International Journal of Computer Applications Technology and Research
Volume 13–Issue 01, 09 - 18, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1301.1003

Alert Correlation Model Based on Hybrid Machine Learning Techniques to Enhance the Performance of NIDS

Joseph Mbugua
Garissa University
Kenya

Enoch Mogendi
Garissa University
Kenya

ABSTRACT

There obstacles in developing an effective intrusion detection systemin this modern digital world. This work proposes a three level model in developingNIDS that offers multiple types of correlations. In the first level, several feature selection techniques are integrated existing feature selection techniques Correlation Feature Selection, Information Gain and Chi square to find the best set of features used in this work. The second level enhances the structural based alert correlation model based on Expectation and Maximization (EM) to improve the quality of alerts and detection capability by grouping alerts with common attributes. Then an anomaly classification module is designed in the third level based on fusion of five heterogeneous classifiers Support Vector Machine (SVM), Instance based Learners (IBL), Random Forest, J48, and Bayes Net using Voting as a Multi-Classifier.

The NSL KDD dataset is used in this experiment. The overall detection rate is 99.9%, false error rate 0.1% and execution rate of 1340.7 seconds. This shows that HAC is effective and practical in providing complete correlation even on high dimensionality, large scaled and low quality dataset used in intrusion detection system.

Keywords: Alert Correlation, Machine Learning, Model, Performance, Intrusion Detection.

Introduction

The advancement of modern computers, network and internet has led to their widespread adoption and application in organizations' critical systems. These organizations are susceptible to intrusions and malicious activities that attempt to compromise the proprietary business plans (integrity and confidentiality) loss of critical business data and disruption of services (availability) of system resources (Alkhpor & Alserhani, 2023). Intrusion detection is a system for detecting intrusions and hence works as the major defensive mechanism in a network environment (Albasheer et al., 2022; Alsoufi et al., 2021; Kiruki, Muketha, & Kamau, 2023). It's main goal is to automatically monitor network traffic and classify them as normal or suspicious activities and inform the security analyst or response system to take appropriate action before the intrusion compromises the network.

Alert Correlation (AC) takes the generated alerts, process and produce compact reports on the security status of the network under surveillance(Albasheer et al., 2022; Alkhpor & Alserhani, 2023).

There are four main techniques proposed in alert correlation focusing on analyzing intrusion alerts produced by computer networks to improve detection and prediction ability in NIDS. In Structural-based AC (SAC), alerts are correlated based on similarity of attributes. that it cannot discover the causal relationships among alerts(Ho, Hua, Siraj, & Din, 2017). The Causal-based AC (CAC) analysis finds the relationship between alert types in the alert stream to discover alert attributes that have the greatest impact on the relationship between intrusion alerts. Research by(Diehl & Ramirez-Amaro, 2023; Makhlouf, Zhioua, & Palamidessi, 2020; Wang et al., 2022) have showed that the technique can discover unknown alerts but it is expensive to build a complete attack database. The Statistical-based AC (STAC) defines normal behavior by collecting data relating to the behavior of legitimate users over a period of time. The work by (Boero et al., 2017)indicates that good performance of Statistical-based AC strongly depends on good parameters setting which is very difficult to estimate. The goal of data mining and machine learning technique is to produce a model expressed as an executable code which can be used to perform data mining tasks such as classification, prediction or other similar task(Kayode Saheed, Idris Abiodun, Misra, Kristiansen Holone, & Colomo-Palacios, 2022; Liu & Lang, 2019; Mari, Zinca, & Dobrota, 2023; Othman, Ba-Alwi, Alsohybe, & Al-Hashida, 2018; Saranya, Sridevi, Deisy, Chung, & Khan, 2020).

The aim of this work is to design alert correlation model for Improving performance of network intrusion detection based on hybrid machine learning techniques. It will determine the optimum features based on hybrid feature selection techniques, enhance the structural based alert correlation model using unsupervised machine learning techniques and enhance the causal-based alert correlation model using supervised machine learning techniques.

