International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| ICRCEDA2025-Conference Proceeding
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.ICRCEDA25-126

Original Article

Securing the Internet of Things (IoT): Developing a Decentralized Blockchain-Based Framework for Device Authentication and Data Integrity

Deepak
Bishop Heber College, Trichy.

Abstract - *The rapid proliferation of Internet of Things (IoT) devices has heightened concerns regarding device authentication and data integrity within IoT ecosystems. Traditional centralized security mechanisms often fall short in addressing these challenges due to scalability and trust issues. This paper proposes a decentralized blockchain-based framework to enhance device authentication and ensure data integrity in IoT networks. Leveraging blockchain's immutable ledger and consensus mechanisms, the framework provides secure and transparent device registration, authentication processes, and tamper-proof data storage. The integration of homomorphic encryption further bolsters data privacy by enabling secure data processing. Through simulation and analysis, the proposed framework demonstrates improved security, scalability, and efficiency, offering a robust solution to the pressing security concerns in IoT environments.*

Keywords - *Internet of Things (IoT), Blockchain Technology, Device Authentication, Data Integrity, Decentralized Framework, Homomorphic Encryption, Security, Privacy, Scalability, Efficiency*.

1. Introduction

1.1. Overview of IoT and Its Significance

The Internet of Things (IoT) refers to a rapidly evolving technological paradigm that integrates physical objects with the digital world by embedding them with sensors, software, and network connectivity. These smart devices, ranging from household appliances and wearable health monitors to industrial machines and autonomous vehicles, are capable of collecting, processing, and exchanging data through the internet without human intervention. This intelligent interconnection has paved the way for unprecedented levels of automation and responsiveness across various sectors. In healthcare, IoT enables real-time patient monitoring, remote diagnostics, and smart medical equipment, leading to improved outcomes and reduced costs. In transportation, connected vehicles and smart traffic management systems contribute to safer and more efficient travel. In agriculture, IoT solutions like soil moisture sensors, weather stations, and livestock trackers help optimize farming practices and resource usage. Similarly, smart cities leverage IoT for managing utilities, waste, energy, and security infrastructure, thereby enhancing urban living standards.

The significance of IoT lies in its ability to transform traditional operations into intelligent systems that respond proactively to changing conditions. By providing continuous feedback and actionable insights, IoT systems drive efficiency, reduce operational costs, and support data-driven decision-making. Furthermore, the proliferation of 5G and edge computing technologies has significantly enhanced the capabilities of IoT by providing low latency, high-speed communication, and real-time processing closer to data sources. However, the exponential growth in IoT adoption also introduces complexity, as billions of heterogeneous devices must communicate securely and reliably. Interoperability, scalability, and security are ongoing challenges that must be addressed to fully realize IoT's potential. Despite these challenges, the ongoing integration of IoT technologies into critical infrastructure signals a paradigm shift in how information is gathered, analyzed, and utilized across industries. The transformative nature of IoT is not just about connecting devices it's about creating a smarter, more responsive, and interconnected world that continually learns and adapts to human needs and environmental conditions.

1.2. Motivation for Enhancing Security in IoT Networks

The widespread deployment of IoT devices across various domains has introduced a new dimension of vulnerability due to the massive scale and diversity of connected endpoints. These devices routinely handle sensitive information such as personal health data, location details, and operational controls of critical infrastructure. Consequently, the security and privacy of data within IoT ecosystems are of paramount importance. Unlike traditional computing systems, IoT networks are characterized by their decentralized architecture, limited computational capabilities, and often inconsistent security standards, making them prime targets for cyberattacks. Common threats to IoT networks include unauthorized access, man-in-the-middle attacks, data tampering, denial-

of-service (DoS) attacks, and malware infections. These threats are exacerbated by the fact that many IoT devices lack proper authentication protocols or are configured with weak, hardcoded credentials. Additionally, the dynamic nature of IoT networks where devices frequently join and leave the network makes it difficult to implement and enforce comprehensive security policies.

