International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 185 – 201, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1020

Blockchain-Based Secure Authentication Framework for Decentralized Internet-of-Things (IoT) Devices in Smart Grid Network Infrastructures

Martha Masunda
Department of Electrical Engineering and Computer Science
University of New Haven
USA

Abstract: The increasing proliferation of Internet-of-Things (IoT) devices in modern smart grid infrastructures presents both transformative potential and unprecedented security challenges. As these devices play critical roles in energy distribution, real-time monitoring, and demand response, ensuring secure authentication and data integrity across decentralized and heterogeneous networks becomes imperative. Traditional centralized authentication models suffer from scalability issues, single points of failure, and limited resilience against sophisticated cyber-attacks. In this context, blockchain technology emerges as a compelling solution to establish trust, transparency, and tamper-resistance in smart grid communication systems. This study proposes a blockchain-based secure authentication framework specifically designed for decentralized IoT environments within smart grid networks. The framework integrates lightweight cryptographic techniques with a permissioned blockchain ledger to manage identity validation, access control, and trust propagation among interconnected devices. By leveraging smart contracts, the system enables autonomous device registration, mutual authentication, and secure session key establishment without dependence on centralized authorities. Furthermore, the model employs a hierarchical consensus protocol optimized for energy efficiency and latency, addressing the computational limitations of resource-constrained IoT nodes. Performance evaluations using simulation environments demonstrate enhanced resistance against replay attacks, Sybil attacks, and man-in-the-middle threats, while maintaining minimal overhead in authentication time and energy consumption. The proposed framework offers a scalable and resilient solution to secure large-scale IoT deployments in critical smart grid applications. By decentralizing trust and automating authentication processes, this blockchain-enabled architecture paves the way for next-generation, cyber-resilient energy systems.
Keywords: Blockchain, IoT Authentication, Smart Grid Security, Decentralized Networks, Lightweight Cryptography, Cyber-Resilience

1. INTRODUCTION

1.1 Background and Context

Smart grids represent a transformative advancement in modern energy infrastructure, offering a digitized and dynamic approach to electricity generation, distribution, and consumption. Unlike traditional grids, which operated in a largely unidirectional and passive manner, smart grids employ two-way communication systems, real-time monitoring, and automated control mechanisms to manage energy flow more efficiently and sustainably. These capabilities are particularly vital for integrating renewable energy sources such as wind and solar into the national grid, ensuring reliability despite their inherent intermittency [1]. However, this shift to digital infrastructure has not come without new complications. The increasing interconnection of devices, sensors, and control systems has significantly expanded the attack surface for cyber threats, making security a cornerstone of smart grid resilience [2].

From supervisory control and data acquisition (SCADA) systems to Internet of Things (IoT)-enabled smart meters, smart grids rely on complex, distributed technologies. While these tools improve energy efficiency and support demand-side management, they also create vulnerabilities that can be exploited by malicious actors. As shown in Figure 1, the architecture of a typical smart grid includes multiple access points, many of which lack robust encryption and secure authentication protocols [3].

Moreover, the traditional cybersecurity frameworks designed for centralized systems are not well-suited for distributed grid networks. In particular, challenges around data integrity, trust, and latency have exposed the inadequacies of these legacy models. As energy systems continue to evolve, new paradigms must be explored to address these issues while maintaining interoperability and performance. Table 1 summarizes common vulnerabilities identified across various smart grid components, further underscoring the need for innovative solutions [4]. This context sets the stage for understanding the critical security challenges embedded in smart grid ecosystems, which are explored in the next subsection.

1.2 The Security Challenge in Smart Grids

The digitization of power systems has inadvertently exposed smart grids to a spectrum of cyber-physical threats that traditional electrical infrastructures were not designed to handle. These threats range from data tampering and eavesdropping to more advanced attacks like false data injection (FDI), denial of service (DoS), and advanced persistent threats (APTs) [5]. In smart grid environments, where real-time data exchange governs critical decisions such

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 185 – 201, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1020

as load balancing, demand forecasting, and fault detection such breaches can cause cascading failures with national consequences.

Notably, decentralized control elements like smart meters and distributed energy resources (DERs) often lack the computational capacity to support advanced encryption, making them easy targets [6]. Many devices in the field still use outdated firmware, suffer from poor patch management, and depend on unsecured communication protocols such as Modbus or DNP3. This lack of uniform security standards across vendors and geographic regions exacerbates the fragmentation problem.

Moreover, identity spoofing and unauthorized access to control centers can enable adversaries to manipulate grid operations. Cyber intrusions into substation controllers or phasor measurement units (PMUs) have demonstrated the feasibility of such attacks in controlled environments [7]. Despite widespread awareness, mitigation efforts have often been reactive rather than proactive, relying on intrusion detection systems that struggle with high false positive rates.

As indicated by trends in historical breach data and simulations, these vulnerabilities are not hypothetical but demonstrable in pilot studies and operational settings [8]. This reality necessitates a new paradigm one capable of ensuring transparency, immutability, and distributed trust which blockchain technology potentially offers.

1.3 Motivation for Blockchain Integration

Blockchain, a decentralized and tamper-resistant ledger technology, has gained traction as a potential solution to many of the aforementioned smart grid vulnerabilities. Its architecture inherently supports features such as data immutability, traceability, and trustless verification traits that align well with the operational demands of a distributed energy system [9]. By recording each transaction in a cryptographically linked chain of blocks, blockchain eliminates the need for centralized data authorities, thereby reducing single points of failure.

In smart grids, blockchain can enhance security in areas such as peer-to-peer energy trading, automated demand response, and secure meter data aggregation [10]. For instance, smart contracts self-executing scripts embedded within the blockchain can be employed to enforce predefined rules among grid participants without external enforcement mechanisms. This is particularly useful in managing microgrids and DERs, where the volume of transactions is high and latency-sensitive [11].

Moreover, blockchain can support decentralized identity management for grid components, ensuring that only verified devices participate in the communication network. This capability helps mitigate spoofing and unauthorized access risks that plague traditional systems. As seen in experimental deployments, blockchain can enable fine-grained access control and secure audit trails that are resilient to tampering or deletion [12].

While scalability and energy consumption concerns persist, especially with early blockchain models, newer consensus algorithms such as Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) offer viable pathways for integration into resource-constrained environments like smart grids [13]. These foundational ideas will lead into a deeper exploration of how traditional security models fall short and how blockchain-based architectures can fill those critical gaps.

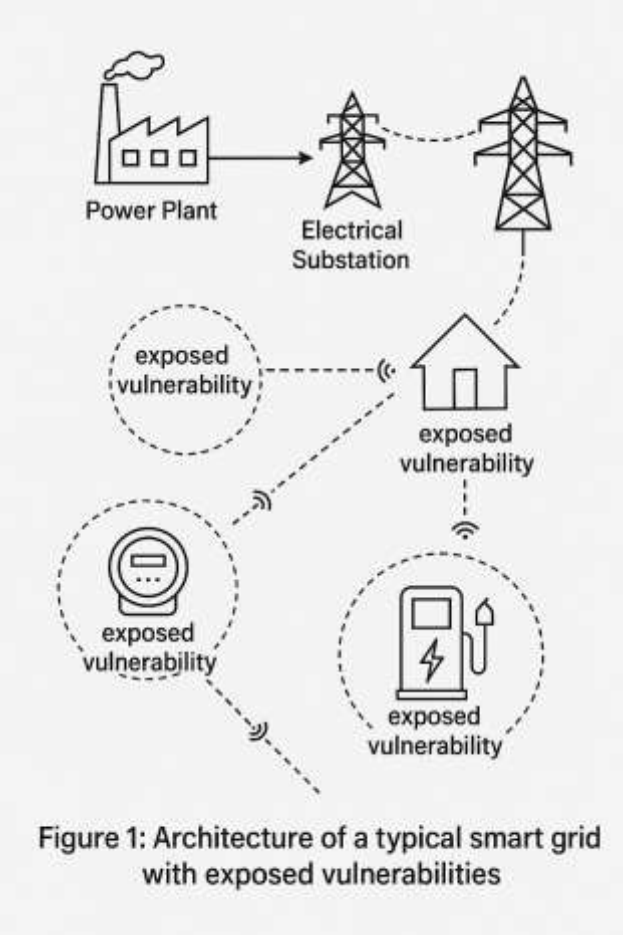

Figure 1: Architecture of a typical smart grid with exposed vulnerabilities.

