to cybersecurity awareness, cyber threats, and employee training. Key search terms included "cybersecurity," "cyber threats," "cyberattacks," "user awareness," "cybersecurity training," and "knowledge of cybersecurity," using databases like Google Scholar, Science Direct, and Springer. The review highlighted various cybersecurity challenges faced by organizations, including internal threats from employees and external threats from hackers and malicious actors.

Keywords: cybersecurity, cyber threats, cyberattacks, user awareness, cybersecurity training and knowledge of cybersecurity.

1. INTRODUCTION

The growing reliance on digital technologies and information systems within organizations has brought about unprecedented levels of interconnectedness and efficiency. However, this technological advancement also introduces significant cybersecurity challenges, particularly related to the human element within organizations. Despite the implementation of sophisticated cybersecurity tools and protocols, employees remain a critical point of vulnerability due to their lack of awareness and understanding of cybersecurity risks. Research in the field of cybersecurity underscores the pivotal role of employees in mitigating cybersecurity threats, emphasizing that human error and behavior often pose the greatest risks to organizational security.

2. METHODOLOGY

The literature review included articles, journals, case studies, and books relating to content on user awareness of cybersecurity, cyberattacks. The terms and keywords used in the search process included cybersecurity, cyberthreats, cyberattacks, user awareness, cybersecurity training, and knowledge of cybersecurity. The databases used were Google Scholar, Science Direct, and Springer. These included conference reports, articles, and journals.

3. LITERATURE REVIEW

Data Safety According to earlier studies, information and information assets have historically been protected from potential cyberthreats and cyberattacks using a technological method (Carcary et al., 2016). It could be argued that the security of information and information assets requires the use of technical tools yet, organizations, including governments, have searched for proactive measures to safeguard data and information systems from human behaviors in response to Carcary et al. (2016)'s research. According to Antoniou (2018), merely employing technological tools to prevent human behaviors like password sharing among coworkers or viewing private information over an unsecured WiFi network is insufficient. Maynard et al. (2018) are among the other academics who have proposed that workers should also be considered a potential cybersecurity risk in addition to the technical concerns. They proposed that one of the primary contributing factors to cyberthreats that target data and information systems is an employee. According to McLane (2018), employees that are primarily regarded as the weakest link must have their information and information assets secured.

Knowledge is another element that affects information security. For instance, Kim et al. (2014) investigated the barriers to employee adherence to security protocols that may avert cyberattacks using a quantitative research methodology. They discovered that the application of preventive measures in the adoption of information security is hampered by ignorance. This is consistent with study by Alqahtani (2017), who discovered that employees think that the adoption of information security preventative measures is mostly influenced by their ability to recognize cyberthreats.

Information systems are facing more dangers and vulnerabilities as a result of the growing use of network solutions (Adebayo, 2012; Chul et al., 2016; Ferrillo & Singer, 2015). According to Ferrillo and Singer's (2015) conclusion, employees' risky activities may negatively impact information and data systems. Employee behavior decisions are strongly correlated with their perception of risk (Ahmad et al., 2019; Ferrillo & Singer, 2015). According to Dang-Pham et al. (2017), employee behavior decisions may have an impact on how information systems are managed. Hadlington (2017) provided evidence for this theory by examining the traits and attitudes of the public sector, including how these factors have affected the employees' intents toward information and cybersecurity. Furthermore, Gordon et al. (2015) and Hwang et al. (2017) looked at how employees behaved and thought about information system security challenges, and they found that workers can build moral convictions about cybersecurity.

Information security is the overarching theme and fundamental building block for the creation of any cybersecurity awareness campaign, according to Fietkiewicz et al. (2017). It is therefore the duty of all government personnel, not only managers and supervisors, to protect confidential information (Gordon et al., 2015). According to

Dykstra and Spafford (2018), research on how people affect information security is essential for developing cybersecurity solutions and equipping staff members with cybersecurity awareness training to fend off potential threats.

Information system access and identification can now be stolen or surmised thanks to the globalization of communication across information systems networks (Gabriel & Mohamed, 2011; Solari, 2012). Additionally, as the majority of cyberthreats and cyberattacks do not originate from the actual location of the attack, it has become more difficult to identify their origins due to the globalization of information systems networks (Gabriel & Mohamed, 2011). But in order to stop hackers and lessen cyberattacks, Bland et al. (2020) created an algorithm to recognize trojan methods and script comments. On the other hand, Solari (2012) supported the initial perspective by examining the elements that preceded cyberattacks and concluded that information security and information threat mitigation needed to be concentrated on identifying elements that can encourage employee behaviors that will increase cybersecurity awareness.

3.1. INTERNAL THREATS

Employees, contractors, and supervisors who have been granted access to confidential information and information systems are examples of internal dangers. Certain researchers (Ahmad et al., 2014; Glasser & Taneja, 2017) have concentrated on internal threats in which the goal was premeditated and hostile. Internal threats that fall under the heading of malicious internal threats that were planned include information theft for monetary gain and retaliation. Internal threats were recognized by Ahmad et al. (2015), along with the reasons why they are detrimental to information security. Scholars such as Harnett (2016) and Kshetri (2013) have concentrated on personnel that pose a threat internally but lack malicious intent. The organization's personnel are merely unable to oversee information security. Internal risks are those that come from within the company, according to Harnett (2016). After reviewing the literature on internal threats, Ahmad et al. 2015 came to the conclusion that the two main contributors to internal security events and significant risks to information security were employees' inappropriate behavior and a lack of cybersecurity awareness. Gabriel and Mohamed (2011) claim that by comprehending what influences employee behavior, internal dangers can be lessened or managed.

3.2 EXTERNAL THREATS

Hackers, former employees, natural calamities, and other governmental organizations are some of these threats. Threats from the outside lack access to the information systems and rights (Harnett, 2016). Stephen (2011) noted in his study on cybercrimes that the 2007 Denial of Service (DoS) assaults against Estonia were a significant example of an external cyberattack. Because it impacted every digital service in the nation over the course of 22 days. This attack was noteworthy and a milestone since every harmful traffic came from somewhere other than Estonia.

Comprehending the factors that impact users' awareness of cybersecurity is a pertinent issue for multiple reasons. First, scholarly research suggests that user knowledge of cybersecurity has a role in the overall decline in cyberattacks on information systems (Asllani et al., 2013; Ki-Aries & Faily, 2017; Knapp & Ferrante, 2012). A company misses out on a chance to avoid cyberattacks and putting information security policies and procedures in place by failing to adopt a cybersecurity awareness posture (Ki-Aries & Faily, 2017). For example, Hajli and Lin (2016) discovered that after creating information security policies, staff members were able to incorporate the policies into their regular tasks, such as sharing their computer's password with coworkers or refraining from utilizing an open WiFi network to access the organization's files.

De Bruijn and Janssen's (2017) case study was one of the research contributions that highlighted the organization's inadequate information management as a contributing element in cyberattacks, as opposed to the employees. This study also highlighted the organization's responsibility in preventing cyberattacks. They insinuated that focusing on information security management and implementing effective governance are necessary to prevent cyberattacks and breaches of data security. A thorough analysis of the literature on cybersecurity trends and potential defenses against cyberattacks was carried out by Steinbart et al. (2016). They found out that a large number of businesses had not taken the necessary precautions to protect their information systems from cyberthreats and cyberattacks, leaving gaps and backdoors open to hackers and other unauthorized users. Furthermore, Steinbart et al. recommended that companies spend money and effort training end users and developing security policies and procedures. According to Creasey (2013), this is important yet frequently disregarded due to a lack of knowledge or resources within the company.

4. ACKNOWLEDGMENTS

Our thanks to the Technical University of Mombasa.