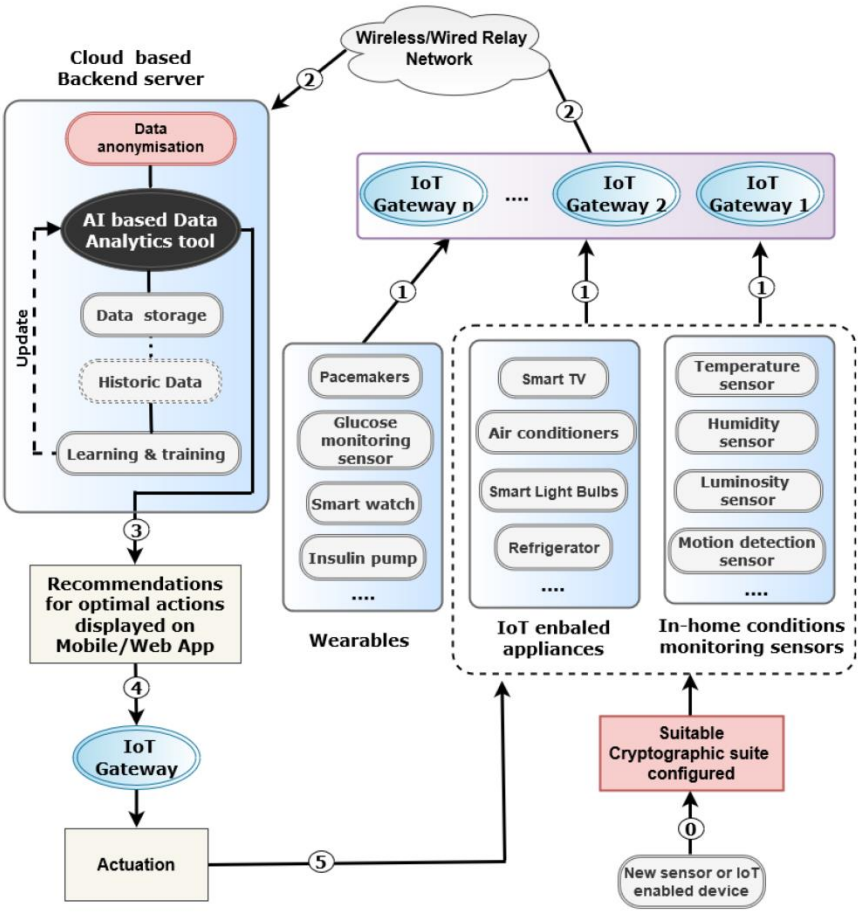

Fig 1: Wireless/Wired Relay Network

The limitations of traditional security mechanisms, such as centralized authentication servers and conventional encryption models, become apparent in IoT environments. Centralized systems introduce single points of failure and may not scale effectively with the growing number of devices. Furthermore, many security solutions are too resource-intensive for low-power IoT devices, leaving them inadequately protected. Addressing these security challenges is not just a technical necessity but also a fundamental requirement for the continued growth and adoption of IoT technologies. Public confidence in IoT systems hinges on the assurance that personal data and system integrity are preserved. Security breaches not only lead to financial and reputational damage but can also compromise critical services in sectors such as healthcare, transportation, and energy. Thus, there is an urgent need for innovative security frameworks tailored to the unique requirements of IoT. Such frameworks should be decentralized, lightweight, and capable of providing end-to-end security across diverse devices and platforms. Enhancing IoT security is critical for safeguarding users, enabling trusted interactions, and supporting the safe evolution of interconnected digital infrastructures.

1.3. Objectives of the Proposed Blockchain-Based Framework

The proposed blockchain-based framework seeks to address the security limitations of traditional IoT infrastructures by introducing a decentralized, transparent, and tamper-resistant system for data management and device authentication. The core objective is to eliminate centralized points of vulnerability and enhance the overall trust and reliability of data transactions within IoT networks. Blockchain, by design, offers an immutable ledger maintained through consensus among distributed nodes. This structure ensures that once data is recorded, it cannot be altered without detection. Applying this to IoT, each device interaction whether data transmission or control command can be logged securely on the blockchain, providing an auditable trail of events. This approach strengthens data integrity, ensures accountability, and simplifies forensic analysis in the event of a breach. Another key objective of the framework is to facilitate decentralized device authentication. Instead of relying on a central authority to

validate devices, the framework enables devices to authenticate each other via cryptographic proofs and blockchain-based trust models.

This reduces the risk of single-point failures and enhances the system's resilience against impersonation and spoofing attacks. To further reinforce, the framework integrates homomorphic encryption, a cryptographic technique that allows computations on encrypted data without decrypting it. This enables sensitive IoT data to be processed securely in untrusted environments such as cloud servers or third-party platforms without exposing the underlying information. This is especially useful in sectors like healthcare and finance, where confidentiality is critical. The framework is also designed with scalability and efficiency in mind. It leverages lightweight consensus algorithms and optimized cryptographic schemes tailored to the resource constraints of IoT devices. This ensures that the security enhancements do not compromise the performance or battery life of connected devices. In summary, the proposed framework aims to deliver a robust, privacy-preserving, and scalable security solution for IoT networks. By combining the strengths of blockchain and advanced encryption, it aspires to build user trust, protect critical data, and support the secure expansion of the IoT landscape across industries.