Literature Review

The research(Mbugua, Thiga, & Siror, 2019)a comparative analysis on performance of three different ensemble methods, bagging, boosting and stacking is performed in order to determine the algorithm with high detection accuracy and low false positive rate. Three different experiments on NSL KDD data set are conducted and their performance evaluated based on accuracy, false alarms and computation time. The overall performance of the different types of classifiers used proved that ensemble machine learning classifiers outperformed the single classifiers with high detection accuracy and low false rates.

A new feature selection model (Chahira, 2020)proposed is based on hybrid feature selection techniques (information gain, correlation, chi squere and gain ratio) and Principal Component Analysis (PCA) for feature reduction. This study employed data mining and machine learning techniques on NSL KDD dataset in order to explore significant features in detecting network intrusions. The experimental results showed that the proposed model improves the detection rates and also speed up the detection process.

Theresearch(Chahira & Kiruki, 2022)compares four unsupervised learning algorithms namely Self-organizing maps (SOM), K-means, Expectation and Maximization (EM) and Fuzzy C-means (FCM) to select the best cluster algorithm based on Clustering Accuracy Rate (CAR), Clustering Error (CE) and processing time. The result inferred that the proposed model based on hybrid feature selection, PCA and EM is effective in terms of Clustering Accuracy Rate (CAR) and processing time for The NSL-KDD Dataset

Methodology

This research addresses the issues of improving the quality of alerts that are generated by multiple NIDSs and recognizing the attack strategy from the unrelated alerts. It is executed through a series of experiments and testing to achieve the goal of objectives of the research. This approach is preferred as the main method due to certain characteristics, such as performance measures, dataset evaluations and the usability of the results.

Proposed Hybrid-Based Alert Correlation Model

The five processing levels includes.

a) Feature selection Extracts the optimum features from synthetic dataset based on ensemble feature selection methods

b) Dimension Reduction uses PCA to reduce the dimensionality of the alerts for optimal correlation performance.

c) Unsupervised Learning Algorithm clusters alerts into groups/attack steps to discover the structural correlation among the alerts.

d) Post-Clustering Algorithms improve the quality of alerts by filtering out the unwanted low quality alerts (redundant, false positives and low-risk alerts).

e) Ensemble Supervised Learning Algorithm classifies alerts into classes/attack stages to discover the causal correlation among the alerts.

f) Statistical Correlation Tests calculate the strength of dependencies among the alerts attributes to discover the statistical correlation,