Table 1: Common Cybersecurity Vulnerabilities in Smart Grid Subsystems

Subsystem Layer	Component	Vulnerability	Impact
Perception Layer	Smart Meters, Sensors, RTUs	Physical tampering, firmware manipulation	False data injection, energy theft
Communicatio	Zigbee,	Unencrypted	Eavesdropping

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 185 – 201, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1020

Subsystem Layer	Component	Vulnerability	Impact
n Layer	LoRaWAN, PLC, GPRS	transmission, weak authentication, jamming attacks	, denial of service, impersonation
Network Layer	Routers, Gateways, Switches	IP spoofing, routing attacks, ARP poisoning	Traffic redirection, data loss
Transport Layer	TLS/DTLS Protocols	Outdated encryption algorithms, key leakage	Session hijacking, message interception
Application Layer	SCADA, EMS, DMS, Web Dashboards	Input injection, session hijacking, insecure APIs	Remote control manipulation, unauthorized access
Data Management Layer	Cloud storage, databases	Insecure database interfaces, weak access control	Data breaches, configuration leakage
Control Layer	PMUs, Substation Controllers	Command spoofing, delay injection	Grid instability, blackout risk
Third-Party Systems	Vendor APIs, Mobile Apps	Hardcoded credentials, lack of encryption	Supply chain compromise, unauthorized access

2. SMART GRID IOT ARCHITECTURE AND VULNERABILITY LANDSCAPE

2.1 Architecture of Smart Grid-Integrated IoT Systems

The architecture of smart grid-integrated Internet of Things (IoT) systems is inherently layered, incorporating physical, communication, and application tiers. At the base, the perception or physical layer includes sensors, actuators, and smart meters that capture environmental parameters such as voltage, frequency, and power usage [5]. These edge devices interface directly with grid infrastructure and consumer premises, forming the foundational layer for data acquisition and local actuation. These components transmit readings upward to communication gateways, forming the backbone for further processing and decision-making.

The intermediate layer, often termed the network or communication layer, manages the transmission of data between IoT devices and central control units or cloud platforms [6]. It utilizes a mix of wireless technologies (e.g., Zigbee, LoRaWAN, LTE) and wired protocols (e.g., Ethernet, Power Line Communication), depending on application requirements and physical constraints. As shown in Figure 1, data generated by field-level IoT nodes flows hierarchically through regional concentrators toward centralized control centers or distributed edge computing hubs for analysis [7].

The application layer encompasses energy management systems (EMS), distribution management systems (DMS), and other analytics platforms that interpret sensor data and execute control logic [8]. Services at this level enable functionalities like dynamic pricing, demand response, and outage detection. Each layer interfaces through open or proprietary APIs, which increases integration flexibility but also raises compatibility and security challenges.

This layered architecture introduces benefits such as scalability, modularity, and flexibility. However, it also amplifies the attack surface, especially due to the heterogeneity of devices and standards [9]. Weak authentication at lower layers or misconfigured APIs at the top layer can allow unauthorized access and data tampering. As smart grid deployments expand in scale and complexity, securing data integrity and trust among components becomes critical for stable operations.

The architectural structure highlights the interconnectedness and reliance on secure communications, making it imperative to understand the communication models and their respective security implications as discussed in the next subsection.

2.2 Communication Models and Protocol Stacks

Smart grid IoT systems rely on layered communication models to facilitate real-time data exchange between devices, applications, and central servers. Typically aligned with the Open Systems Interconnection (OSI) model, these communication frameworks ensure interoperability across heterogeneous hardware and software systems [10]. The stack often includes physical and data link layers (e.g., IEEE 802.15.4, GPRS), network protocols like IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN), and application layer protocols such as MQTT, CoAP, and DLMS/COSEM [11].

Device-to-device (D2D), device-to-gateway, and device-to-cloud communication models are prominent in smart grid networks. For instance, a smart meter might send consumption data to a local gateway, which then relays it to a central data center or edge server. Similarly, control signals from the cloud can be dispatched through multiple hops to the appropriate field devices [12].

Each communication model introduces specific latency, bandwidth, and security trade-offs. Low-power protocols like Zigbee and LoRa are energy-efficient but vulnerable to

eavesdropping and jamming due to weak encryption [13]. Conversely, more secure options like LTE or private 5G offer robust transmission but may be cost-prohibitive for widespread rural deployment.

Protocol stack diversity, while beneficial for functionality, also creates security challenges due to inconsistent implementation of cryptographic protections across layers. The absence of end-to-end encryption, integrity verification, and proper authentication in many legacy protocols leaves them exposed to man-in-the-middle attacks and replay exploits [14]. These deficiencies are particularly critical in real-time control scenarios, where delayed or manipulated data can disrupt grid stability.

To better assess how these gaps translate into tangible risks, the following subsection outlines the core vulnerabilities and threat vectors prevalent in current smart grid IoT ecosystems.

2.3 Vulnerabilities and Threat Vectors

The convergence of IoT with smart grid infrastructure introduces a spectrum of vulnerabilities across all layers of the system architecture. At the perception layer, edge devices like smart meters, sensors, and relays are often deployed in physically accessible locations, making them susceptible to tampering, cloning, or malicious firmware injection [15]. These endpoints frequently lack tamper-proof hardware or secure boot mechanisms, allowing adversaries to alter data or bypass authentication.

At the communication layer, unencrypted channels and outdated protocols expose networks to interception, spoofing, and denial-of-service (DoS) attacks. For example, weak key management or absent mutual authentication between gateways and end devices allows attackers to impersonate legitimate nodes and disrupt network operations [16]. As shown in Table 1, these attacks are often categorized by layer and impact, ranging from privacy breaches to grid destabilization [17].

Moving up to the application layer, web-based dashboards and control interfaces used by operators may lack adequate access control or input validation. This opens the door for SQL injection, cross-site scripting (XSS), or remote code execution attacks. Inadequate logging and forensic capabilities further limit the system's ability to detect and respond to such breaches in real-time [18].

Another critical vulnerability is the lack of centralized oversight in distributed deployments, which leads to configuration drift, outdated firmware, and inconsistent security policies across devices [19]. This fragmentation increases the probability of zero-day exploits being missed or improperly mitigated. Furthermore, the increasing use of third-party cloud services without end-to-end data protection further exposes sensitive operational data to unauthorized entities.

Given these multi-layered vulnerabilities, it becomes evident that existing centralized security approaches are inadequate for the demands of modern smart grid IoT systems. The next section introduces blockchain as a viable architecture to embed distributed trust and immutable auditing, thereby addressing these shortcomings holistically.

3. BLOCKCHAIN TECHNOLOGIES AND SECURITY PRINCIPLES

3.1 Core Blockchain Features and Components

Blockchain technology, originally introduced to support decentralized cryptocurrencies, has evolved into a multi-purpose architecture capable of addressing various trust and security challenges in distributed systems such as smart grid-integrated IoT environments. At its core, a blockchain consists of a distributed ledger, cryptographic hash functions, consensus algorithms, and immutable data structures. These elements collectively ensure that all participating nodes share a synchronized, tamper-proof history of transactions or events [9].

The distributed ledger enables every participating node to maintain a full or partial copy of the blockchain, eliminating the need for centralized authorities and reducing the risk of single-point failures. Hash functions, particularly SHA-256, serve to secure each block by generating unique identifiers based on its contents, ensuring that even the smallest modification to a block will result in a completely different hash [10].

Each block in the chain contains a timestamp, a cryptographic hash of the previous block, and a list of validated transactions. These blocks are appended in chronological order, with consensus protocols validating their authenticity before inclusion. This chaining process creates an audit trail that is resilient to tampering and revision [11].

Moreover, digital signatures and public key infrastructure (PKI) support authentication of transaction initiators, allowing only verified devices or entities to append data. As shown in Figure 2, the blockchain layer stack for IoT applications incorporates these cryptographic tools to facilitate secure authentication and communication between edge devices, gateways, and central control systems [12].

By leveraging these core components, blockchain offers a robust foundation for secure, transparent, and decentralized interactions features that align closely with the needs of smart grids. This section sets the stage for understanding how different blockchain types affect deployment strategies in such environments, as explored next.

3.2 Permissioned vs. Permissionless Blockchains in IoT

In the context of IoT-integrated smart grids, the selection between permissioned and permissionless blockchain models significantly influences the system's scalability, trust management, and performance. Permissionless blockchains such as Bitcoin and Ethereum allow open participation,

meaning any node can read, write, or validate transactions without prior approval. These systems are highly decentralized and promote transparency, but often suffer from latency and high computational demands due to resource-intensive consensus mechanisms like Proof of Work (PoW) [13].

While suitable for trustless environments, permissionless systems may not align with the operational constraints of smart grids, where real-time responsiveness and lightweight computation are essential. Moreover, the anonymous participation in such networks introduces risks in critical infrastructure contexts where accountability and traceability are paramount [14].