2. Literature Review

2.1. Existing Security Challenges in IoT

The Internet of Things (IoT) ecosystem is inherently complex, diverse, and distributed, which introduces a range of unique security challenges. One of the most pressing issues arises from the limited computational and energy resources of many IoT devices. Unlike traditional computing systems, many IoT devices operate with constrained processing power, memory, and battery life, which restricts the implementation of strong encryption, authentication, and other robust security protocols. As a result, these devices often become vulnerable entry points for cyber attackers. Common threats include unauthorized **access**, where attackers exploit weak or default credentials to take control of devices. Data interception is another major concern, especially when communication occurs over unsecured or poorly encrypted channels. Additionally, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are frequently used to overwhelm IoT devices or networks, rendering them inoperable. The Mirai botnet attack is a well-known example where IoT devices were hijacked to launch large-scale DDoS attacks.

Physical tampering also poses a significant risk, as many IoT devices are deployed in public or semi-public environments where they are easily accessible. Attackers can manipulate hardware or firmware to gain control or extract sensitive data. Another challenge lies in the heterogeneity of IoT devices, which differ significantly in terms of hardware, software, communication protocols, and operating environments. This diversity makes it extremely difficult to implement uniform security standards or apply a one-size-fits-all approach. Moreover, the scale of IoT deployments, often involving thousands or even millions of devices, introduces challenges in monitoring, updating, and securing each endpoint. The dynamic and often ad-hoc nature of IoT networks further complicates security management. Devices may join or leave the network at any time, requiring real-time and adaptive security policies. This lack of centralized control and oversight creates opportunities for evolving and sophisticated threats to exploit vulnerabilities at multiple layers device, network, and application. In essence, the existing security challenges in IoT are multifaceted and demand a comprehensive, adaptable, and lightweight security approach that can accommodate resource-constrained devices, high scalability, and diverse communication environments.

2.2. Review of Current Solutions and Their Limitations

Various security mechanisms have been developed to protect IoT systems, ranging from encryption techniques and authentication protocols to intrusion detection systems (IDS) and secure communication frameworks. While these solutions have proven effective in traditional computing environments, their direct application to IoT networks presents significant limitations due to the unique constraints and characteristics of IoT devices. Encryption is a cornerstone of data security. Techniques such as AES, RSA, and ECC are commonly employed to protect data in transit and at rest. However, these algorithms often require substantial computational power and energy, making them unsuitable for low-power IoT devices. Even lightweight encryption schemes can pose challenges when devices operate on minimal resources or in latency-sensitive environments. Access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), help restrict device and user permissions. Nonetheless, these systems can struggle to adapt to the dynamic nature of IoT, where devices frequently change roles or operate in mobile settings. Managing permissions at scale can also become complex and error-prone. Intrusion Detection Systems (IDS) aim to detect unusual or malicious behavior.

While effective in traditional networks, they often generate high false-positive rates in IoT environments due to the unpredictable nature and sheer volume of data generated by connected devices. Furthermore, deploying IDS on constrained IoT devices is not always feasible. Secure communication protocols, such as TLS/SSL, offer end-to-end encryption but are often too heavy for devices with minimal computational capabilities. Protocols like Datagram TLS (DTLS) and Lightweight Machine-to-Machine (LwM2M) have been developed to address this, but compatibility and integration issues remain. Additionally, many

current security frameworks are designed with centralized architectures in mind, which introduces single points of failure. This approach contradicts the distributed nature of IoT systems and can hinder scalability and resilience. In conclusion, while existing solutions offer a foundation for IoT security, they are not always suitable for the resource-constrained, heterogeneous, and dynamic nature of IoT networks. These limitations underscore the urgent need for innovative, decentralized, and lightweight security frameworks specifically tailored to the evolving IoT ecosystem.