5. REFERENCES

[1] Adebayo, A. O. (2012). A foundation for breach data analysis. Journal of Information Engineering and Applications, 2, 17-21

[2] Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25, 357-370. https://doi.org/10.1007/s10845-012-0683-0

[3] Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35, 717-723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

[4] Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. Information and Computer Security. https://doi.org/10.1108/ICS-10- 2017-0073

[5] Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. Procedia Computer Science, 124, 691-697. https://doi.org/10.1016/j.procs.2017.12.206

[6] Antoniou, G. S. (2018). A framework for the governance of information security: Can it be used in an organization. SoutheastCon, 1-30. https://doi.org/10.1109/secon.2018.8479032

[7] Asllani, A., White, C. S., and Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. Journal of Legal, Ethical and Regulatory Issues, 16(1),17-14

[8] Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine learning cyberattack and defense strategies. Computers & Security, 92. https://doi.org/10.1016/j.cose.2020.101738

[9] Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. IT Professional, 18(2), 22–30. https://doi.org/10.1109/mitp.2016.27

[10] Chul H, L., Xianjun, G., & Raghunathan, S. (2016). Mandatory standards and organizational information security. Information Systems Research, 27(1), 70-86. https://doi.org/10.1287/isre.2015.0607

[11] Creasey, J. (2013). Cybersecurity incident response guide. https://www.crestapproved.org/wpcontent/uploads/2014/11/CSIRProcurementGui de.pdf

[12] Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organization. Computers & Security, 70, 111-123. https://doi.org/10.1016/j.cose.2017.05.010

De Bruijn, H. & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34 (1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

[13] Dykstra, J., & Spafford, E. H. (2018). The case for disappearing cybersecurity. Communications of the ACM, 61(7), 40– 42. https://doi.org/10.1145/3213764

[14] Ferrillo, P., & Singer, R. (2015). Is employee awareness and training the holy grail of cybersecurity? Corporate Governance Advisor, 23(3), 10-13.

[15] Fietkiewicz, K. J., Mainka, A., & Stock, W. G. (2017). eGovernment in cities of the knowledge society. An empirical investigation of smart cities' governmental websites. Government Information Quarterly, 34(1), 75–83. https://doi.org/10.1016/j.giq.2016.08.003

[16] Gabriel, B. A., & Mohamed, A. (2011). Impact of globalization. European Business Review, 23(1), 120-132. https://doi.org/10.1108/09555341111098026

[17] Glasser, D. & Taneja, A. (2017). A routine activity theory-based framework for combating cybercrime. In Identity theft: Breakthroughs in research and practice, (pp. 69-78).

[18] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1, 3-17. https://doi.org/10.1093/cybsec/tyv011

[19] Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), 1-18. https://doi.org/10.1016/j.heliyon.2017.e00346

[20] Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), 111. https://doi.org/10.1007/s10551-014-2346-x

[21] Harnett, T. (2016). Protecting your most valuable assets crafting a cybersecurity strategy to guard against internal and external threats. Chief Learning Officer, 15(8), 26.

[22] Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. Online Information Review, 41(1), 2-18. https://doi.org/10.1108/oir-11-2015-0358

[23] Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. Computers & Security, 70, 663-674. https://doi.org/10.1016/j.cose.2017.08.001

[24] Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. The Scientific World Journal, 2014,1-12. https://doi.org/10.1155/2014/463870

[25] Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. Journal of Management Policy and Practice, 13(5), 66–80

[26] Kshetri, N. (2013). Privacy and security issues in cloud security: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386. https://doi.org/10.1016/j.telpol.2012.04.011

[27] Maynard, S. B., Tan, T., Ahmad, A., & Ruighaver, T. (2018). Towards a framework for strategic security context in information security governance. Pacific Asia Journal of the Association for Information Systems, 10(4), 65. https://doi.org/10.17705/1pais.10403

[28] McLane, P. (2018). Cyberattacks put every enterprise at risk: Techniques diversify as corporate adversaries get smarter. Multichannel News (15), 8

[29] Solari, L. (2012). Globalization will make us all more different. People and Strategy, 35(2), 30-35

[30] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. Journal of Information Systems, 30(1), 71-92. https://doi.org/10.2308/isys-51257

[31] Stephen, H. (2011). Revisiting the Estonian cyberattacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[32] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[33] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[34] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 42 – 46, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1007

Adaptive Resource Management in CI/CD Environments Using Deep Deterministic Policy Gradients

Junaid Jagalur
DevOps Expert
Independent Researcher
Jersey City, New Jersey

Abstract: This paper explores the theoretical application of reinforcement learning (RL) to dynamic resource management in Continuous Integration and Continuous Delivery (CI/CD) environments like build and test environments. Focusing on the scaling and capacity optimization of virtual machine (VM) pools, the study proposes the use of a Deep Deterministic Policy Gradient (DDPG) model, tailored for environments characterized by continuous action spaces and complex, dynamic demands. The paper delineates a theoretical framework where an RL agent dynamically adapts VM allocations based on real-time requirements, potentially enhancing operational efficiency and reducing costs. Tthe research outlines a conceptual model that leverages the capabilities of RL to address resource allocation challenges inherent to modern software development. The discussion anticipates that the integration of RL could revolutionize traditional resource management strategies by providing more agile, efficient, and cost-effective solutions. Future research directions are suggested, focusing on exploration of alternative RL algorithms for practical implementations in CI/CD environments. This work contributes to the literature by proposing a novel approach to optimizing resource management in CI/CD systems, setting a foundation for future studies and technological advancements in the field.

Keywords: Continuous Integration, Continuous Deployment, DevOps, Machine Learning, Reinforcement Learning, Automation

1. INTRODUCTION

Continuous Integration and Continuous Delivery (CI/CD) pipelines represent automated processes in software development that enable frequent and reliable code changes through automated testing and deployment methods. These pipelines are fundamental in supporting rapid development cycles and ensuring that the integration and delivery of code changes are both smooth and efficient. They primarily involve a series of steps that include compiling code, running tests, and deploying to production environments.

Resource management within CI/CD environments like build and test environments pose significant challenges, primarily due to the changing development needs and the variability in workload demands. Traditional static resource allocation strategies often lead to either underutilization of resources, which is cost-inefficient, or resource scarcity, which can delay the pipeline processes [4]. The fluctuating demands on CI/CD systems can therefore benefit from a more adaptive approach to manage computing resources effectively, particularly in environments where multiple pipelines are concurrently active. [5]

This paper aims to explore the application of reinforcement learning for dynamic resource management in CI/CD environments, focusing specifically on the scaling and capacity optimization of VM pools across multiple pipelines. The application described is conceptual and builds on a robust theoretical understanding of both the operational challenges in CI/CD systems and the capabilities of modern reinforcement learning techniques. By modeling the CI/CD environment and the application of RL, this work proposes a novel approach to resource management that could significantly enhance the efficiency and effectiveness of CI/CD pipelines. The contributions of this paper, therefore, provide a solid framework and offer substantial insights for future research and practical implementations in this area.

2. BACKGROUND

2.1 Current Practices

Current practices in resource allocation within CI/CD environments typically involve static or semi-static resource management strategies [21]. These strategies are defined by predetermined rules based on average loads and peak performance needs. For instance, organizations might provision a fixed number of virtual machines (VMs) or containers that are expected to handle the anticipated workload. This approach, while straightforward and easy to implement, often fails to account for the unpredictable variances in demand typical in software development processes, resulting in either excessive cost due to over-provisioning or delays in pipeline execution due to under-provisioning [22, 29].