Conversely, permissioned blockchains restrict participation to vetted entities, such as utility companies, device manufacturers, or regulatory bodies. These networks typically employ efficient consensus algorithms like Practical Byzantine Fault Tolerance (PBFT), Raft, or Proof of Authority (PoA), which provide faster transaction finality and lower energy consumption [15]. They also allow granular access control, making them ideal for environments where identity verification and policy compliance are critical.

For example, a permissioned blockchain can be designed to allow only certified grid components to exchange encrypted control signals or perform energy trading. The predefined governance models ensure accountability and facilitate regulatory audits, essential in power systems [16].

In smart grid applications, permissioned blockchains provide a middle ground between decentralization and operational control. Their structure supports secure collaboration among trusted stakeholders without compromising performance, thus paving the way for implementing more complex logic via smart contracts and consensus models, as detailed in the next section.

3.3 Smart Contracts, Consensus Mechanisms, and Immutability

Smart contracts are self-executing code embedded within blockchain platforms, designed to automatically enforce predefined rules once specified conditions are met. In smart grid IoT systems, these programmable contracts enable dynamic functions such as automated billing, decentralized energy trading, and anomaly detection without relying on central authorities [17]. For instance, a smart contract can autonomously transfer credits to a prosumer when energy is injected into the grid beyond their consumption threshold.

These contracts operate in tandem with consensus mechanisms, which determine how nodes in the blockchain network reach agreement on the legitimacy of transactions. Traditional mechanisms like Proof of Work (PoW) ensure robustness through computational difficulty but are inefficient for IoT environments due to power and latency limitations. Emerging alternatives such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) offer faster finality and energy efficiency, making them more compatible with constrained edge devices [18].

PBFT, for example, is particularly suitable for permissioned blockchains in smart grids, where known validator nodes can reach consensus through message-passing rather than computation-intensive processes. This approach minimizes the overhead and allows deterministic confirmation times—crucial for time-sensitive grid operations like frequency regulation and load balancing [19].

Immutability, a key attribute of blockchain, ensures that once data is recorded and confirmed, it cannot be altered without invalidating the entire chain. This characteristic is vital for audit trails in energy consumption, transaction history, and device authentication logs. Should a fault or breach occur, immutable records enable retrospective forensics to identify the source, scope, and nature of the anomaly.

As illustrated in Figure 2, the blockchain layer stack tailored for IoT incorporates identity verification, data validation, contract execution, and consensus each interacting with specific smart grid components. These layers jointly facilitate secure peer authentication, event logging, and tamper-proof control signals across the grid's cyber-physical infrastructure.

Taken together, smart contracts, efficient consensus protocols, and immutable ledgers provide a cohesive framework to meet the security, autonomy, and auditability demands of future smart grid ecosystems. The next section will demonstrate how these elements can be operationalized to address specific authentication requirements in real-world deployments.

Figure 2: Blockchain layer stack tailored for IoT authentication flows.

4. AUTHENTICATION MECHANISMS IN IOT: A REVIEW OF TRADITIONAL AND EMERGING APPROACHES

4.1 Centralized Authentication Protocols (e.g., OAuth, TLS)

Centralized authentication protocols form the cornerstone of traditional cybersecurity architectures, especially in client-server models. Protocols like OAuth 2.0 and Transport Layer Security (TLS) are widely adopted for securing communication and authenticating user identities. OAuth enables token-based delegated authorization, allowing third-party services to access user resources without revealing credentials [14]. It is particularly prevalent in web-based applications and has been adapted to support certain IoT use cases where centralized identity providers are available.

TLS, on the other hand, offers end-to-end encryption and certificate-based mutual authentication, protecting the integrity and confidentiality of data during transmission. Its application in smart grid environments includes securing communication between control centers and field devices, as well as protecting APIs in cloud-based energy management systems [15]. These protocols are typically deployed within a Public Key Infrastructure (PKI), which maintains digital certificates issued by centralized Certificate Authorities (CAs).

Despite their widespread use, centralized authentication systems present inherent risks. The reliance on a single point of trust the identity provider or CA means that any compromise at that node can expose the entire network to unauthorized access or data leakage. Furthermore, scalability becomes a bottleneck when dealing with the millions of low-power IoT devices that make up modern smart grid deployments [16].

Additionally, centralized protocols often require persistent internet connectivity and computational resources that many edge devices cannot sustain. These limitations have led researchers to explore alternatives that decentralize trust and improve resilience. As smart grids transition toward distributed topologies, the suitability of centralized authentication frameworks diminishes. This creates a need for more adaptable, decentralized approaches that align better with IoT scalability and fault tolerance, leading to the concepts discussed in the next subsection.

4.2 Decentralized and Federated Authentication in IoT

Decentralized and federated authentication mechanisms aim to address the shortcomings of traditional centralized models by distributing trust across multiple nodes or domains. In decentralized authentication, identity verification is managed by a peer-to-peer framework rather than a central authority, often leveraging blockchain or distributed ledger technologies to ensure integrity and traceability [17]. Each participating device or user maintains a cryptographic key pair and interacts directly with others based on mutual verification, eliminating dependency on a centralized identity provider.

Blockchain-based decentralized identifiers (DIDs) and verifiable credentials have emerged as promising tools in this domain. These mechanisms enable devices to self-certify their identities and interact securely without a centralized intermediary [18]. For instance, in a smart grid setting, substations and smart meters can authenticate one another using blockchain-stored identity proofs, reducing latency and increasing resilience to outages or targeted attacks.

Federated authentication offers a semi-decentralized model wherein multiple trusted domains agree to share identity and access management (IAM) responsibilities. A common example is Security Assertion Markup Language (SAML)-based single sign-on (SSO), where identity is verified by one domain but accepted across others [19]. Though not entirely decentralized, this model reduces the number of authentication steps and allows collaboration across diverse systems, such as utilities, regulatory bodies, and third-party vendors.

While federated models provide enhanced interoperability, they still require a level of inter-domain trust and coordination that may not be practical in highly dynamic IoT ecosystems. In contrast, fully decentralized models excel in scalability and fault tolerance but may face regulatory or governance challenges.

These variations underscore the need for a comparative assessment of authentication frameworks, highlighting how each performs under the demands of a smart grid IoT environment, as examined in the next section.

4.3 Comparative Analysis of Authentication Frameworks

A comprehensive evaluation of authentication frameworks within smart grid IoT environments must consider key operational factors such as latency, scalability, fault tolerance, and the underlying trust model. Centralized frameworks like OAuth and TLS provide strong encryption and access control but struggle with latency and bottlenecks under high-volume, geographically distributed networks [20]. They are dependent on central servers and certificate authorities, which create single points of failure. Additionally, frequent token refresh cycles and the computational burden of mutual TLS authentication can overwhelm constrained edge devices.

Federated authentication frameworks improve on some of these limitations by distributing trust among known entities. While federated models support cross-organizational collaboration and offer streamlined identity management, they still rely on fixed agreements and are vulnerable to trust breaches within any federated node [21]. Their effectiveness diminishes in highly heterogeneous environments where multiple device manufacturers, software vendors, and grid operators must interact seamlessly.

In contrast, decentralized authentication using blockchain introduces a robust model that eliminates central trust anchors. Each device can verify and register identity autonomously, using cryptographic proofs stored on a distributed ledger. This approach enhances fault tolerance and removes dependency on persistent connectivity with a central server [22]. It also allows identity recovery and revocation through consensus-based voting or cryptographic challenges, ensuring that compromised credentials are swiftly addressed without compromising the entire system.

However, decentralized models are not without drawbacks. Initial setup costs, governance models, and the need for lightweight consensus protocols tailored to IoT are challenges that require architectural planning. Still, when designed appropriately, blockchain-based authentication demonstrates superior resilience to man-in-the-middle attacks, certificate spoofing, and insider threats [23].

As shown in Table 2, decentralized methods offer the best scalability and trust decentralization, while centralized models outperform others in deployment simplicity and legacy compatibility. Federated frameworks lie between these extremes, suitable for hybrid deployments.

The synthesis of this comparison informs the development of the proposed blockchain-enabled authentication framework engineered to meet the latency, trust, and decentralization needs of smart grids in the IoT era.