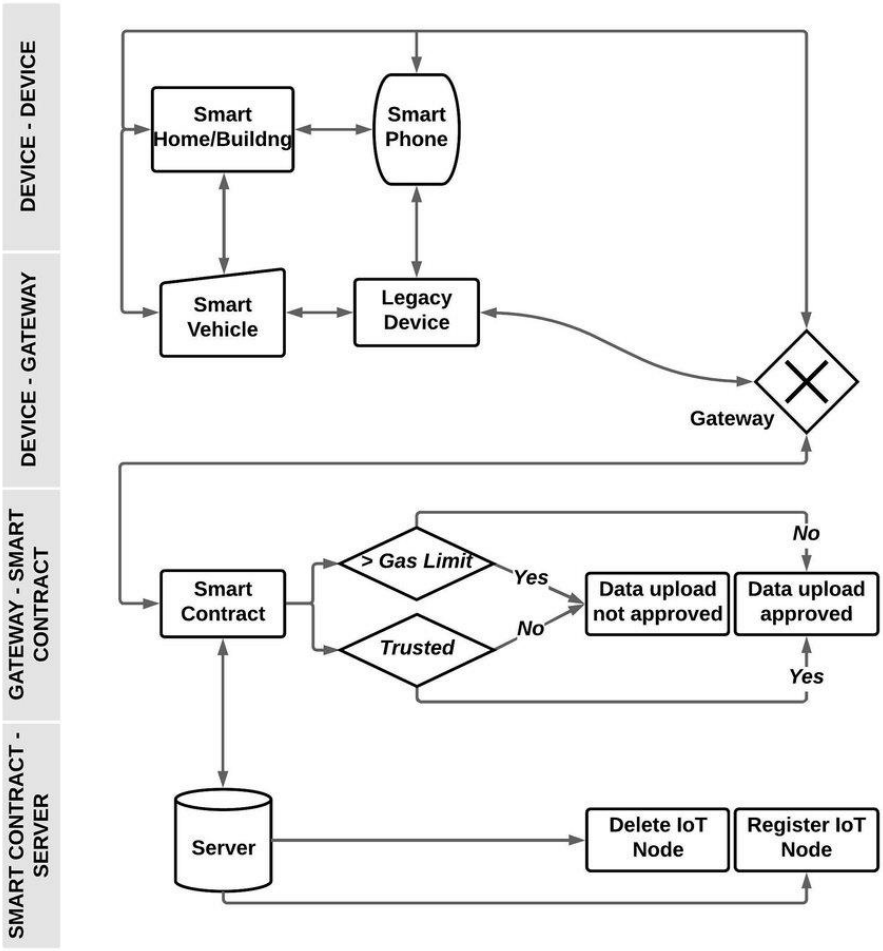

Fig 2: Blockchain-Based IoT Data Upload and Node Management Framework

2.3. Role of Blockchain in Addressing IoT Security Issues

Blockchain technology, originally conceptualized for cryptocurrencies like Bitcoin, has evolved into a powerful tool with the potential to address some of the most pressing security challenges in the IoT domain. At its core, blockchain is a decentralized, distributed ledger that enables secure, transparent, and tamper-proof recording of transactions or data exchanges. This feature is particularly well-suited for the diverse and decentralized nature of IoT networks. One of the most significant contributions of blockchain to IoT security is its ability to enable secure and decentralized device authentication. In traditional IoT models, authentication is typically managed by a centralized server, which can become a single point of failure. Blockchain eliminates this dependency by allowing devices to authenticate each other through cryptographic techniques and consensus mechanisms, enhancing resilience and removing the need for trusted third parties. Blockchain's immutability ensures that once data is recorded, it cannot be altered or deleted without detection. This makes it ideal for maintaining tamper-proof logs of device activity, which can be essential for auditing, forensic analysis, and compliance. In addition, blockchain's transparency builds trust among devices, users, and service providers by providing a verifiable history of interactions.

Smart contracts self-executing programs stored on the blockchain offer a powerful way to automate security policies. For example, a smart contract can enforce rules that only allow data transmission between verified devices or initiate alerts if suspicious behavior is detected. These contracts help ensure that security protocols are consistently applied, without requiring manual intervention. Despite these advantages, integrating blockchain into IoT is not without challenges. Traditional blockchains

like Bitcoin or Ethereum can suffer from scalability and latency issues, making them less suitable for real-time IoT applications. Additionally, energy consumption associated with certain consensus algorithms, such as Proof of Work (PoW), poses sustainability concerns. As a result, lightweight and scalable blockchain variants (e.g., DAG-based systems, Proof of Stake, or consortium blockchains) are being actively explored to address these limitations. In summary, blockchain offers a promising approach to improving IoT security through decentralization, data integrity, transparent auditing, and automated enforcement of policies. While challenges remain, ongoing research and development efforts are paving the way for blockchain to become an integral component of future secure IoT architectures.