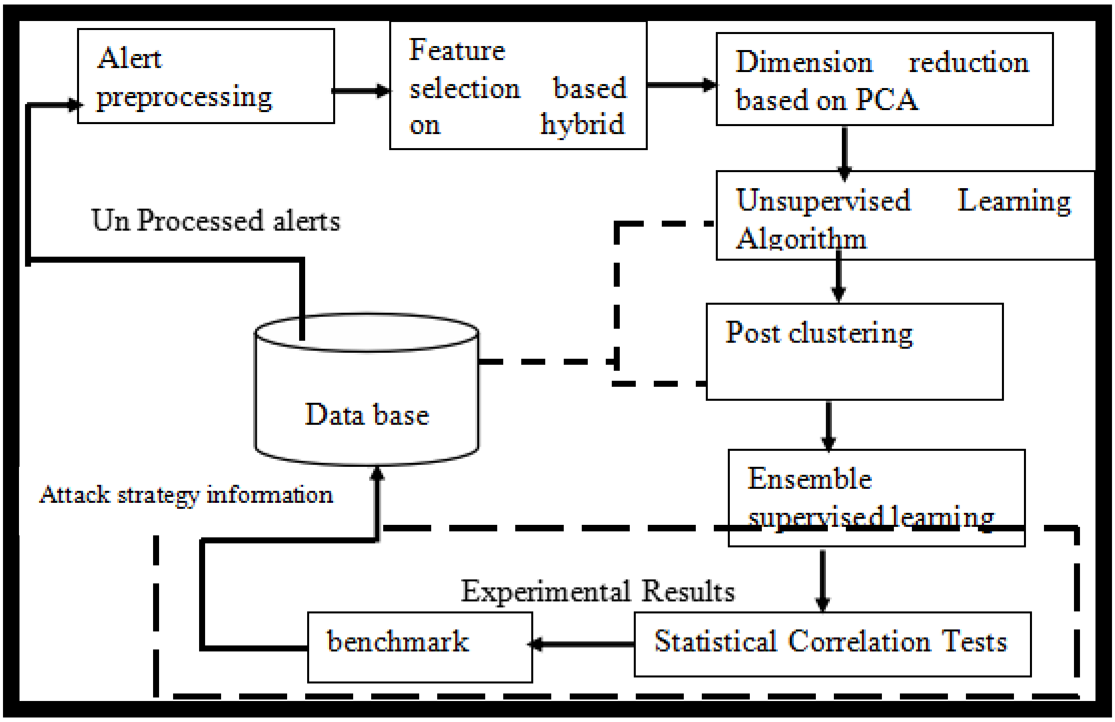

Alert preprocessing
Feature selection based on hybrid
Dimension reduction based on PCA
Unsupervised Learning Algorithm
Un Processed alerts
Post clustering
Data base
Ensemble supervised learning
Attack strategy information
Experimental Results
benchmark
Statistical Correlation Tests

Figure 1: Hybrid-Based Alert Correlation Model

Step 1 **Ensemble-based Multi-Filter Feature Selection (EMFFS) Method**

In this phase, irrelevant and less important features are removed. An ensemble for feature evaluation and feature selection algorithms were invoked to select the set of relevant features. a novel feature selection model is proposed based on hybridizing feature selection techniques (information gain, correlation feature selection and chi square). The experiment, select attribute set based on the repetition of attribute from four scheme. Existing FS that are employed in experiments are 1) Correlation Feature Selection (CFS) based evaluator with Best-first searching method, 2) Information Gain (IG) based Attributes Evaluator with ranker searching method, and 3) Chi Squared Eval and Ranker searching method we obtained

Each algorithm evaluated each class dependent dataset created resulted in a relevant set of features for each particular class. The researcher considered only features that are selected by ten folds (like., k = 10). On the other hand, features that not selected by any algorithm were irrelevant and removed from the list. Output of this phase is a reduced set of common relevant features that were ranked by its relevance value for each attack class.

In the proposed model, these algorithms select the best features set for all attack types in NSL KDD dataset (DOS, PROBE, R2L, U2R, and NORMAL. NSL-KDD, 2014 which contains simulated attack scenarios in a protected environment an off-site server. KDD"99 testing set includes 37 attack types that are included in the testing set. The optimum features selected using the hybrid feature selection technique include: duration, src bytes, dst bytes, logged_in, same_srv_rate, diff_srv_rate, dst_host_count, dst_host_count, dst_host_srv, diff_host_rate, dst_host_srv_rerror_rate. Protocal_type, service, attck. Detailed experiment process and results are disscussed in (Chahira, 2020)

Step 2 Enhanced Structural-Based Alert Correlation Method

The detection component of NIDSs generates a massive amount of alerts and can overwhelm the security experts. An automated and intelligent clustering system is important to reveal their structural correlation by grouping alerts with common attributes. The aim of this objective is to enhance the Structural-based AC model using machine learning technique to improve the quality of alerts and identify attack strategy. A novel hybrid clustering model is developed based on normalization, discretization and Improved Unit Range (IUR) technique to preprocess the dataset, EMFFS, Principal Component Analysis (PCA), SAC and proposed Post-Clustering algorithms is implemented to reduce the alerts dimensionality and optimize the performance and unsupervised learning algorithm to aggregate similar alerts and to reduce the number of alerts. In the proposed model the performance of various unsupervised learning techniques like Self-organizing maps (SOM), Expectation Maximization, K-means, hybrid clustering and Fuzzy c-means (FCM) is compared. The output are comtained in (Chahira & Kiruki, 2022)

Mode	FCM				K Means				SOM				EM			
	CE	ER	AR	TI	CE	ER	AR	TI	CE	ER	AR	TI	CE	ER	AR	TI
HFS	74	17.5	82.6	1.3	57	13.4	86.6	4.4	135	31.8	68.2	4.2	45	10.6	89.4	1.9
PCA	133	31.3	68.6	3.6	141	33.3	66.2	5.2	170	40.1	60.0	6.5	86	20.3	79.7	2.7
IPCA	67	15.8	84.2	4.8	46	10.9	89.2	6.2	112	26.4	73.6	7.4	41	9.7	90.3	4.6

Figure 2: Clustering Performance based on Self-organizing maps (SOM), Expectation Maximization, K-means and Fuzzy c-means (FCM) The result inferred that the proposed model based on hybrid feature selection, PCA and EM is effective in terms of clustering accuracy and processing time for this dataset.