2.2 Literature Review

Reinforcement learning (RL) has been used to optimize resource allocation across various technology sectors, demonstrating its effectiveness in environments with dynamic requirements. In cloud computing, RL has been extensively used to automate the scaling of computing resources, ensuring optimal resource utilization. Specific instances include algorithms that predict server load and dynamically adjust the number of active server instances. For example, Amazon Web Services uses predictive scaling in its Auto Scaling service, which employs machine learning models to schedule the right number of EC2 instances in anticipation of demand spikes. This approach optimizes cost and maintains system responsiveness without manual intervention.

Further literature review revealed that data centers benefit significantly from RL in two main areas: energy management and system stability. One notable example is Google's use of DeepMind's AI to control data center cooling systems. The RL algorithm analyzes historical data and current conditions to adjust cooling valves and fans, reducing energy consumption by up to 40% [23]. This application not only decreases operational costs but also improves the environmental footprint of data center operations. Similarly, RL has been used to optimize power allocation across servers and other hardware to maximize energy efficiency without compromising on performance.

In network management, RL contributes to smarter bandwidth allocation and latency reduction. Algorithms learn from real-time traffic data to anticipate bottlenecks and redistribute network resources accordingly. This dynamic adjustment helps in maintaining high service quality and managing network congestion effectively, especially during high-demand periods. Companies have explored RL-based models for adaptive traffic routing that respond to changing network conditions instantaneously, ensuring optimal data flow and minimizing packet loss [24].

2.3 Gaps in Current Research

Despite the advancements in applying AI to resource management, there is a noticeable gap in its application specifically within CI/CD pipeline management [1]. Most existing research focuses on the general optimization of resource allocation without tailoring approaches to the unique characteristics and challenges of CI/CD systems, such as the need for rapid scaling and the integration of various development tools and platforms [6]. This gap presents an opportunity to develop specific AI-driven strategies, particularly using reinforcement learning, to address the distinct aspects of CI/CD environments. Such strategies could lead to more responsive and cost-effective resource management solutions tailored to the needs of software development and delivery processes [28].

This paper contributes to the body of knowledge by specifically focusing on the application of reinforcement learning for dynamic scaling and capacity optimization in CI/CD environments. The proposed model leverages principles of reinforcement learning to propose optimal scaling strategies that respond adaptively to changing demands in VM pools. The approach builds on established AI methodologies and adapts them to the specificities of CI/CD operations, offering a novel contribution to the field [7].

3. THEORETICAL FRAMEWORK

3.1 Fundamentals of Reinforcement Learning

Reinforcement Learning (RL) involves an agent that improves its decision-making strategy through interactions with a dynamic environment. By observing states and receiving feedback in the form of rewards or penalties based on actions carried out, the agent refines its policy to maximize long-term returns. Sometimes the agent is further broken down into agent and interpreter, where the agent carries out actions based on an interpreter applying the policy to generate rewards and calculate state (Figure 1). The core mechanics of RL involve balancing the exploration of untested actions to uncover potentially superior strategies against the exploitation of known actions that it knows will yield high rewards. An RL model can be broadly defined in terms of the state space, which consists of all possible scenarios the agent can encounter, the action space, which details possible actions the agent can take, the reward function, which is the immediate value of actions, the policy, a strategy mapping states to actions, and the value function, estimating the expected return from each state under the current policy.

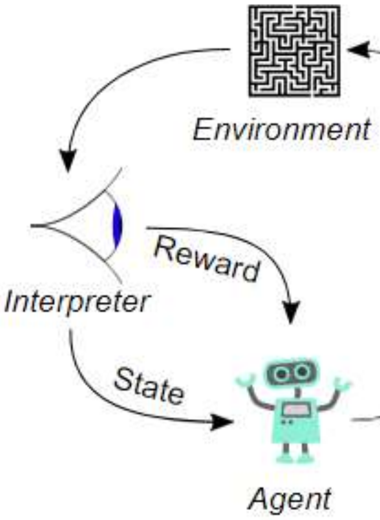


Figure. 1

3.2 Model of the CI/CD Environment

A CI/CD pipeline consists of various stages that build, test, and release software (Figure 2). However, for simplicity, the CI/CD environment for this study is modeled as a system where the states represent various levels of demand and resource availability within the pipeline [2]. Actions in this context refer to scaling decisions—specifically, the scaling up or down of VM pools and the adjustment of VM capacities. The reward function is designed to optimize resource utilization and cost, providing positive rewards for actions that enhance efficiency and negative penalties for wasteful resource allocation or delays in pipeline processing [10].

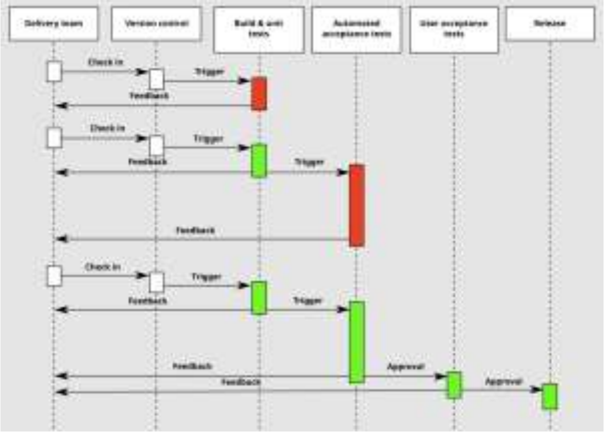


Figure. 2

3.3 Impact of Reinforcement Learning

Reinforcement learning (RL) offers a methodological framework for addressing the issue of dynamic resource allocation. By using agents that learn from interactions with the environment without explicit instruction, RL can adaptively manage resources based on the observed state of the system and the feedback received from the environment. In the context of CI/CD pipelines, an RL agent can learn optimal strategies for scaling up or down virtual machine (VM) pools based on real-time demands, thus optimizing resource utilization and minimizing costs [32, 33].

The application of reinforcement learning in this environment enables more agile and cost-effective management of resources [25]. By continuously learning from the system's performance and adapting to changes in demand, the RL agent can determine the most efficient allocation strategies in real-time. This adaptive approach reduces wastage of resources and ensures that the CI/CD pipelines operate smoothly without unnecessary delays, thereby supporting faster software development cycles and reducing operational costs [26].

4. METHODOLOGY

4.1 Design of the Reinforcement Learning Agent

The reinforcement learning agent is based on a Deep Deterministic Policy Gradient (DDPG) model, a type of algorithm well-suited for continuous action spaces, which is appropriate given the nature of resource allocation in CI/CD environments.

4.1.1 Actor-Critic Approach

DDPG is an actor-critic algorithm that learns a policy (actor) to map states to actions and an estimated value function (critic) that predicts the expected rewards of taking those actions in given states. [3] In an actor-critic approach, the actor network proposes actions based on the current state, and the critic network evaluates these actions by estimating the future rewards. The Actor Network maps states to actions, using a deep neural network to learn the policy function. This network outputs the optimal action given the current state. The Critic Network estimates the value of taking an action in a given state, based on the reward function. It takes both the current state and the action provided by the actor as inputs, facilitating the training of the actor by providing gradient information.

4.1.2 Model Configuration

We can model the DDPG agent at a high level as an agent carrying out actions on an environment to receive rewards and state updates (Figure 3). Then we can further break down these 3 parts into:

4.1.2.1 State Space

The state space consists of a comprehensive snapshot of the system's current resource utilization and demand across multiple CI/CD pipelines. Each state vector includes:

- Number of Active Pipelines: An integer count of currently active pipelines, which provides a direct measure of workload and demand.

- Resource Requirements of Each Pipeline: A vector where each element represents the resource demand (CPU, memory, I/O throughput) of a corresponding pipeline. This could be normalized against maximum available resources to standardize input scale.

- Current Capacity of VM Pools: Quantitative metrics such as total number of VMs, and the distribution of their capacity (e.g., percentage utilization of CPU and memory resources).