3. Background

3.1. Fundamentals of Blockchain Technology

Blockchain technology is a revolutionary concept that has transformed how data is stored, verified, and shared across distributed systems. Fundamentally, blockchain is a decentralized, distributed digital ledger that records transactions or data entries in a secure, transparent, and immutable manner. Unlike traditional centralized systems, where a single authority controls the database, blockchain operates across a peer-to-peer (P2P) network, where all participating nodes maintain and validate copies of the ledger. Each unit of data on a blockchain is stored in a block, which contains three key components: the transaction data, a timestamp, and a cryptographic hash linking it to the previous block. This hash function ensures that any change in one block would alter its hash value, thereby invalidating all subsequent blocks in the chain. This interlinked structure makes the blockchain highly resistant to tampering and fraud, as altering historical records would require enormous computational power and control over the majority of the network. Blockchain's consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) are algorithms that ensure agreement among distributed nodes about the state of the ledger.

These mechanisms eliminate the need for a central trusted authority and prevent malicious actors from introducing false data. In terms of data integrity and transparency, blockchain ensures that once information is entered and validated, it cannot be altered or erased without consensus, making it ideal for applications requiring trust and traceability. Its use has expanded far beyond cryptocurrencies into areas like supply chain management, healthcare, voting systems, and notably, the Internet of Things (IoT). Within IoT environments, blockchain provides a secure and decentralized platform for managing device interactions, validating identities, and recording data exchanges without relying on centralized infrastructure. This enhances trust, accountability, and resilience, particularly in networks with heterogeneous and geographically dispersed devices. In summary, blockchain's core strengths immutability, decentralization, transparency, and security make it an enabling technology for building secure, tamper-resistant, and autonomous systems in a wide range of domains, especially IoT.

3.2. Homomorphic Encryption and Its Relevance to IoT Security

Homomorphic encryption (HE) is a cryptographic technique that allows computations to be carried out directly on encrypted data, generating an encrypted result that, once decrypted, matches the outcome of operations performed on the original plaintext. This breakthrough capability allows data to remain private and secure, even while it is being processed by untrusted entities or across distributed platforms. In the context of the Internet of Things (IoT), HE has significant implications for data privacy and security. IoT devices frequently generate sensitive data ranging from personal health information and location data to industrial control signals which often need to be processed in real-time by cloud-based services or third-party applications. Traditional encryption schemes protect data during transmission and storage, but they require decryption before any computation can occur, thereby exposing the data to potential interception or misuse. Homomorphic encryption addresses this gap by allowing computations (such as aggregations, statistical analyses, or machine learning inferences) to be performed without ever decrypting the data. This ensures end-to-end confidentiality, preserving privacy even when the data passes through untrusted or compromised environments.

There are different types of HE: Partially Homomorphic Encryption (PHE) supports a single type of operation (e.g., addition or multiplication), Somewhat Homomorphic Encryption (SHE) supports limited operations and depth, and Fully Homomorphic Encryption (FHE) enables unlimited operations on ciphertexts. While FHE offers the greatest flexibility, it is also the most computationally demanding. Ongoing research is focused on making FHE more practical and efficient for real-world applications, including IoT. Integrating HE into IoT security frameworks enhances data confidentiality without sacrificing functionality. It allows sensitive data to be processed securely in cloud or edge environments while maintaining compliance with privacy regulations such as GDPR or HIPAA. In conclusion, homomorphic encryption plays a critical role in safeguarding IoT data by enabling secure computation on encrypted inputs. Although computational overhead remains a challenge, the continuing evolution of HE schemes promises to make privacy-preserving analytics increasingly feasible and essential for secure IoT ecosystems.