Step 3 Enhanced causal-based alert correlation model.

In the third phase, the output from the second phase which is the results from the hybrid clustering model (PCA and EM) is fed as input to the Multiple IDS Unit (MIU), and the output is the local decision (yi) derived from running different learning algorithms on the same data set. This section has five IDSs, each utilizing a unique algorithm is used independently for detecting a certain class of attack with improved accuracy, while performing moderately on the other classes. The five different types of IDS algorithms used are Support Vector Machines (SVM), IBK, Random Forest, J48, and Bayes Net and different results obtained and five outputs (local decisions) y1, y2, to y5 are obtained.The output from each IDS in MIU, considered as local decision (yi), is passed onto the multi classifier component based on majority voting rule and makes the final decision. Each classifier has a weight to denote the contributions of the classifier to the voting system. For each class to be identified, a weighted sum of base learners can be calculated. The output from each classifier is taken to the decision unit, and the global decision is taken based on the majority voting rule. If majority outputs from the MIU unit suggest Attack, then the decision unit decides that the input traffic is of ATTACK type; else it is NOT ATTACK. Detailed experiment process and results are disscussed in (Mbugua et al., 2019)

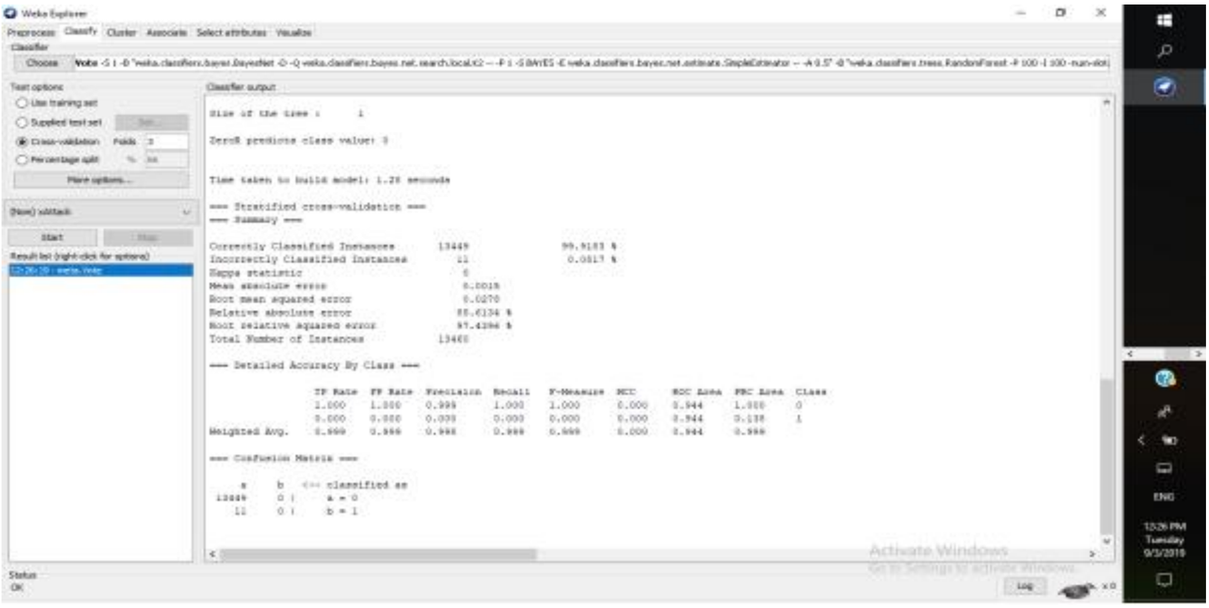
Experimentation, Results and Discussion

In the experiment, we apply full dataset as training set and 10-fold cross validation for the testing purposes. The available dataset is randomly subdivided into 10 equal disjoint subsets and one of them is used as the test set and the remaining sets are used for building the classifier. In this process, the test subset is used to calculate the output accuracy while the N1 subset is used as a test subset and to find the accuracy for each subset. The process is repeated until each subset is used as test set once and to compute the output accuracy of each subset. The final accuracy of the system is computed based on the accuracy of the entire 10 disjoint subsets.

The experiments will be conducted on MIT Lincoln's Lab's DARPA 2000 Scenario Specific

The performance of the proposed intrusion detection system is evaluated with the help of confusion matrix. The conducted experiments will be evaluated according to four performance measures which are defined below:

i. TPR: TP/(TP+FN), also known as detection rate (DR) or sensitivity or recall.
ii. The False Alarm Rate (FAR) is the rate of the misclassified to classified records,
iii. Precision (P): TP/(TP+FP) is defined as the proportion of the true positives against all the positive results.
iv. Total Accuracy (TA): (TP+TN)/(TP+TN+FP+FN) is the proportion of true results (both true positives and true negatives) in the population.