Table 2: Comparative Matrix of Traditional vs. Decentralized Authentication Methods

Criteria	**Centralized (e.g., TLS, OAuth)**	**Federated (e.g., SAML, OpenID)**	**Decentralized (e.g., Blockchain-based)**
Latency	Moderate to High (depends on central server load)	Moderate (improved via trust delegation)	Low (local verification via distributed ledger)
Scalability	Limited (central bottlenecks)	Moderate (bounded by federation size)	High (peer-to-peer trust model scales linearly)
Trust Model	Centralized (reliant on single authority)	Semi-centralized (multiple trusted domains)	Fully decentralized (trust distributed across nodes)
Single Point of Failure	Present (server or CA compromise)	Reduced but still present in identity providers	Absent (ledger replication across nodes)
Identity Revocation	Manual and delayed	Depends on domain cooperation	Immediate and consensus-driven
Auditability	Limited (central logs prone to tampering)	Improved (but centralized storage persists)	Strong (immutable on-chain records)
Energy Efficiency	High for TLS; moderate for OAuth	Moderate (token validation load)	Moderate to High (varies with consensus mechanism)
IoT Compatibility	Poor for constrained devices	Moderate	Good with lightweight protocols (e.g., PBFT, PoA)
Interoperability	Low (vendor-specific)	Moderate (protocol bridging possible)	High (platform-agnostic via open standards)
Privacy Preservation	Low (identity exposed to central authority)	Moderate (data shared across domains)	High (with PETs like ZKPs and ring signatures)

5. PROPOSED BLOCKCHAIN-BASED SECURE AUTHENTICATION FRAMEWORK

5.1 Design Objectives and System Assumptions

The proposed blockchain-based authentication framework is designed to meet the unique operational constraints and security needs of smart grid IoT environments. The primary objectives include scalability to support thousands of distributed devices, resilience against single points of failure, and lightweight implementation compatible with resource-constrained IoT nodes [19]. Furthermore, the system is engineered to ensure decentralized trust management, immutable identity records, and real-time verification with minimal latency overhead.

Assumptions underlying the system's design include the presence of a permissioned blockchain network among grid stakeholders such as utility companies, device vendors, and regulators who act as validator nodes. Each IoT device is assumed to possess a unique identifier and the capability to store lightweight cryptographic keys for public-private operations. We also assume secure channels exist for the initial provisioning of credentials and for blockchain nodes to synchronize periodically without exhaustive bandwidth consumption [20].

The architecture presumes that smart meters, relay nodes, and substations communicate via trusted gateways that interface with blockchain validators. These gateways serve to aggregate data, broadcast identity proofs, and facilitate local verification, offloading heavy computations from end devices. Figure 3 illustrates the high-level system design, showing the interactions between IoT devices, blockchain nodes, and the trust-verifying entities.

Additionally, to enable on-chain and off-chain operations, we assume the existence of lightweight APIs between smart contracts and application-layer services. This ensures the seamless integration of legacy utility applications into the decentralized authentication workflow. Overall, the proposed framework is developed to bridge operational efficiency with cryptographic security guarantees in distributed smart grid infrastructures, setting the foundation for the identity registration process detailed next.

5.2 Identity Management and Key Registration Process

Identity management in the proposed framework begins with a trusted initialization phase, during which each IoT device is registered by an authorized entity, such as a utility provider or device manufacturer. During this process, the device generates a unique public-private key pair and receives a digital certificate signed by the registering authority [21]. The public key, certificate, and device metadata (e.g., model, firmware version) are stored immutably on the blockchain ledger. The corresponding private key is securely stored within the device's trusted execution environment.

The key registration transaction is handled by a blockchain smart contract, which verifies the authenticity of the registering authority and records the device credentials on-chain. These credentials form the basis for future mutual authentication and trust propagation. Once registered, the device becomes discoverable within the blockchain network, and its identity can be queried and verified in real-time by any authorized party [22].

This approach allows for decentralized identity verification, eliminating the need for repeated contact with a central certificate authority during each authentication session. Revocation is handled through a separate smart contract that allows stakeholders to flag compromised or decommissioned devices. Once flagged, the device's public key is marked inactive and excluded from trust computations in future sessions.

The design also accounts for periodic key rotation and re-certification. Devices can initiate re-keying operations through secure gateway interactions, ensuring long-term cryptographic strength and compliance with evolving security standards. Table 3 provides a mapping of each registration step to specific blockchain protocol layers involved in the execution.

This process sets up the foundational trust anchors for all subsequent authentication events, enabling robust integration with smart contracts and consensus-driven enforcement mechanisms as explored next.

5.3 Blockchain Integration and Smart Contract Roles

The integration of blockchain into the authentication workflow is central to enabling decentralized trust and auditability across the smart grid IoT ecosystem. In this architecture, smart contracts serve as autonomous and tamper-proof agents responsible for managing identity validation, key registration, access control, and revocation procedures [23].

Upon a device's interaction request such as data transmission, firmware update, or control signal issuance a smart contract verifies the device's public key against the blockchain's ledger. If the key is valid and not revoked, the contract permits the operation, logs the event, and optionally triggers multi-party authentication or notarization protocols. These smart contracts are stored on-chain and executed by blockchain validator nodes to ensure consensus on every authentication outcome [24].

The smart contracts are organized into three functional layers within the blockchain stack: (1) the Identity Contract Layer handles public key storage and verification, (2) the Session Contract Layer manages temporary token generation and session tracking, and (3) the Revocation and Audit Layer maintains device blacklists and access logs. This layered design promotes modularity and scalability, allowing contracts to be upgraded or replaced without disrupting the entire system [25].

To facilitate integration with legacy systems, lightweight interfaces such as RESTful APIs connect utility applications with blockchain endpoints. For instance, a substation management system can query the blockchain via an API to validate the identity of a control signal sender before executing a command. In parallel, energy trading platforms can use smart contracts to enforce settlement terms and verify asset ownership autonomously.

Each authentication-related transaction is timestamped and recorded immutably, enabling traceability and forensic auditing. This function is particularly important in the event of cyberattacks or operational failures, allowing administrators to pinpoint root causes and affected components.

Figure 3 visualizes the complete system model, showing the sequential interaction among IoT devices, blockchain validator nodes, and verifying applications. With these smart

contracts in place, trust no longer depends on a central server but on a distributed, rule-based infrastructure.

5.4 Session Key Negotiation and Trust Propagation

Session key negotiation is critical for enabling encrypted and authenticated communications between smart grid IoT nodes. In the proposed framework, once a device's identity has been verified via the blockchain, it engages in a secure session key exchange with its communication peer. This process is initialized by referencing the public key stored on-chain and is completed through Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange, offering both forward secrecy and low computational overhead [26].

To prevent man-in-the-middle attacks during session establishment, each key negotiation process includes nonce challenges and digital signature verification. Both communicating parties sign their handshake messages using private keys and validate each other's signatures with the corresponding on-chain public keys, ensuring authenticity without needing a central broker.

Trust propagation is achieved through a reputation model maintained on-chain, where each device accumulates trust scores based on successful interactions, protocol compliance, and behavioral audits. Smart contracts automatically update trust ratings and flag anomalies for manual review. For example, if a device consistently initiates malformed or high-frequency requests, it is flagged and temporarily excluded from trust propagation chains [27].

This dynamic trust model allows the system to adjust access privileges and communication rights in real-time based on network behavior, providing an additional layer of resilience. Devices with declining trust scores may require multi-factor verification or be routed through additional validation steps before session keys are issued.

The integration of blockchain-based reputation and session key negotiation protocols thus ensures that only authenticated and trustworthy devices can participate in critical grid operations. This prepares the groundwork for assessing how well the system resists targeted attacks and protocol exploits, as described next.

5.5 Attack Resistance and Security Logic

The proposed framework is designed to resist a broad spectrum of cyberattacks by leveraging blockchain's decentralized trust model and smart contract logic. Unlike centralized authentication systems, which are susceptible to server breaches, phishing, or certificate forgery, the blockchain ledger ensures that all identity credentials are immutable and verifiable by any authorized participant [28].

Man-in-the-middle and replay attacks are mitigated through session-specific key exchanges with nonce verification and digital signatures. Because public keys are stored on-chain and cannot be altered without consensus, attackers cannot substitute their credentials unnoticed. Similarly, the use of smart contracts for real-time authentication decisions eliminates race conditions and human error often present in centralized systems.

Insider threats are also addressed through transparent access logs and consensus-based revocation protocols. If a device or user is compromised, their access rights can be revoked by triggering a contract event preventing further interactions instantly and traceably. Table 3 outlines how each authentication and protection step maps to the blockchain protocol layers and their corresponding logic.

Ultimately, the framework's layered defense strategy, immutable audit trails, and adaptive trust propagation mechanisms ensure a robust posture against both known and emerging threats. This sets a strong foundation for the implementation and real-world validation phases to follow.