4.1.2.2 Action Space

The action space in the DDPG framework is continuous, which allows for fine-grained control over resource allocation decisions. Actions are real-valued vectors that specify:

- Initiation or Termination of VM Instances: A set of values where each represents the change in the number of VMs dedicated to a pipeline, where positive values indicate initiation, and negative values indicate termination.

- Adjustments to Computational Power or Memory of Existing VMs: Continuous adjustments to the configurations of existing VMs, scaled as a percentage increase or decrease relative to their current configurations.

4.1.2.3 Reward Function

The reward function is designed to evaluate the efficiency and cost-effectiveness of the actions taken by the agent. It is computed as a weighted sum of several factors:

- Reduction of Idle VM Time: Rewards the agent for decreasing the amount of underutilized VM resources, which correlates directly with cost savings.

- Avoidance of Pipeline Delays: Penalizes delays in pipeline execution, incentivizing the agent to maintain or improve throughput.

- Minimization of Operational Costs: Incorporates cost metrics such as power consumption and VM rental costs, providing a direct incentive for cost-effective resource management.

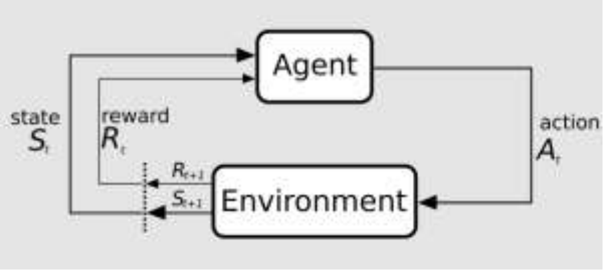


Figure. 3

4.2 Capacity Optimization Techniques

The RL agent will use the learned policy to dynamically adjust the number of VMs in the pool. It will consider current demand, pipeline priorities, and historical data on peak times to predict future needs. It uses both Proactive Scaling (adjusting resources in anticipation of increased activity based on trends and past usage patterns) and Reactive Scaling (responding in real-time to changes in demand, scaling up resources to meet an unexpected surge and scaling down during idle periods) [12].

Beyond simply scaling the number of VMs, the agent also decides on the capacity configuration for each new VM instance in terms of CPU, memory, and storage. This decision is based on the specific requirements of the pipelines currently in operation, aiming to match resource provisioning closely with the actual needs of each job. This approach minimizes the wastage associated with over-provisioning and the performance issues related to under-provisioning [30, 31].

The DDPG model allows for continuous learning and adjustment as the environment changes [13]. The agent's policy will evolve as it receives feedback from the environment in the form of rewards, which are based on the efficiency and cost-effectiveness of the resource allocation. The critic component helps in reducing the potential of sub-optimal policy convergence by providing a baseline to evaluate the effectiveness of a policy [14].

4.3 Explanation of Model Choice

The DDPG model is particularly well-suited for this application because of its ability to handle complex, continuous action spaces efficiently and its robustness in dealing with environments with a high degree of uncertainty and variability—characteristics common in CI/CD systems [8]. This architecture also enables the agent to handle the high-dimensional state space of a CI/CD system, where the number of active pipelines and the status of each VM can vary significantly. This model supports a sophisticated level of decision-making that is essential for managing the dynamic and often unpredictable demands of multiple CI/CD pipelines.

5. DISCUSSION

5.1 Benefits of Using Reinforcement Learning

The application of reinforcement learning (RL) in the management of CI/CD environments offers several benefits. Firstly, RL's ability to learn optimal policies through trial and error allows it to adapt to changing software development workflows, which are characterized by fluctuating demands and varying task complexities [15].

Traditional resource scaling methods in CI/CD environments typically rely on static rules or thresholds that trigger scaling actions when certain metrics are met [20]. These methods, while predictable and simple to implement, often do not account for the nuanced variations in resource requirements that can occur within and across pipeline executions. In contrast, an RL-based approach can provide more granular control over resource allocation by making decisions based on the state of the system at any given moment [16, 19]. This can lead to more efficient use of resources, as the system only scales up when necessary and scales down as soon as feasible, thus avoiding both under-utilization and over-provisioning.

The use of RL in CI/CD resource management has the potential to significantly enhance both efficiency and cost-effectiveness. The RL agent, by continuously updating its policy based on real-time feedback, can ensure that resource allocation is always aligned with current needs, thus reducing the overhead costs associated with static resource provisioning methods [11]. By optimizing the allocation and scaling of resources dynamically, the system can ensure that resources are not wasted on underutilized VMs and that pipeline processes are not delayed by resource shortages [17]. This can lead to faster development cycles and reduced operational costs, providing a competitive advantage to organizations that implement such advanced resource management systems.

5.2 Potential Challenges and Mitigation Strategies

Implementing an RL-based system for resource management in CI/CD pipelines presents several challenges. One major challenge is the requirement for a significant amount of data to train the RL agent effectively. Without adequate data, the agent may not be able to learn effective policies, leading to poor performance and potential resource wastage [18]. Additionally, the integration of RL into existing CI/CD systems can be complex, requiring substantial changes to infrastructure and processes. To mitigate these challenges, it is advisable to begin with a hybrid approach, where RL-based scaling decisions are initially guided by existing static rules. Furthermore, simulation environments can be used to train the RL agent before full deployment, reducing the risk of errors in a live setting [27].

6. CONCLUSION

6.1 Summary

This paper has explored the conceptual application of reinforcement learning (RL) to the problem of dynamic resource management in CI/CD environments, specifically addressing the scaling and optimization of virtual machine (VM) pools. The methodology employs a Deep Deterministic Policy Gradient (DDPG) model, chosen for its suitability in handling continuous action spaces and complex decision environments like those found in CI/CD systems. The theoretical framework outlines how an RL agent could dynamically adapt resource allocation based on real-time demands, thereby enhancing operational efficiency and reducing costs.

The significance of this research lies in its potential to transform traditional static resource management strategies in CI/CD practices into more adaptive, efficient, and cost-effective processes. By integrating RL into CI/CD resource management, organizations can potentially achieve more agile responses to changing demands, minimize resource wastage, and expedite development cycles [9]. The research presented lays a foundational framework for future studies and practical implementations that could substantiate and further develop these concepts.

6.2 Future Research Directions

Future research in this area could focus on several key aspects. Firstly, exploring alternative RL algorithms and comparing their performance in similar settings could provide deeper insights and potentially identify more optimized approaches. Further research could also examine the integration of RL with other AI techniques, such as predictive analytics, to enhance the predictive accuracy of resource demand and further optimize resource allocation strategies.

7. REFERENCES

[1] N. Railić and M. Savić, "Architecting Continuous Integration and Continuous Deployment for Microservice Architecture," 2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2021, pp. 1-5

[2] Bhavsar, S., Rangras, J., Modi, K. (2021). Automating Container Deployments Using CI/CD. In: Kotecha, K., Piuri, V., Shah, H., Patel, R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 52. Springer, Singapore.

[3] Zhou, Z., Wang, Q., Li, J. et al. Resource Allocation Using Deep Deterministic Policy Gradient-Based Federated Learning for Multi-Access Edge Computing. J Grid Computing 22, 59 (2024)

[4] Faustino J, Adriano D, Amaro R, Pereira R, da Silva MM. DevOps benefits: A systematic literature review. Softw: Pract Exper. 2022; 52(9): 1905–1926.