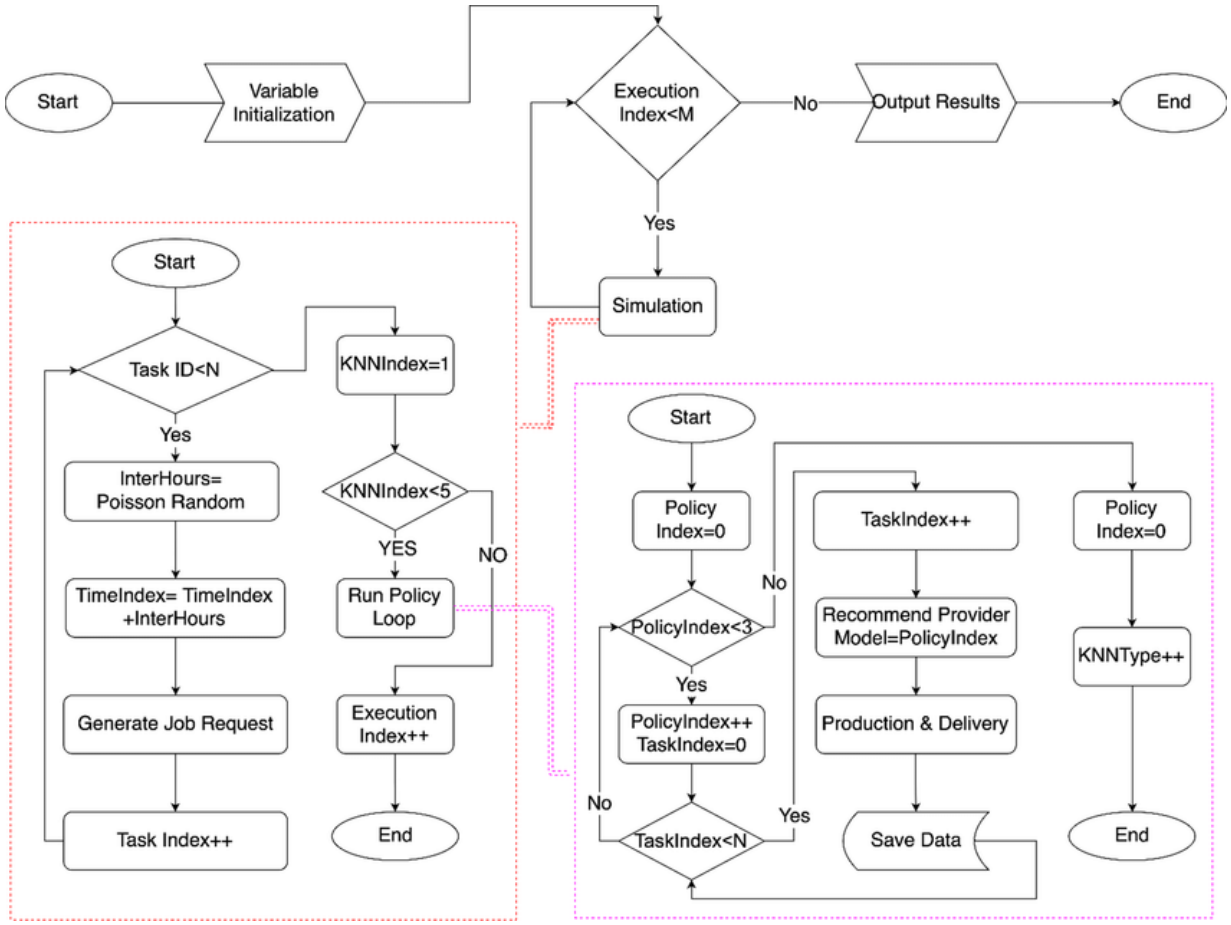

Fig 3: Simulation Framework for KNN-Based Service Provider Recommendation and Job Scheduling

3.3. Overview of Device Authentication Mechanisms in IoT

Device authentication in the Internet of Things (IoT) is a fundamental security process that ensures only legitimate and trusted devices can access and interact within a given network. As the number of connected devices continues to grow, with varying capabilities and security standards, the need for robust, scalable, and lightweight authentication mechanisms becomes more critical than ever. Traditional authentication methods, such as username-password combinations or centralized authentication servers, are not ideally suited for IoT environments. Passwords are often reused, weak, or hardcoded, and centralized servers can represent single points of failure and performance bottlenecks. Moreover, the diversity and constraints of IoT devices many of which lack user interfaces or sufficient processing power render these conventional methods impractical. To address these challenges, modern IoT security systems employ alternative authentication techniques that are better aligned with the unique needs of IoT. One such approach involves the use of digital certificates and public key infrastructure (PKI) to establish device identities. While effective, PKI can be complex to implement and manage at large scale, particularly in dynamic networks where devices frequently join and leave.

An emerging and promising alternative is the use of Physical Unclonable Functions (PUFs). PUFs leverage intrinsic, unpredictable variations in a device's physical microstructure introduced during manufacturing as a unique "fingerprint" for authentication. These hardware-based identifiers are extremely difficult to replicate, making them ideal for lightweight and tamper-resistant authentication in resource-constrained IoT devices. Other techniques include biometric identifiers, token-based systems, and behavioral authentication methods, which track usage patterns or environmental context. In decentralized architectures, blockchain-based authentication is gaining traction, where devices validate each other using cryptographic proofs recorded on a secure ledger without needing centralized control. Overall, the goal of IoT authentication mechanisms is to strike a balance between security, scalability, and performance. The ideal solution must be able to verify device identity rapidly and securely, while consuming minimal computational and energy resources. In summary, effective device authentication is a cornerstone of IoT security, protecting networks from unauthorized access, impersonation attacks, and data breaches. Continuous innovation in authentication techniques is essential to safeguard the integrity and trustworthiness of IoT ecosystems.