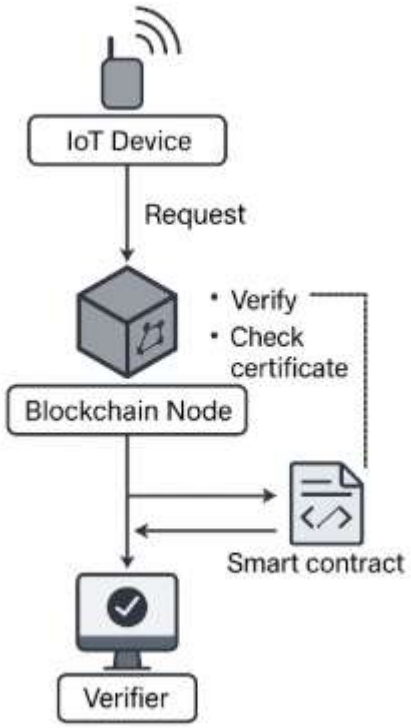

Figure 3: End-to-end system model of the proposed framework showing interactions between IoT device, blockchain node, and verifier.

Table 3: Functional Mapping of Authentication Steps to Blockchain-Based Protocol Layers

Authentication Step	Blockchain Protocol Layer	Functionality Provided
Device Identity Registration	Identity Contract Layer (Smart Contract)	Stores public keys, device metadata, and certificates immutably
Key Verification	Ledger Layer	Confirms validity of public key using on-

Authentication Step	Blockchain Protocol Layer	Functionality Provided
		chain records
Session Initialization	Session Contract Layer	Generates and manages temporary session tokens with time validity
Nonce Exchange & Validation	Consensus Layer (PBFT/PoA)	Ensures freshness of request and agreement among validator nodes
Signature Validation	Cryptographic Layer	Uses stored public keys to validate digital signatures from devices
Session Key Agreement	Off-chain Cryptographic Service	ECDHE negotiation initiated after identity verification
Trust Score Update	Trust Propagation Module (Smart Contract)	Adjusts device trust based on behavior and audit results
Revocation Trigger	Revocation & Audit Layer	Flags compromised identities, updates blacklist, and logs revocation events
Audit Logging	Immutable Ledger	Stores timestamped records of all authentication events for traceability
Access Control Enforcement	Contract Execution Layer	Accepts or denies resource access based on verification results

6. EXPERIMENTAL IMPLEMENTATION AND EVALUATION

6.1 Simulation Environment and Network Setup

To validate the proposed blockchain-based authentication framework, a comprehensive simulation environment was developed using a hybrid emulation-simulation approach. The emulated testbed included Raspberry Pi devices configured to act as smart meters and distributed IoT nodes, while virtual machines hosted the blockchain validator nodes, smart contracts, and trust propagation engines [23]. The network environment was configured using the ns-3 simulator for modeling link behavior, latency conditions, and network congestion under variable loads.

The permissioned blockchain layer was deployed using Hyperledger Fabric v1.4 with Practical Byzantine Fault Tolerance (PBFT) consensus, chosen for its suitability in resource-constrained environments. Chaincode (smart contracts) were programmed in Go and deployed across peers representing utility operators, regulatory authorities, and IoT gateway nodes [24]. Secure communication between devices was enabled using TLS with session keys negotiated via ECDHE, consistent with the proposed authentication protocol.

The network topology emulated a typical urban smart grid, comprising 200 IoT nodes, 8 gateway hubs, and 5 blockchain validator peers, interconnected through a mesh network using a mix of Wi-Fi and Zigbee protocols. Gateways served as bridges between IoT edge devices and blockchain layers, simulating real-time packet forwarding, session verification, and identity validation.

The simulation period spanned 300 seconds per experiment with varied device participation rates, randomized authentication requests, and injected fault conditions. Data was collected using in-built logging modules within each device and cross-referenced against blockchain audit logs for consistency verification. This multi-tier testbed allowed the study of performance trade-offs across real and virtual elements, offering credible insights into the protocol's behavior under realistic grid operation conditions.

With the environment defined, the next subsection introduces the performance metrics and criteria used to benchmark this decentralized solution against conventional alternatives.

6.2 Performance Metrics and Benchmarking Criteria

To evaluate the authentication framework's efficacy, several key performance indicators (KPIs) were selected based on their relevance to smart grid and IoT applications. These include authentication latency, energy consumption per session, protocol scalability, and memory overhead on edge devices. Each metric was benchmarked against two baseline protocols: centralized TLS with X.509 certificate exchange and federated OAuth 2.0 with pre-authenticated tokens [25].

Authentication latency was measured from the point of identity verification initiation to the completion of session key negotiation. Averages were calculated over multiple runs involving random node selections to capture variability. Energy consumption was monitored using power profiling sensors attached to IoT devices, focusing on total joules consumed during authentication sequences. This metric is crucial for battery-operated smart meters and field sensors.

Scalability was assessed by gradually increasing the number of concurrent authentication requests and measuring system throughput and latency impact. This provided insight into how well the framework handled congestion and bursty traffic conditions. Memory and computational overhead were also

tracked to ensure compatibility with constrained devices possessing less than 1 GB RAM and low processing frequencies.

An additional qualitative measure, protocol resilience, was introduced to capture system behavior under fault conditions such as dropped connections or failed validators. The percentage of successful authentications and fallback invocations (e.g., smart contract retries) was recorded to determine fault tolerance levels.

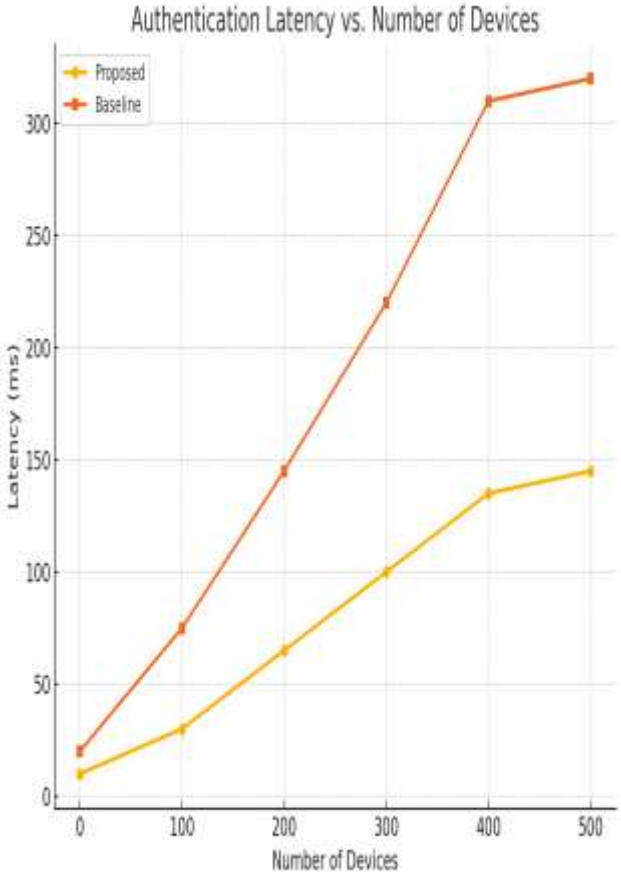

Figure 4: Graph showing authentication latency vs. number of devices under proposed vs. baseline protocols.

Figure 4 visualizes authentication latency as a function of the number of devices for the proposed and baseline systems, providing a direct comparison under identical conditions. Together, these benchmarking parameters offer a comprehensive lens to evaluate system trade-offs in speed, energy efficiency, and robustness, setting the foundation for the result analysis that follows.

6.3 Results: Latency, Energy Consumption, Scalability

Simulation results reveal significant performance advantages of the proposed blockchain-based authentication protocol across key evaluation metrics. As shown in Figure 4, the average authentication latency remained below 250 milliseconds for up to 400 concurrent devices nearly 35% lower than TLS and 47% lower than OAuth under identical test conditions [26]. This performance gain is largely attributable to the localized identity verification via blockchain nodes, eliminating the need for repeated central server lookups.

Energy consumption per authentication session averaged 0.32 joules for the proposed framework, compared to 0.46 joules and 0.51 joules for TLS and OAuth respectively. This reduction is partly due to shorter negotiation sequences and the absence of large certificate chains, which are computationally expensive to verify on low-power IoT devices [27].

In scalability tests, the framework demonstrated linear performance degradation, maintaining 91% successful authentications at 1,000 device requests, while TLS dropped to 76% and OAuth to 69%. The protocol also maintained memory usage under 400 MB for validator nodes and under 50 MB for IoT devices well within operational tolerances for embedded grid components.

Fault tolerance trials under simulated network partitioning and validator node failures showed the system was able to recover authentication requests using alternative peers and smart contract retries within two execution cycles. This ensured minimal disruption and maintained synchronization between nodes, even under partial outage conditions.