[5] Erdenebat B, Bud B, Batsuren T, Kozsik T. Multi-Project Multi-Environment Approach—An Enhancement to Existing DevOps and Continuous Integration and Continuous Deployment Tools. Computers. 2023; 12(12):254

[6] M. S. Ali and D. Puri, "Optimizing DevOps Methodologies with the Integration of Artificial Intelligence," 2024 3rd International Conference for

Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1-5

[7] T. Mboweni, T. Masombuka and C. Dongmo, "A Systematic Review of Machine Learning DevOps," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-6

[8] Hrusto, A., Runeson, P. & Engström, E. Closing the Feedback Loop in DevOps Through Autonomous Monitors in Operations. SN COMPUT. SCI. 2, 447 (2021)

[9] Z. Wang, M. Shi and C. Li, "An Intelligent DevOps Platform Research and Design Based on Machine Learning," 2020 Eighth International Conference on Advanced Cloud and Big Data (CBD), Taiyuan, China, 2020, pp. 42-47

[10] A. F. Nogueira, J. C.B. Ribeiro, M. A. Zenha-Rela and A. Craske, "Improving La Redoute's CI/CD Pipeline and DevOps Processes by Applying Machine Learning Techniques," 2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC), Coimbra, Portugal, 2018, pp. 282-286

[11] Farmani, M., Farnam, S., Mohammadi, R. et al. D2PG: deep deterministic policy gradient based for maximizing network throughput in clustered EH-WSN. Wireless Netw (2024)

[12] Fu, J., Liang, L., Li, Y., Wang, J. (2022). Deep Deterministic Policy Gradient Algorithm for Space/Aerial-Assisted Computation Offloading. In: Gao, H., Wun, J., Yin, J., Shen, F., Shen, Y., Yu, J. (eds) Communications and Networking. ChinaCom 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 433. Springer, Cham

[13] L. Lyu, Y. Shen and S. Zhang, "The Advance of Reinforcement Learning and Deep Reinforcement Learning," 2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 2022, pp. 644-648

[14] A. Jeerige, D. Bein and A. Verma, "Comparison of Deep Reinforcement Learning Approaches for Intelligent Game Playing," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0366-0371

[15] Faustino J, Adriano D, Amaro R, Pereira R, da Silva MM. DevOps benefits: A systematic literature review. Softw: Pract Exper. 2022; 52(9): 1905–1926

[16] Kupwiwat, Ct., Hayashi, K. & Ohsaki, M. Deep deterministic policy gradient and graph attention network for geometry optimization of latticed shells. Appl Intell 53, 19809–19826 (2023)

[17] D. Kreuzberger, N. Kühl and S. Hirschl, "Machine Learning Operations (MLOps): Overview, Definition, and Architecture," in IEEE Access, vol. 11, pp. 31866-31879, 2023

[18] Gupta, S., Pal, S., Kumar, K. et al. Coupling Effect of Exploration Rate and Learning Rate for Optimized Scaled Reinforcement Learning. SN COMPUT. SCI. 4, 638 (2023)

[19] de Lellis Rossi, L., Rohmer, E., Dornhofer Paro Costa, P. et al. A Procedural Constructive Learning Mechanism with Deep Reinforcement Learning for Cognitive Agents. J Intell Robot Syst 110, 38 (2024)

[20] N. D. R and Mohana, "Jenkins Pipelines: A Novel Approach to Machine Learning Operations (MLOps)," 2022 International Conference on Edge Computing and Applications (ICECAA), Tamilnadu, India, 2022, pp. 1292-1297

[21] S. S. Pandi, P. Kumar and R. M. Suchindhar, "Integrating Jenkins for Efficient Deployment and Orchestration across Multi-Cloud Environments," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2023, pp. 1-6

[22] Radhika, E. G., & Sudha Sadasivam, G. (2021). A review on prediction based autoscaling techniques for heterogeneous applications in cloud environment. Materials Today: Proceedings, 45(2), 2793-2800.

[23] Ewim, D. R. E., Ninduwezuor-Ehiobu, N., Orikpete, O. F., Egbokhaebho, B. A., Fawole, A. A., & Onunka, C. (2023). Impact of Data Centers on Climate Change: A Review of Energy Efficient Strategies. The Journal of Engineering and Exact Sciences, 9(6), 16397–01e.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 47 – 53, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1008

Technology Acceptance Model- Based Usability Testing of a Fingerprint Attendance Register System

Emmanuel Kaingu Charo
Technical University of Mombasa
Mombasa, Kenya

Kennedy Hadullo
Technical University of Mombasa
Mombasa, Kenya

Mvurya Mgala
Technical University of Mombasa
Mombasa, Kenya

Abstract: Institutions of higher learning in Kenya have traditionally used paper-based attendance registers, which have been seen to lack validity for decision-making. There is a trend to adopt Biometric attendance registers in a number of institutions, however, they still have usability issues. This study uses a modified Technology Acceptance Model (TAM) to investigate the usability of the fingerprint biometric students' attendance register system. The original TAM used perceived usefulness, and perceived ease of use, as the test factors for acceptance of technology. Researchers have modified the TAM to include more test factors such as attitude toward use, and trust and security. In this study, we use the extended TAM-TRA model. The model includes the attitude toward, trust, and security in using the technology, in addition to the original perceived usefulness, and perceived ease of use, to conduct usability of the fingerprint attendance register system. These are important factors in the successful implementation, acceptance, and adoption of such systems. The study applies quantitative and qualitative surveys and observations, to collect data from sampled users of the fingerprint biometric attendance register system and test its usability using the modified TAM. A class of twenty students at the Technical University of Mombasa interacted with the fingerprint biometric attendance register system, and for each student, the usability tests were carried out, recorded, and analyzed. The perceived usefulness, perceived ease of use, attitude toward use, trust, and behavioral intention to use, scored 88.75%, 70%, 77.5%, 65%, and 77.5% levels of acceptance respectively. The contribution of this paper is in the insight to organizations that seek to improve the acceptance of their biometric recognition systems.

Keywords: Usability; Perceived Usefulness; Perceived Ease of Use; Attitude Toward Using; Trust, Security; Behavioural Intention to Use.

1. INTRODUCTION

Advancements in technology have led to a heavy reliance by governments on digital systems, [1] [8]), that are integrated into our daily life activities at both personal and organizational levels. Organizations rely on technology to manage information and human resources. Biometric technology for example has been widely adopted in the identification of bonified staff in the workplace and also in staff attendance management [25] [21]

Biometric technology is presented by researchers as a measure of the human physiological and behavioral characteristics which provide reliable identification of a person [26]. The technology uses unique and accessible parts of a person's biological makeup such as the face, retina, iris, voice, and fingerprint for verification purposes [12]. It is a system of recognizing image patterns acquired from the biometric data of the person presented for identification. The features of the image are extracted and then compared against the previously stored template images in a database [6]. Depending on the area of application, biometric systems may be used either for *the identification or verification* of persons [16] [2]

The use of fingerprints in biometric systems increased rapidly because of the special strengths fingerprints provide, compared to other human physiological traits. Fingerprint based biometric systems are found to be easy to use, and cheaper to implement [23]. In addition, these systems consume less power and they can easily be implemented in a mobile environment [23]. In schools, colleges, and universities, biometric technology, such as fingerprint attendance register systems, has been used to manage students' attendance with rewarding success and accuracy [23].

However, the success in implementing fingerprint students' attendance register systems does not depend only on its functions, but also on its usability and acceptability by the target users. A product has good usability if both the experts and the novice can use it with ease [11]] [7].

Theoretical models have been suggested that measure usability and acceptance of new technology, such as the Technology Acceptance Model (TAM) (Meennapa Rukhiran, 2023) [1], Theory of Reasoned Action (TRA)[27] [14], Motivational Model (MM) [19], Theory of Planned Behavior (TPB) [5], Combined TAM and TRA (C-TAM-TRA) [16], Model of PC Utilization (MPCU), Innovation Diffusion Theory (IDT) [13], Social Cognitive Theory (SCT) [10], and Unified Theory of Acceptance and Use of Technology (UTAUT) which is an integration of several technology acceptance theories [19].