v. F-measure: 2PR/(P+R) is the harmonic mean of precision and recall.



Vote -S 1 -B "weka.classifiers.bayes.BayesNet -D -Q weka.classifiers.bayes.net.search.local.K2 -- -P 1 -S BAYES -E weka.classifiers.bayes.net.estimate.SimpleEstimator -- -A 0.5" -B "weka.classifiers.trees.RandomForest -P 100 -I 100 -num-slots

Folds 3

(Nom) isAttack

```
Size of the tree :      1

ZeroR predicts class value: 0


Time taken to build model: 1.28 seconds

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances       13449              99.9183 %
Incorrectly Classified Instances        11               0.0817 %
Kappa statistic                          0
Mean absolute error                      0.0015
Root mean squared error                  0.0270
Relative absolute error                 88.6134 %
Root relative squared error             97.4296 %
Total Number of Instances            13460

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1.000    1.000    0.999      1.000    1.000      0.000    0.944     1.000     0
                 0.000    0.000    0.000      0.000    0.000      0.000    0.944     0.138     1
Weighted Avg.    0.999    0.999    0.998      0.999    0.999      0.000    0.944     0.999

=== Confusion Matrix ===

     a     b   <-- classified as
 13449     0 |     a = 0
    11     0 |     b = 1
```

Figure 3: Performance of Proposed Hybrid-Based Alert Correlation Model

The value of TP, P, R, FM and ROC are 0.998, 0.99, 0.99 and 0.94 that close to '1' indicates excellent performance and below '0.5' indicates average or bad performance. A smaller value of FP (close to zero) shows good performance since the amount of false classification is very small. The time taken to build the model is only 1340.7seconds.

Conclusion

The approach based on classifier combination achieve effective attack detection as the combination of multiple evidences usually exhibits higher accuracies, like. lower false positives, than individual decisions. In addition, the generalization capabilities of pattern recognition algorithms allow for the detection of novel attacks that is not provided by rule-based signatures.

References

Albasheer, H., Siraj, M. M., Mubarakali, A., Tayfour, O. E., Salih, S., Hamdan, M., … Kamarudeen, S. (2022). Cyber-Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey. *Sensors*, *22*(4), 1–15. https://doi.org/10.3390/s22041494

Alkhpor, H. K., & Alserhani, F. M. (2023). Collaborative Federated Learning-Based Model for Alert Correlation and Attack Scenario Recognition. *Electronics (Switzerland)*, *12*(21). https://doi.org/10.3390/electronics12214509

Alsoufi, M. A., Razak, S., Siraj, M. M., Ali, A., Nasser, M., & Abdo, S. (2021). Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey. *Lecture Notes on Data Engineering and Communications Technologies*, *72*(May), 659–675. https://doi.org/10.1007/978-3-030-70713-2_60