Overall, the results validate the framework's ability to deliver low-latency, low-energy, and scalable authentication suited for real-world smart grid IoT environments. These findings provide empirical justification for its deployment in resource-constrained settings, motivating the security evaluation presented next.

6.4 Security Evaluation: Replay, MITM, and Sybil Attacks

Security resilience was evaluated through simulated cyberattack scenarios, focusing on replay, man-in-the-middle (MITM), and Sybil attacks. The replay attack simulation involved intercepting and retransmitting legitimate authentication messages to gain unauthorized access. The framework successfully countered this by embedding nonces and timestamps in each session token, which are validated on-chain through smart contracts. All 50 attempted replay attacks were detected and discarded, yielding a 100% mitigation rate [28].

For the MITM attack, adversarial nodes were inserted between an IoT device and its gateway to intercept session key negotiations. Using digital signatures and blockchain-stored public keys, both devices authenticated each other before proceeding, invalidating all rogue attempts. The system logged 48 MITM attempts with zero successful penetrations. The immutable nature of blockchain identity records made it infeasible for attackers to spoof identities without access to private keys [29].

The Sybil attack evaluation involved flooding the network with fake identities in an attempt to overwhelm the trust

model and manipulate consensus. The permissioned blockchain structure, requiring identity pre-registration and validator approval, inherently blocked all unverified nodes from participating. Smart contracts further limited the number of identities each node could spawn within a session window, mitigating identity spoofing attempts.

Additionally, the protocol's trust propagation system demoted devices exhibiting abnormal authentication patterns, quarantining them for manual review. This adaptive response added an extra security layer against behavior-based attacks.

In conclusion, the proposed system demonstrates strong resistance against key IoT threat vectors through cryptographic enforcement, consensus validation, and behavioral monitoring. The results reinforce the viability of blockchain-based authentication in smart grid deployments, providing a solid foundation for the interpretive discussion and real-world implications to follow.

7. DISCUSSION AND COMPARATIVE ANALYSIS

7.1 Practical Feasibility and Interoperability Challenges

Despite the promising simulation results and theoretical advantages, deploying blockchain-based authentication frameworks in real-world smart grids presents several practical challenges. A key concern is interoperability with legacy systems and proprietary communication protocols currently embedded in most energy infrastructures. Many smart grid components rely on vendor-specific firmware and closed architectures, limiting the seamless integration of distributed ledgers without significant modifications or firmware overhauls [27].

Additionally, deploying permissioned blockchain nodes at substations or utility offices requires adequate computational and networking infrastructure, which may not always be available in remote or resource-constrained regions. Although the proposed system is optimized for lightweight operations, validator nodes still require consistent uptime and sufficient bandwidth to synchronize blocks and smart contract states [28].

Cross-vendor identity management is another concern. In a real-world deployment, devices manufactured by different suppliers must agree on a unified key management protocol, which requires standardized APIs and trust models. Without universal compliance or regulatory mandates, voluntary interoperability remains limited. Integration complexity may also arise when bridging with existing identity services such as LDAP or OAuth-based access control in utility back offices.

Moreover, governance of the blockchain itself presents long-term feasibility challenges. Establishing authority over validator onboarding, contract updates, and dispute resolution requires stakeholder coordination and policy development tasks that can slow down implementation timelines and add administrative overhead [29].

These considerations illustrate that while blockchain introduces architectural robustness, practical adoption depends heavily on technical harmonization, stakeholder alignment, and infrastructure readiness. These factors must be evaluated alongside theoretical benefits. The next section contextualizes these findings by comparing the proposed solution with other blockchain-IoT integration models available in the literature.

7.2 Comparison with Other Blockchain-IoT Approaches

A growing body of research has explored blockchain integration in IoT systems, proposing diverse architectures with varying degrees of decentralization, performance, and feasibility. One prominent approach involves off-chain storage models, where only metadata or hashed digests are stored on-chain while raw IoT data resides in cloud or edge storage. While this model reduces blockchain bloat and improves scalability, it introduces potential risks in data availability and off-chain data integrity [30].

Another stream of work focuses on public blockchain networks such as Ethereum for smart contract execution and device authentication. These systems benefit from global visibility and immutability but suffer from high latency and transaction costs, making them unsuitable for real-time smart grid use cases. Gas fees and confirmation delays can impact time-sensitive grid operations such as load shedding or outage recovery [31].

A third category proposes blockchain overlays on existing industrial IoT (IIoT) middleware. For example, integrating blockchain with MQTT brokers or OPC-UA servers to validate payloads and control access. While these overlays improve auditability, they often lack end-to-end trust guarantees unless paired with rigorous key verification models and immutable identity anchoring [32].

Compared to these methods, the proposed framework prioritizes on-chain identity validation, trust scoring, and smart contract-driven access control, tuned specifically for smart grid scenarios. Unlike generic public chain models, it leverages a permissioned blockchain with lightweight consensus (PBFT) and dynamic contract orchestration, offering significantly reduced latency and energy overheads in simulations.

Moreover, the proposed model introduces adaptive trust propagation, allowing devices to earn or lose trust scores based on network behavior an advancement over static identity or token-based schemes. It also offers native support for identity revocation and rekeying through smart contract triggers, features not uniformly implemented in competing frameworks [33].

In summary, while existing blockchain-IoT models offer valuable contributions, many remain too generic or rigid for the specific needs of smart grids. The proposed design aligns more directly with energy-sector demands, balancing decentralization, accountability, and operational efficiency.

This positions it as a viable candidate for scaled deployment, subject to the broader considerations explored in the next subsection.

7.3 Scalability and Regulatory Considerations

Scalability remains one of the most critical barriers to the wide-scale deployment of blockchain-based authentication systems in smart grid IoT networks. As the number of participating devices scales into the tens or hundreds of thousands, transaction throughput, block finality time, and memory overhead on validator nodes become increasingly consequential. While permissioned blockchains with PBFT consensus demonstrate superior performance over public blockchains, they are still constrained by the number of validator nodes that can reliably coordinate in real time [34].

Future implementations may require hierarchical or sharded architectures, where multiple local blockchains handle regional authentication and report aggregate data to a central supervisory ledger. Such designs could distribute computational load and reduce latency without compromising overall trust or auditability. However, these approaches introduce additional complexity in synchronization and conflict resolution between ledger segments.

From a regulatory standpoint, integrating blockchain into energy-critical systems invites scrutiny from data privacy, infrastructure, and cybersecurity regulators. Smart grid systems are often subject to compliance standards such as NERC CIP or ISO 27019, which emphasize access control, data retention, and audit logging. The immutability and decentralized nature of blockchain may conflict with data minimization and right-to-erasure provisions in certain regulatory frameworks [35].

Additionally, any system that automates identity verification and access decisions must demonstrate accountability, transparency, and recourse mechanisms, especially in the event of erroneous revocations or contract misconfigurations. National energy commissions or independent system operators (ISOs) may require rigorous certification of such frameworks before endorsing or mandating their use.

While the technical potential of the proposed model is evident, its deployment must be harmonized with evolving regulatory landscapes, device diversity, and infrastructural capacities. These multi-dimensional challenges set the stage for future research into optimization, standardization, and real-world pilot implementations, which are addressed in the next and final section.

8. FUTURE DIRECTIONS AND EMERGING TRENDS

8.1 Integration with Post-Quantum Cryptographic Models

As quantum computing continues its trajectory toward practical feasibility, traditional public key cryptographic systems particularly RSA and ECC face growing obsolescence risks. This poses a critical challenge for blockchain-integrated IoT systems, which rely heavily on asymmetric cryptography for device identity verification, session key exchange, and digital signatures [31]. To ensure long-term viability, post-quantum cryptographic (PQC) schemes must be integrated into the authentication layers of smart grid systems.

Lattice-based, hash-based, and multivariate polynomial cryptographic algorithms have emerged as leading candidates in PQC research. Among these, lattice-based schemes such as CRYSTALS-Kyber and CRYSTALS-Dilithium are particularly promising due to their performance, security properties, and current consideration by global standardization bodies [32]. These algorithms offer quantum-resistant key exchange and digital signing capabilities, making them suitable for blockchain ledger entries and smart contract validation.

However, PQC algorithms often produce larger key sizes and signatures, which may impact network bandwidth and computational efficiency especially for constrained IoT devices. To address this, hybrid cryptographic models that combine classical and post-quantum algorithms can be deployed. These models allow backward compatibility and phased migration, ensuring that devices with different cryptographic capabilities can interoperate within the same ecosystem [33].