This study aims to carry out usability and acceptance tests of a fingerprint biometric student attendance register system using the extended TAM-TRA model. These tests were conducted on a proposed fingerprint college students' attendance register for the Technical University of Mombasa. After this introduction, the next section is the related work on TAM-Based Usability Testing of a Fingerprint Attendance Register System. Section 3 provides the methodology used to implement the TAM-based testing model for a fingerprint attendance register system. Section 4 gives the test results, followed by a discussion in section 5, and conclusions in section 6.

1.1 Research Highlights

- A modified TAM-TRA model was realized.

- Successful use of the model on the register system was made

- System effectiveness, satisfaction, and efficiency were found

- Above average scores of usability parameters were achieved.

2. RELATED WORK

Usability was defined by researchers as “the quality of a product that makes it easy to understand, learn, use and attractive to users” [11]. It has also been defined as the extent to which a given product can be used by specific users to obtain predefined goals effectively, efficiently, and satisfactorily [22]. In the field of Human-Computer Interaction (HCI), researchers investigated factors that increase the usability of a product [4]. These factors included effectiveness, efficiency, accessibility, satisfaction, affordance, anthropometry fit, and privacy concerns [11]. Of these factors, effectiveness, efficiency, and satisfaction were identified as key factors of usability (Anh Tho To, Thi Hong Minh Trinh, 2021), [11].

On a stable weighted super-matrix scale, used to show the relative ranking of a given set of usability criteria from a field study test, privacy was the most important concern for biometric recognition systems, and of these systems, fingerprint recognition scored highest [11]. The International Organization for Standardization (ISO) recommended that usability metrics could include effectiveness, efficiency, and satisfaction [18]. Effectiveness was defined as the accuracy and completeness with which users achieved specified goals. Efficiency had to do with the time it would take for a process to complete a given task. Satisfaction was used to describe the comfort or freedom of discomfort and acceptability of the product by the users (ISO, 2010), [18][11].

In investigating the usefulness of fingerprint biometric attendance registers at Nyamagana Municipality of the United Republic of Tanzania, using the Theory of Planned Behaviour, it was found that to change employees’ behavior at work, their attitudes and social norms (social pressure) toward the desired behavior should be addressed first. [17].

Research on the measure of adoption of Information and Communication Technology (ICT) led to the development of various models to predict and understand the acceptance of technology. A notable model was the Technology Acceptance Model (TAM) (Aceron, 2021). TAM is a model that analyzes the factors influencing and motivating users to adopt identification management systems. The acceptance test factors used in the TAM model include the intention of the user to use the technology, the attitude toward using the technology based on trust, the perceived usefulness, and the perceived ease of use [3].

TAM is based on two primary factors that affect the intention to use a given technology [24]. These factors were the Perceived Usefulness (PU) of the product and the Perceived Ease of Use (PEU) of the product. PU was described as the extent to which a person was convinced or believed that a given technology would improve job performance. PEU was described as the extent to which a person was convinced. believed that using the given technology would be effortless [15]. Early Technology Acceptance Model questionnaires consisted of 12 items, six testing on PU and six on PEU. The responses were then weighted on a 1-7 scale from extremely unlikely, quite likely, slightly, neither, slightly, quite unlikely, and extremely unlikely. The responses could either be all verbal or all numbered 1-7. The severity of the likelihood could be from lowest to highest or from highest to lowest [15].

Modifications on TAM were made to include not only the likelihood ratings of PU and PEU but also to measure User Experience (UX) by using Experiential ratings. [15] in research that used a modified TAM, used three questionnaires that rated PU and PEU in four versions of responses. These versions were the use of weightings of the responses on a 1 – 7 scale starting from extremely likely to extremely unlikely for both verbal and numeric verbal left-right, verbal right-left, numeric left-right, and numeric right-left in the order of severity. The following formulae were used:

PU = (Average (Tam01, Tam02, Tam03, Tam04, Tam05, Tam06) – 1) (100/6)

PEU = (Average (Tam07, Tam08, Tam09, Tam10, Tam11, Tam12) – 1) (100/6), Where Tam01 – Tam12 ranged from 1-7 on the weighted scale. [15].

The results were then subjected to an analysis of mean differences, factor analyses, regression analyses, and analysis of response errors. The numeric L-R version of scoring responses with a magnitude of agreement increasing from left to right gave the most significant Likelihood-To-Recommend (LTR) the product for use [15].

In investigating user acceptance factors related to biometric face recognition technologies, [16] also used questionnaires to elicit students’ perceptions and test hypotheses on biometric facial recognition for the use of an examination attendance register.

In a usability evaluation of an integrated electronic medication management system for an outpatient Oncology unit of a major teaching hospital, five UTAUT constructs were identified [22]. These constructs are performance expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Facilitating Conditions (FC), and Behavioral (BI) [22]. Performance Expectancy is the degree to which a user of a given system believes that using the system results in gains in job performance. Effort Expectancy (EE) is the extent of ease associated with using the system. Social Influence (SI) is the degree to which a user perceives that others are recommending him or her to use the new system [22]. Facilitating Conditions (FC) is the extent to which the user believes that an organizational and technical infrastructure exists to support the use of the system. Behavioral Intention (BI) is the willingness of respondents to use the system [11]. **To** adopt a conceptual framework for the usability testing of a fingerprint biometric attendance register these constructs were considered:

Performance Expectancy can be directly related to the biometric attendance register's Perceived Usefulness (PU) [11]. It is the factor that predicts the gains (or usefulness) of the biometric technology. Effort Expectancy is the Perceived Ease of Use (PEU) [11]. It predicts the effort used in terms of how difficult, or how easy the system is to use in taking enrolment and the attendance of students in a class session. An increase in PEU directly influences the PU [3][4].

The Social Influence (SI) construct according to [15]), and [11], is the Attitude Toward Using (ATU). It was used to predict the influence other potential users have on the current user of the biometric attendance register that could affect the perceived usefulness. Facilitating Conditions (FC): - This construct was redefined as the Trust (T). It was used to predict the level of trust the users had in the organization to obtain and maintain the required infrastructure for the biometric system [4]. Behavioral Intention (BE) is referred to as the Behavioral Intention to Use (BIU). It was used to predict whether the users would prefer the biometric attendance register to the traditional paper-based attendance register [3][4].

The security (S) construct was added to the traditional TAM-TRA model. The aim was to separate the Trust construct from the Security [3][4]. In our case, Security is the level of confidence the user has in the system to protect attendance data as provided for in the laws and policies on data protection and privacy. This construct has a direct influence on the users' willingness to use the biometric attendance register. It is effective in measuring user confidence in the biometric system. It is an external factor in the user's willingness to use the system.

3. METHODOLOGY

Surveys, observations, and interviews were conducted to collect data from students as the primary users of the biometric attendance registers. The students were allowed to interact with the fingerprint biometric attendance register system. Online Google form questionnaires were then given to the students to fill out and submit. The data collected was analyzed and the results were recorded.

3.1 Usability Testing

The usability test model, which is a modified extended TAM-TRA model is shown in Figure 3.1. From research, PU and PEU constructs are grouped under effectiveness, ATU and TS fall under satisfaction, while BIU, considering the average time to perform the tasks, can be considered as efficiency. The main tasks in this study were affixing the fingerprint on the sensor during enrolment and class attendance.