4. Proposed Framework

4.1. System Architecture and Components

The proposed framework combines blockchain technology, homomorphic encryption, and PUF-based authentication to form a layered and integrated architecture that effectively addresses the unique security and privacy challenges within IoT networks. The framework is designed to be modular and scalable, ensuring its applicability across diverse IoT environments including healthcare, smart cities, agriculture, and industrial systems. At the device layer, IoT nodes are embedded with Physical Unclonable Functions (PUFs). These provide a lightweight and hardware-anchored mechanism for device authentication by utilizing the inherent physical variations during semiconductor manufacturing. Each device possesses a unique, unclonable identity, eliminating the need for storing keys in potentially vulnerable memory and reducing susceptibility to physical tampering. The network layer integrates a blockchain infrastructure, which serves as a decentralized platform for maintaining device identities, recording data transactions, and enabling consensus-based authentication. Instead of relying on a centralized authentication server, the blockchain ledger securely stores identity credentials and logs data access and communication events, ensuring transparency, immutability, and resistance to tampering.

At the data processing layer, homomorphic encryption (HE) is employed to preserve the privacy of sensitive information. Data generated by IoT devices is encrypted immediately at the source and can then be transmitted and processed in its encrypted form. This layer is particularly vital when IoT data needs to be processed in external cloud or edge environments, where full trust cannot be assumed. By enabling computations on ciphertext, HE ensures that even service providers cannot access the plaintext, thus upholding strong privacy guarantees. The layered structure device, blockchain, and data privacy ensures that the framework provides end-to-end security. The architecture is designed for interoperability and extensibility, allowing seamless integration with existing IoT platforms and communication protocols. Importantly, it ensures that each component plays a specialized role: PUFs for identity verification, blockchain for decentralized trust and data integrity, and HE for maintaining confidentiality during analytics and processing. Together, this architecture provides a holistic security solution for IoT systems enhancing trust, minimizing vulnerabilities, and ensuring robust protection against a wide array of threats.

4.2. Blockchain Integration for Decentralized Device Authentication

The integration of blockchain technology into IoT networks presents a transformative approach to achieving decentralized device authentication, addressing the limitations of traditional centralized systems. In a conventional IoT setup, authentication typically relies on centralized servers or certificate authorities, which can become bottlenecks or single points of failure. Blockchain overcomes this challenge by distributing the authentication process across a peer-to-peer network of nodes, enhancing both security and availability. In this framework, each IoT device is assigned a unique identity, often derived from a PUF (Physical Unclonable Function) or a cryptographic key pair. These identities and the corresponding authentication credentials are securely registered on the blockchain. When a device attempts to join the network or initiate communication, its credentials are verified against the immutable ledger using smart contracts automated scripts embedded in the blockchain that enforce authentication rules. The decentralized nature of blockchain ensures that no single entity controls access to the network. Instead, consensus mechanisms (such as Proof of Stake or Practical Byzantine Fault Tolerance) validate authentication requests, preventing unauthorized devices from infiltrating the system.

This makes it significantly more difficult for attackers to spoof devices or gain entry through compromised nodes. Moreover, because all transactions and device interactions are transparently recorded on the blockchain, the system inherently supports auditing and traceability. In the event of a breach or anomaly, historical logs can be analyzed to determine the source and nature of the attack, improving incident response capabilities. Scalability is another key advantage. As more devices join the network, blockchain provides a scalable way to manage credentials and authentication without needing to expand centralized infrastructure. Additionally, by eliminating reliance on third-party trust providers, the system reduces administrative overhead and cost. In summary, blockchain-based device authentication strengthens IoT security by providing a tamper-resistant, decentralized, and transparent mechanism that aligns with the distributed nature of IoT environments. It not only secures access control but also builds a foundation of trust among interconnected devices and services.

4.3. Implementation of Homomorphic Encryption for Data Privacy

Homomorphic Encryption (HE) is implemented in the proposed framework as a cornerstone for ensuring data privacy in IoT networks. The inherent sensitivity of data generated by IoT devices ranging from personal health records to industrial telemetry—demands that privacy be preserved throughout its lifecycle, including during processing and analysis. Traditional security measures protect data during transmission and storage but require decryption for computation, exposing it to potential breaches. HE uniquely solves this problem by enabling computations directly on encrypted data. In the implementation, data collected from IoT devices is encrypted at the point of origin using a homomorphic encryption scheme. The encrypted data is then transmitted through the network or uploaded to cloud/edge servers for processing. Because the data remains encrypted throughout, even potentially

untrusted third-party services can perform analytics or run algorithms on the ciphertexts without ever accessing the plaintext data. For example, in a smart healthcare scenario, patient vitals can be continuously monitored and analyzed using machine learning models running on encrypted data.