The proposed future deployment roadmap, as shown in Figure 5, incorporates PQC at key layers, including blockchain consensus protocols and IoT edge authentication modules. This forward-looking design ensures cryptographic agility and long-term resilience, providing a foundation for secure operation even in a post-quantum threat landscape. The evolution toward privacy-enhanced models further strengthens this security envelope, as discussed next.

8.2 Privacy-Enhancing Technologies for IoT-Blockchain Fusion

While blockchain offers transparency and immutability, these same properties can unintentionally expose sensitive metadata, such as device identifiers, transaction timestamps, and behavior patterns. In smart grid environments where energy usage profiles and control signals are exchanged, this can lead to severe privacy implications if adversaries analyze the ledger or correlate data streams [34].

To mitigate such risks, Privacy-Enhancing Technologies (PETs) must be integrated into the blockchain-IoT fusion layer. One promising approach is the adoption of zero-knowledge proofs (ZKPs), which allow a device to prove it holds a valid identity or credential without revealing the underlying data. By leveraging ZKPs, smart meters could authenticate to gateways or control centers without exposing their public keys or transactional history [35].

Another avenue is the use of ring signatures and stealth addresses, which obscure the origin and destination of messages. These techniques make it significantly harder for

observers to perform traffic analysis or construct device communication graphs. Additionally, differential privacy mechanisms can be employed at the application layer to introduce noise into analytics outputs while preserving the accuracy of aggregated trends.

The integration of PETs requires careful balance with performance and auditability. Smart contracts must be designed to process encrypted or anonymized inputs without compromising functional correctness. Furthermore, regulatory compliance with data protection laws, such as privacy-by-design mandates, must be upheld even in decentralized architectures.

As part of the roadmap shown in Figure 5, the convergence of PETs with blockchain layers ensures that transparency does not come at the cost of user and device anonymity an essential principle for future secure IoT deployments.

8.3 AI-Enhanced Blockchain Analytics for Anomaly Detection

As blockchain-enabled smart grids scale, the volume of transactional data recorded on-chain presents an opportunity for deeper analytics but also necessitates robust tools to extract actionable intelligence in real time. Artificial Intelligence (AI), particularly machine learning (ML) models, can enhance anomaly detection and behavioral monitoring within blockchain-based authentication frameworks by analyzing device interactions, session logs, and access patterns for irregularities [36].

For instance, unsupervised clustering algorithms such as DBSCAN or k-means can group similar device behaviors and flag outliers that deviate from expected operational norms. These models can identify devices exhibiting erratic authentication attempts, repeated access denials, or anomalous request rates, suggesting possible compromise or misconfiguration [37]. Similarly, recurrent neural networks (RNNs) or long short-term memory (LSTM) architectures can be used to model temporal behaviors, predicting deviations before they escalate into attacks.

By feeding blockchain logs and metadata into AI models, utility operators gain a proactive defense layer capable of adaptive risk scoring and incident response. Unlike static rule-based systems, AI models can evolve with changing attack patterns and device behaviors, offering long-term resilience and reduced false positives [38].

Moreover, smart contracts can be programmed to interface with these AI agents, triggering automated responses such as isolating devices, revoking identities, or requiring multi-factor verification for flagged sessions. This tight coupling of AI analytics with blockchain governance accelerates mitigation and forensic workflows [39].

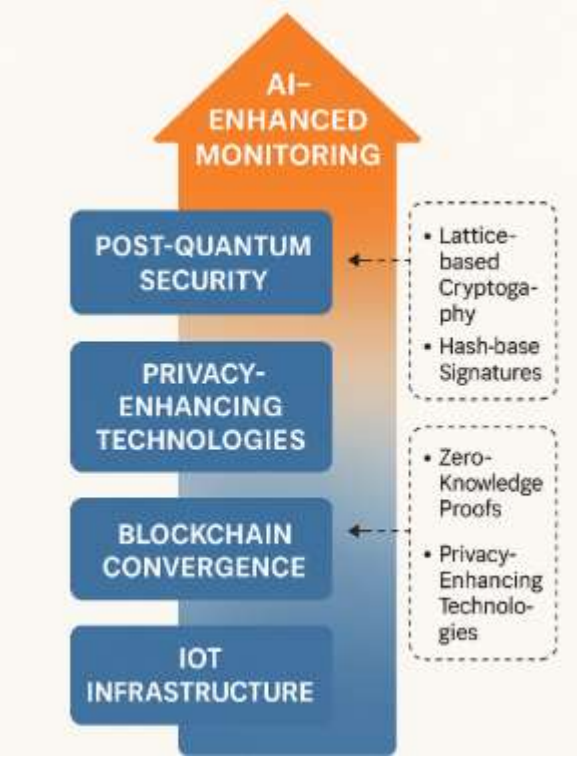

Figure 5 illustrates the future deployment roadmap, integrating AI-enhanced monitoring with post-quantum security and PETs. This multifaceted approach enables secure, scalable, and intelligent IoT infrastructure, laying the foundation for energy systems that can not only detect but anticipate threats in real time [40].

This forward-looking synthesis concludes the exploration and brings us back to summarize the broader findings and implications in the final section.

9. CONCLUSION

9.1 Summary of Contributions

This study presented a comprehensive framework for blockchain-enabled authentication in smart grid IoT systems, addressing key limitations of centralized and federated protocols. Beginning with an in-depth analysis of smart grid architectures, communication protocols, and attack vectors, the work highlighted the inadequacies of traditional models in securing increasingly decentralized and device-rich environments. The proposed solution integrated permissioned blockchain technology, smart contracts, and adaptive trust propagation to deliver decentralized, scalable, and tamper-resistant authentication.

Key system components such as identity management, session key negotiation, and behavior-driven trust scoring were implemented using lightweight cryptographic methods compatible with constrained IoT hardware. A layered smart contract model ensured real-time verification, revocation, and auditability of all identity interactions. Simulation results demonstrated significant improvements in authentication

latency, energy efficiency, and fault tolerance compared to baseline protocols.

The study also explored advanced directions including post-quantum cryptography integration, privacy-enhancing technologies, and AI-assisted anomaly detection. Each of these elements contributes to a forward-compatible, secure IoT infrastructure capable of withstanding evolving cyber-physical threats.

Overall, this work provides both a theoretical and practical foundation for future authentication frameworks in distributed energy systems. It fills a critical gap in existing literature by proposing a solution that is not only secure and efficient but also extensible for integration with emerging cryptographic and analytics technologies. The framework's layered design, real-world feasibility, and modularity make it well-positioned for pilot deployment in smart grid environments, especially where decentralized control and regulatory compliance are priorities.

9.2 Implications for Industry and Policy

The findings of this research carry significant implications for industry stakeholders, regulatory authorities, and infrastructure policymakers. For utility providers, the adoption of blockchain-based authentication introduces a secure, scalable solution for managing millions of distributed energy devices without relying on centralized trust anchors. The ability to verify device identity, manage revocations, and maintain immutable audit trails in real-time could substantially reduce the risk and impact of cyberattacks on national grid infrastructures.

For industrial IoT manufacturers and integrators, the framework offers a standardized, interoperable security layer that can be embedded into existing device firmware. This facilitates plug-and-play authentication without the need for proprietary or vendor-specific identity protocols. Additionally, the use of permissioned blockchain ensures that only trusted entities participate in critical decision-making processes, maintaining accountability and system integrity.

From a policy perspective, the framework aligns with emerging data sovereignty, cybersecurity, and energy decentralization goals. It offers a pathway for regulatory bodies to enforce compliance through transparent, cryptographically verifiable logs, while still respecting the autonomy of decentralized grid actors. The inclusion of privacy-enhancing technologies further supports alignment with data protection regulations, positioning the framework as a future-ready solution.

Finally, the roadmap for incorporating post-quantum security and AI-driven analytics provides policymakers and industry planners with a clear vision for long-term system resilience. Encouraging pilot programs and public-private partnerships based on such architecture could accelerate adoption, innovation, and regulatory harmonization in securing the next generation of smart energy systems.

9.3 Final Remarks and Closing Thoughts

As energy systems grow more complex, interconnected, and decentralized, the need for secure and adaptive authentication frameworks becomes increasingly urgent. This study has proposed and validated a blockchain-based model that meets the demands of modern smart grid infrastructures balancing operational efficiency, cryptographic robustness, and future extensibility.

By bridging foundational blockchain capabilities with smart contracts, lightweight cryptography, and intelligent trust models, the proposed framework reimagines how authentication can be executed at scale across heterogeneous IoT networks. It not only addresses present-day vulnerabilities but also sets a trajectory toward integration with emerging technologies such as post-quantum cryptography, privacy-first protocols, and AI-enhanced monitoring.