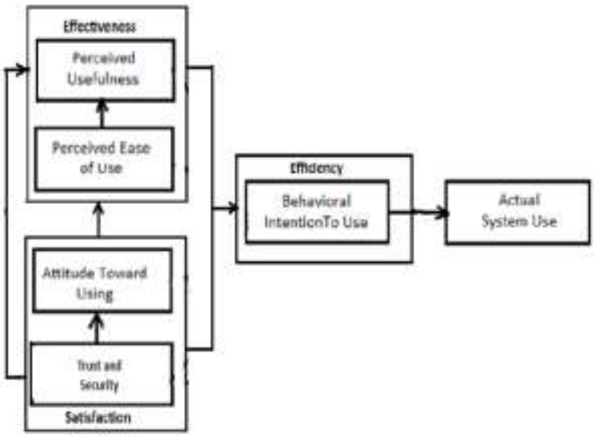


Figure 3.1 The Extended TAM-TRA model with regrouped test factors adopted from [16].

3.2 Data collection

Interviews were conducted using Google form online questionnaires. A group of 20 students at the Technical University of Mombasa were allowed to interact with the fingerprint attendance register system and then filled out the questionnaire shown in Table 3.

Table 3. The adopted questionnaire for effectiveness, satisfaction, and efficiency.

Classification	Question
Perceived Usefulness (Effectiveness)	My names were correctly displayed on the system
	The system was able to take student attendance
	Taking attendance was effective with this system.
	Once attendance has been taken, no changes can be made
Perceived Ease of Use (Effectiveness)	The biometric attendance register was easy to use
	My fingerprint was captured on the first attempt
	There were at least two unsuccessful attempts
	Parents and guardians can access the attendance records.
Attitude Towards Use	Attendance reports can be printed from the system
	In this biometric system, a student cannot

(Satisfaction)	fake attendance.
	You prefer the biometric register to the paper register.
	No fear of disease infections with this attendance register
Trust and Security (Satisfaction)	Attendance can be taken on day one of the semester.
	The biometric register is foolproof and data is secure.
	The biometric register is likely to be hacked by students
	Student data in the biometric register is protected by law
Behavioral Intention to Use (Efficiency)	The biometric register may cause queues during attendance.
	Fingerprint sensors in every classroom are too expensive
	Internet is not fast and sufficient throughout the university
	The biometric register is fast and prevents cheating in exams

A Likert scale was used for the questionnaire responses. The answers were: Strongly Agree (SD), Agree (A), Neutral (N), Disagree (DA), and Strongly Disagree (SD). During analysis, the total responses for SA and A were added and presented as A. DA and SD were added together and presented as DA.

3.3 Determination of effectiveness, satisfaction, and efficiency

The test factors in the adopted TAM-TRA model were the Perceived Usefulness (PU) and Perceived Ease of Use (PEU), used in the original TAM, the Attitude Toward Using (ATU), Trust and Security (TS), and the Behavioural Intention to Use (BIU) [14]. PU and PEU were grouped as tests for the effectiveness of the biometric attendance register system. ATU and TS were classified under the test for satisfaction whereas BIU was the efficiency test.
According to [18], the effectiveness of the attendance register was determined by the scores for PU and PEU.

Effectiveness can be calculated from the usability metrics format:

$$Effectiveness = \frac{\varphi}{\omega} X\ 100\%$$

$$where\ \varphi = Number\ of\ tasks\ completed\ successfully\ \ and$$

$$\omega = Total\ number\ of\ tasks\ undertaken.$$

The test for satisfaction was calculated from the scores for ATU, and TS
Since there is a direct relationship between effectiveness and satisfaction, then:

$$Satisfaction = k\frac{\varphi}{\omega} X\ 100\%$$

Where k is a constant, assuming all factors remain constant in both the test for effectiveness and satisfaction, k was taken as 1[18.
Efficiency can also be calculated using the formula for time-based efficiency:

$$Efficiency) \ = \frac{\sum_{j=1}^{R} X \sum_{i=1}^{N} \frac{n_{ij}}{t_{ij}}}{NR}$$

Where:

N = The total number of tasks, or goals, R = The number of users
n_{ij} = The result of task i by user j; if the user completes the task, then N_{ij} = 1, if not, then N_{ij} = , t_{ij} = The time spent by user j to complete task i. If the task is not completed, then time is measured till the moment the user quits the task [18].

4. RESULTS

Students who were the target users of the fingerprint biometric register interacted with the system and filled in questionnaires to test its usability and adoption. The five test parameters were Perceived Usefulness, Perceived Ease of Use, Attitude Towards Using, Trust and Security, and Behavioural Intention to Use. Of these test parameters, the first two were tests for effectiveness, the next two tested for satisfaction, and the last tested for efficiency. The results for each test are shown in Tables 4.1, 4.2, and 4.3.
Table 4.4 summarises the calculated values of each test factor's usability levels.

Table 4.1. Results for usability test on effectiveness.

Test Parameter	**Question**	**A**	**N**	**DA**	**Total**
Perceived Usefulness (PU) (Effectiveness)	My names were correctly displayed on the system	16	3	1	20
	The system was able to take student attendance	20			20
	Taking attendance was effective with this system.	19		1	20
	Once attendance has been taken, no changes can be made	16	3	1	20

Perceived Ease of Use (PEU) (Effectiveness)	The biometric attendance register was easy to use	18	2		20
	My fingerprint was captured on the first attempt	14	1	5	20
	There were at least two unsuccessful attempts	9	2	7	20
	Parents and guardians can access the attendance records.	15	5		20

Table 4.2. Results for usability test on satisfaction.

Test Parameter	Question	A	N	DA	Total
Attitude Toward Using (ATU) (Satisfaction)	Attendance reports can be printed from the system	17	3		20
	In this biometric system, a student cannot fake attendance.	19		1	20
	You prefer the biometric register to the paper register.	16	1	3	20
	No fear of disease infections with this attendance register	10	4	6	20
Trust and Security (TS) (Satisfaction)	Attendance can be taken on day one of the semester.	20			20
	The biometric register is foolproof and data is secure.	13	6	1	20
	The biometric register is likely to be hacked by students	10	6	4	20
	Student data in the biometric register is protected by law	9	9	1	19

Table 4.3. Results for usability test on efficiency.

Test Parameter	Question	A	N	DA	Total
Behavioral Intention to Use (BIU) (Efficiency)	The biometric register may cause queues during attendance.	16	4		20
	Fingerprint sensors in every classroom are too expensive	12	7	1	20
	Internet is not fast and sufficient throughout the university	17	3		20
	The biometric register is fast and prevents cheating in exams	17	2	1	20

Table 4.4. Summary of usability outcomes.

Test Group	Test factor	Total positive responses	Total possible responses	% Level of Usability
Effectiveness	PU	71	80	88..75
	PEU	56	80	70
Satisfaction	ATU	62	80	77.5
	TS	52	79	65
Efficiency	BIU	62	80	77.5

5. DISCUSSION

The three tests that were conducted on the fingerprint biometric attendance register were effectiveness, satisfaction, and efficiency. These tests used five parameters: PU, PEU, ATU, TS, AND BIU. The high score for effectiveness of 88.75% for PU and 70% for PEU showed that the biometric attendance register was useful and easy to interact with even without prior knowledge of such systems. Key considerations in the use of biometric registers were the ability to capture the fingerprint, accurate display of students' information, and the ability to take students' attendance without undue changes in the attendance record. A score of 88.75% indicated that the register was effective in enrolment and taking attendance. The lower score of 70% for PEU could have been due to variations in internet speeds and speeds within the classroom. Overall, the effectiveness test was high.

On satisfaction, the usability test on ATU, scored 77% while TS scored 65%. The score reflected the confidence and redness of the students to use the technology. The test considered factors on attitude and expectations from the attendance register. Tests on Trust and Security focused on whether the biometric attendance register was foolproof and whether their personal information was secure. The 77.5% score on BIU was an indicator that the fingerprint attendance register was efficient. The average time a student took to interact with the register system was four seconds. Some of the factors that could affect behavior and efficiency could be the crowding of students at the classroom door waiting to take attendance. Although these crowds were not witnessed, any system for students' attendance must be efficient and avoid time wastage during attendance.