Boero, L., Cello, M., Marchese, M., Mariconti, E., Naqash, T., & Zappatore, S. (2017). Statistical fingerprint-based intrusion detection system (SF-IDS). *International Journal of Communication Systems*, *30*(10). https://doi.org/10.1002/dac.3225

Chahira, J. M. (2020). Model for Intrusion Detection Based on Hybrid Feature Selection Techniques. *International Journal of Computer Applications Technology and Research*, *09*(03), 115–124. https://doi.org/10.7753/ijcatr0903.1005

Chahira, J. M., & Kiruki, J. K. (2022). Model for Enhancing Performance of Network Intrusion Detection based on Hybrid Feature Selection and Unsupervised Learning Techniques. *International Journal of Computer Applications Technology and Research*, *11*(08), 341–350. https://doi.org/10.7753/ijcatr1108.1008

Diehl, M., & Ramirez-Amaro, K. (2023). A causal-based approach to explain, predict and prevent failures in robotic tasks. *Robotics and Autonomous Systems*, *162*, 104376. https://doi.org/10.1016/j.robot.2023.104376

Ho, H., Hua, W., Siraj, M., & Din, M. M. (2017). Integration of PSO and K-Means Clustering Algorithm for Structural-Based Alert Correlation Model. *International Journal of Innovative Computing*, *7*(2), 34–39.

Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395–9409. https://doi.org/10.1016/j.aej.2022.02.063

Kinanu Kiruki, J., Muchiri Muketha, G., & Kamau, G. (2023). a Novel Alert Correlation Technique for Filtering Network Attacks. *International Journal of Network Security & Its Applications*, *15*(03), 33–47. https://doi.org/10.5121/ijnsa.2023.15303

Kiruki, J. K., Muketha, G. M., & Kamau, G. (2023). Metrics for Evaluating Alerts in Intrusion Detection Systems. *International Journal of Network Security & Its Applications*, *15*(01), 15–37. https://doi.org/10.5121/ijnsa.2023.15102

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences (Switzerland)*, *9*(20). https://doi.org/10.3390/app9204396

Makhlouf, K., Zhioua, S., & Palamidessi, C. (2020). *Survey on Causal-based Machine Learning Fairness Notions*. *Proceedings of ACM Conference (Conference'17)* (Vol. 1). Association forComputing Machinery. Retrieved from http://arxiv.org/abs/2010.09553

Mari, A. G., Zinca, D., & Dobrota, V. (2023). Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network. *Sensors*, *23*(3). https://doi.org/10.3390/s23031315

Mbugua, J., Thiga, M., & Siror, J. (2019). A Comparative Analysis of Standard and Ensemble Classifiers on Intrusion Detection System. *International Journal of Computer Applications Technology and Research*, *8*(4), 107–115. https://doi.org/10.7753/ijcatr0804.1005

Othman, S. M., Ba-Alwi, F. M., Alsohybe, N. T., & Al-Hashida, A. Y. (2018). Intrusion detection model using machine learning algorithm on Big Data environment. *Journal of Big Data*, *5*(1). https://doi.org/10.1186/s40537-018-0145-4

Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Computer Science*, *171*(2019), 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133

Wang, L., Adiga, A., Chen, J., Sadilek, A., Venkatramanan, S., & Marathe, M. (2022). CausalGNN: Causal-Based Graph Neural Networks for Spatio-Temporal Epidemic

Forecasting. *Proceedings of the 36th AAAI Conference on Artificial Intelligence, AAAI 2022*, *36*(Cdc), 12191–12199. https://doi.org/10.1609/aaai.v36i11.21479

Wu, M., & Moon, Y. (2019). Alert Correlation for Cyber-Manufacturing Intrusion Detection. *Procedia Manufacturing*, *34*, 820–831. https://doi.org/10.1016/j.promfg.2019.06.197

Yu, M., & Zhang, X. (2023). AlertInsight: Mining Multiple Correlation For Alert Reduction. *Computer Systems Science and Engineering*, *46*(2), 2447–2469. https://doi.org/10.32604/csse.2023.037506