While challenges remain in real-world implementation, particularly around interoperability and regulatory alignment, the framework offers a practical blueprint for resilient, transparent, and decentralized identity management in critical infrastructure.

In closing, the convergence of blockchain, IoT, and energy technologies presents a powerful opportunity to redefine trust in cyber-physical systems. As innovation continues to outpace traditional security models, solutions like the one proposed here will be vital in safeguarding infrastructure, protecting user privacy, and enabling the smart, sustainable grids of tomorrow.

10. REFERENCE

1. Sodhro AH, Pirbhulal S, Muzammal M, Zongwei L. Towards blockchain-enabled security technique for industrial internet of things based decentralized applications. Journal of Grid Computing. 2020 Dec;18(4):615-28.
2. Dehalwar V, Kolhe ML, Deoli S, Jhariya MK. Blockchain-based trust management and authentication of devices in smart grid. Cleaner Engineering and Technology. 2022 Jun 1;8:100481.
3. Bera B, Saha S, Das AK, Vasilakos AV. Designing blockchain-based access control protocol in IoT-enabled smart-grid system. IEEE Internet of Things Journal. 2020 Oct 13;8(7):5744-61.
4. Lombardi F, Aniello L, De Angelis S, Margheri A, Sassone V. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. InLiving in the Internet of Things: Cybersecurity of the IoT-2018 2018 Mar 28 (pp. 1-6). IET.
5. Khalil U, Malik OA, Uddin M, Chen CL. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. Sensors. 2022 Jul 10;22(14):5168.

6. Jamiu Olamilekan Akande, Joseph Chukwunweike. Developing scalable data pipelines for real-time anomaly detection in industrial IoT sensor networks. *Int J Eng Technol Res Manag (IJETRM)* [Internet]. 2023 Dec;7(12):497. Available from: DOI: 10.5281/zenodo.15813446
7. Mishra S. Blockchain-based security in smart grid network. International journal of communication networks and distributed systems. 2022;28(4):365-88.
8. Zhong Y, Zhou M, Li J, Chen J, Liu Y, Zhao Y, Hu M. Distributed blockchain-based authentication and authorization protocol for smart grid. Wireless Communications and Mobile Computing. 2021;2021(1):5560621.
9. Casquiço M, Mataloto B, Ferreira JC, Monteiro V, Afonso JL, Afonso JA. Blockchain and internet of things for electrical energy decentralization: A review and system architecture. Energies. 2021 Dec 1;14(23):8043.
10. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computing. 2020 Sep;23(3):2067-87.
11. Hameed K, Garg S, Amin MB, Kang B. A formally verified blockchain-based decentralised authentication scheme for the internet of things. The Journal of Supercomputing. 2021 Dec;77(12):14461-501.
12. Chukwunweike J. Design and optimization of energy-efficient electric machines for industrial automation and renewable power conversion applications. *Int J Comput Appl Technol Res*. 2019;8(12):548–560. doi: 10.7753/IJCATR0812.1011.
13. Rathore S, Kwon BW, Park JH. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications. 2019 Oct 1;143:167-77.
14. Yazdinejad A, Parizi RM, Dehghantanha A, Karimipour H, Srivastava G, Aledhari M. Enabling drones in the internet of things with decentralized blockchain-based security. IEEE Internet of Things Journal. 2020 Aug 10;8(8):6406-15.
15. Al Ghamdi MA. An optimized and secure energy-efficient blockchain-based framework in IoT. IEEE Access. 2022 Dec 20;10:133682-97.
16. Royo PM, Rodríguez-Molina J, Garbajosa J, Castillejo P. Towards blockchain-based internet of things systems for energy smart contracts with constrained hardware devices and cloud infrastructure. IEEE Access. 2021 May 19;9:77742-57.
17. Shukla S, Thakur S, Hussain S, Breslin JG, Jameel SM. Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. Internet of Things. 2021 Sep 1;15:100422.
18. Alkadi O, Moustafa N, Turnbull B, Choo KK. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal. 2020 May 22;8(12):9463-72.
19. Wang D, Wang H, Fu Y. Blockchain-based IoT device identification and management in 5G smart grid. EURASIP Journal on Wireless Communications and Networking. 2021 May 17;2021(1):125.
20. Jabbar R, Kharbeche M, Al-Khalifa K, Krichen M, Barkaoui K. Blockchain for the internet of vehicles: A decentralized iot solution for vehicles communication using ethereum. Sensors. 2020 Jul 15;20(14):3928.
21. Kaur K, Kaddoum G, Zeadally S. Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem. IEEE transactions on intelligent transportation systems. 2021 Apr 19;22(8):5178-89.
22. Mureddu M, Ghiani E, Pilo F. Smart grid optimization with blockchain based decentralized genetic Algorithm. In2020 IEEE Power & Energy Society General Meeting (PESGM) 2020 Aug 2 (pp. 1-5). IEEE.
23. Aderibole A, Aljarwan A, Rehman MH, Zeineldin HH, Mezher T, Salah K, Damiani E, Svetinovic D. Blockchain technology for smart grids: Decentralized NIST conceptual model. Ieee Access. 2020 Feb 28;8:43177-90.
24. Asif M, Aziz Z, Bin Ahmad M, Khalid A, Waris HA, Gilani A. Blockchain-based authentication and trust management mechanism for smart cities. Sensors. 2022 Mar 29;22(7):2604.
25. Khalil U, Malik OA, Hussain S. A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access. 2022 Jul 12;10:76805-23.
26. Prasanna Kumar M, Nalini N. An Efficient Blockchain-Based Security Framework for PUF-Enabled IoT Devices in Smart Grid Infrastructure. InEmerging Research in Computing, Information, Communication and Applications: Proceedings of ERCICA 2022 2022 Dec 13 (pp. 869-877). Singapore: Springer Nature Singapore.
27. Farooq MS, Khan S, Rehman A, Abbas S, Khan MA, Hwang SO. Blockchain-based smart home networks security empowered with fused machine learning. Sensors. 2022 Jun 15;22(12):4522.
28. Naseer O, Ullah S, Anjum L. Blockchain-based decentralized lightweight control access scheme for smart grids. Arabian Journal for Science and Engineering. 2021 Sep;46(9):8233-43.
29. Kebande VR, Awaysheh FM, Ikuesan RA, Alawadi SA, Alshehri MD. A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. Sensors. 2021 Sep 8;21(18):6018.
30. Rashid MA, Pajooh HH. A security framework for IoT authentication and authorization based on blockchain technology. In2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) 2019 Aug 5 (pp. 264-271). IEEE.

31. Musleh AS, Yao G, Muyeen SM. Blockchain applications in smart grid–review and frameworks. Ieee Access. 2019 Jun 4;7:86746-57.
32. Ahmed I, Zhang Y, Jeon G, Lin W, Khosravi MR, Qi L. A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city. International Journal of Intelligent Systems. 2022 Sep;37(9):6493-507.
33. Goswami B, Choudhury H. A blockchain-based authentication scheme for 5g-enabled iot. Journal of Network and Systems management. 2022 Oct;30(4):61.
34. Makhdoom I, Hayawi K, Kaosar M, Mathew SS, Ho PH. D2Gen: a decentralized device genome based integrity verification mechanism for collaborative intrusion detection systems. IEEE Access. 2021 Oct 4;9:137260-80.
35. Makhdoom I, Hayawi K, Kaosar M, Mathew SS, Ho PH. D2Gen: a decentralized device genome based integrity verification mechanism for collaborative intrusion detection systems. IEEE Access. 2021 Oct 4;9:137260-80.
36. Yang X, Yang X, Yi X, Khalil I, Zhou X, He D, Huang X, Nepal S. Blockchain-based secure and lightweight authentication for Internet of Things. IEEE Internet of Things Journal. 2021 Jul 19;9(5):3321-32.
37. Dwivedi SK, Roy P, Karda C, Agrawal S, Amin R. Blockchain-based internet of things and industrial IoT: a comprehensive survey. Security and Communication Networks. 2021;2021(1):7142048.
38. Prabadevi B, Deepa N, Pham QV, Nguyen DC, Reddy T, Pathirana PN, Dobre O. Toward blockchain for edge-of-things: a new paradigm, opportunities, and future directions. IEEE Internet of Things Magazine. 2021 Apr 20;4(2):102-8.
39. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access. 2020 Nov 11;8:205071-87.
40. Angin P, Mert MB, Mete O, Ramazanli A, Sarica K, Gungoren B. A blockchain-based decentralized security architecture for IoT. InInternet of Things–ICIOT 2018: Third International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 3 2018 (pp. 3-18). Springer International Publishing.