6. CONCLUSION

The usability of the fingerprint attendance register was tested and scores were calculated. The fingerprint biometric attendance register was deployed to a class sample of twenty students. Firstly, the students enrolled in the system and validated their records. A class session was then activated and students took attendance in turn. While the students took attendance, observations on the system's effectiveness and efficiency were made. The number of attempts to affix the fingerprint during attendance and the display of correct students' records were keenly observed and recorded. Upon taking attendance, students were given online questionnaires to fill out and submit.

Data collected from the interactions of students on the attendance register and from the questionnaires were tabulated and analyzed. Usability tests for the effectiveness of the system, level of satisfaction with the use of the register, and its efficiency were calculated and tabulated. The usability tests showed a considerably high score in effectiveness, satisfaction, and efficiency. A PU score of 88.75% and a PE score of 70% were obtained. These were strong indicators of the effectiveness of the register system. ATU and TS scored a considerable high of 77.5% and 65% respectively. On efficiency, BIU scored 77.5%. These scores gave a good indicator that the biometric attendance register was efficient and satisfactory to use.

The results obtained help to reveal important factors that should be considered in conducting usability on biometric attendance registers. These include gender, social influences, age, and experiences with similar technologies. Emerging issues on privacy and security of information are also factors to be considered. Overall, the usability test results obtained gave a strong indicator that biometric attendance register technologies are effective, efficient, and secure for use.

7. Acknowledgment

I acknowledge the directorate of Partnership and Research Institute of the Technical University of Mombasa, Kenya for partly funding this research.

8. REFERENCES

[1] Abdella Kamal A. et al (2022). The Effect of Intensive Usage of Digital Payment in Egypt*Compunet 299*

[2] Abderrahmane Herbadji et al.2020Contactless Multi-biometric System Using Fingerprint and Palmprint Selfies*Traitement du Signal Vol. 37, No. 6, December, 2020*889-897

[3] Aceron, V. P. (2021). *An Evaluative Study on the Citizen's perception towards the Philippine Identification System through the lens of Technology Acceptance Model.* Manila: Kuleuven.

[4] Anh Tho To, Thi Hong Minh Trinh (2021). Understanding behavioral intention to use mobile wallets in Vietnam: Extending the tam model with trust and enjoyment*Cogent Business & Management, 8:1, 1891661, DOI: 10.1080/23311975.2021.1891661*3-5

[5] Ajzen, I. (2020). The Theory of Planned Behavior: Frequently Asked Questions2020*Wiley Periodicals*314-315

[6] Cao, k. & Jain, A. K. . (2019). *Automated Latent Fingerprint Recognition.* Retrieved from IEEE Transactions on Pattern Analysis and Machine Intelligence, 41(4), 788–800. : https://doi.org/10.1109/TPAMI.2018.2818162

[7] F. Rangraz Jeddi et al.(2020). Usability evaluation of a comprehensive national health information system: A heuristic evaluation*Elsevier Informatics in Medicine Unlocked*1-2

[8] Genia Kostka et al (2023). Under Big Brother's Watchful Eye: Cross-country Attitudes Toward Facial Recognition Technology *Government Information Quarterly 40*

[9] ISO. (2010). *Ergonomics of Human System Interaction.* Switzerland: International Standardization Organization

[10] Jerusalem Merkebu et al. (2020). Situativity: a family of social cognitive theories for understanding clinical reasoning and diagnostic error*Diagnosis, vol. 7, no. 3*169-176

[11] Junhjoung Oh, U. L. (2019). Usability Evaluation Model for Biometric System Considering Privacy Concerns Based on MCDM Model. *Security and Communication Networks*

[12] Khan, S. U. et, al. (2017). A New Biometric Matching Fingerprints System for Personal Authentication Using R305. *Academia of Information Computing Research, 1(1).*, 1581-1588

[13] Kum Fai Yuen et al2020Factors influencing autonomous vehicle adoption: an application of the technology acceptance model and innovation diffusion theory*Technology Analysis & Strategic Management 33.5*507-508

[14] Lai, PC. (2017). The Literature Review of Technology Adoption Models and Theories For The Novelty Technology2017*Journal of Information Systems and Technology Management Vol. 14, No. 1, Jan/Apr., 2017 pp. 21-38 ISSN online: 1807-1775* 21-28

[15] Lewis, J. R. (2019). Comparison of Four TAM item formats: Effects of Response Option Labels and Order. *Journal of Usability Studies Vol. 14 Issue 4,* 224 - 236.

[16] Meennapa Rukhiran, S. W.-I. (2023). User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model. *Sustainability, MDPI*, 7-8.

[17] Michael Greyson Mgonja, Alexander Boniface Makulilo. (2022). Are Biometric Attendance Registers a Panacea for Workplace Absenteeism in Tanzania? A Lesson from Public Secondary Schools in Nyamagana Municipality. *Tanzania Journal of Sociology Vol. 8, Issue No.1*, 77 - 99.

[18] Mifsud, J. (2022). *Usability Metrics, A guide to Quantify the Usability of any System*. Retrieved from UsabilityGeek: file:///C:/Users/emman/Zotero/storage/K3UT5GCA/usability-metrics-a-guide-to-quantify-system-usability.html

[19] Momani, Alaa M. (2020). The Unified Theory of Acceptance and Use of Technology: A New Approach in Technology Acceptance*International Journal of Sociotechnology and Knowledge Development 12, no.* 379-98

[20] Nabil Hasan Al-Kumaim et al. (2021). Exploring the Impact of the COVID-19 Pandemic on University Students' Learning Life: An Integrated Conceptual Motivational Model for Sustainable and Healthy Online Learning*Sustainability 2021, 13(5), 2546; https://doi.org/10.3390/su13052546*

[21] Namiti, A. (2020). Adoption of Biometric System to Manage Teachers Absenteeism for Improvement of Teachers Performance: A Case Study for Karuri High School in Kiambu County, Kenya2020 *International Journal of Scientific and Research Publications, Volume 10, Issue 5, ISSN 2250-3153*434

[22] Racha Dabliz, e. (2021). Usability evaluation of an integrated electronic medication management system implemented in an oncology setting using the unified theory of acceptance and use of technology. *BMC Medical Informatics and Decision Making*, 3.

[23] Reddy, Y. S and Pooja, P. (2019(Review of Fingerprint Recognition Based Automatic Attendance System*International Journal of Innovative Research in Electrical, Electronics, Instrumentation, and Control Engineering Vol. 7, Issue 10, October 2019* 24

[24] Sri Rahayu Natasia et al. (2021). Acceptance analysis of NUADU as e-learning platform using the Technology Acceptance Model (TAM) Approach *Information Systems International Conference (ISICO 2021)* 514-515 Balikpapan, 76127, IndonesiaElsevier B.V.

[25] Wanjiku, J. (2022). Biometric Clocking System Infrastructure and Performance of Selected Tertiary Institutions in Kiambu County, Kenya2022*East African Scholars Journal of Economics, Business and Management ISSN 2617-4464 (Print) | ISSN 2617-7269 (Online)* 378-378

[26] Wieclaw, L. et, al. (2017). Biometric Identification for Raw ECG Signal Using Deep Learning Techniques. *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS*, 127-133.

[27] Xiao, M. (2020). Factors Influencing eSports Viewership: An Approach Based on the Theory of Reasoned Action2020*Communication & Sport 8(1) College of Journalism and Communications, University of Florida, Gainesville, FL, USA*94