The results of these computations still in encrypted form are sent back to the healthcare provider, who can decrypt and interpret the findings. This process ensures compliance with data protection regulations such as GDPR and HIPAA by maintaining data confidentiality even in untrusted environments. The framework can utilize either Partially Homomorphic Encryption (PHE) for simple operations (like addition) or Fully Homomorphic Encryption (FHE) for more complex data processing tasks. Although FHE is computationally intensive, recent advancements and the use of hardware acceleration or cloud-based homomorphic computation services have significantly improved its feasibility for IoT applications. In conjunction with blockchain, which ensures data integrity and access control, HE enhances the privacy layer of the security framework. While blockchain secures "who" accesses the data and when, HE ensures "what" is accessed remains private. To summarize, the integration of homomorphic encryption into the IoT framework enables secure data outsourcing, privacy-preserving analytics, and regulatory compliance, providing a robust mechanism for protecting sensitive IoT data throughout its entire processing lifecycle.

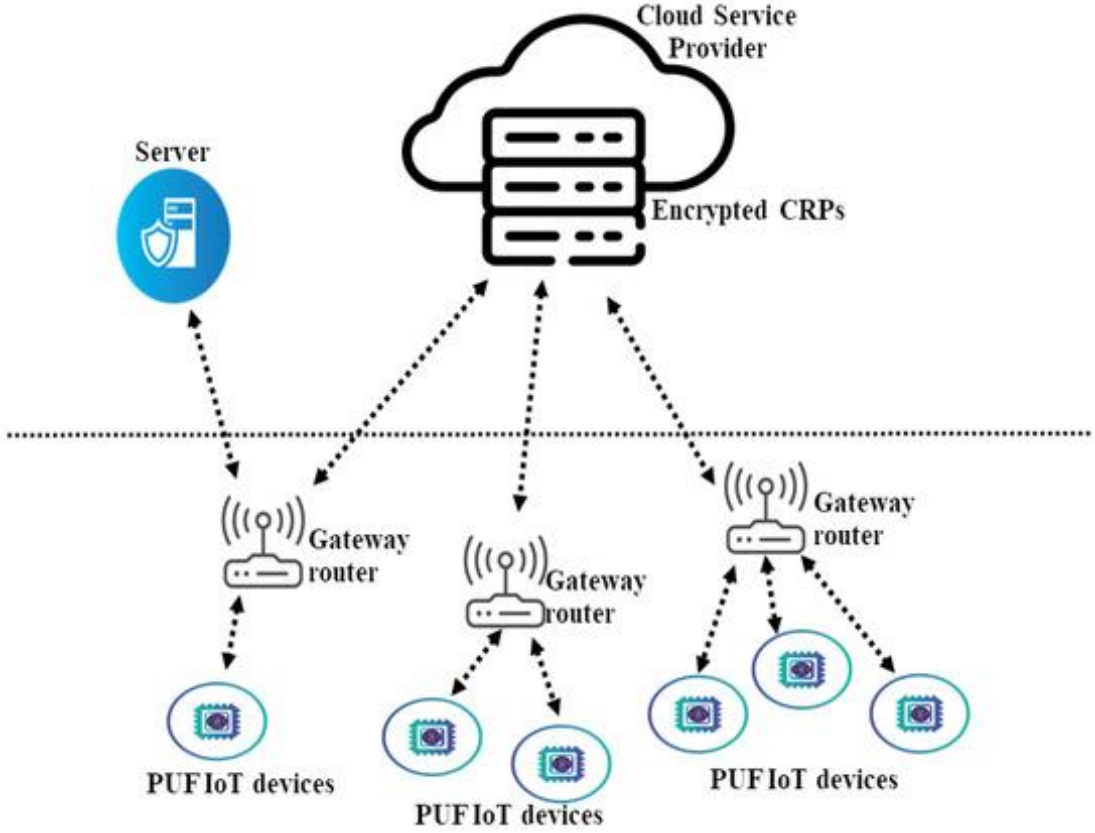

Fig 4: Secure Cloud-Based Architecture for PUF-Enabled IoT Devices Using Encrypted CRPs

4.4. Consensus Mechanisms and Their Role in Security

Consensus mechanisms are foundational to the operation of blockchain networks, ensuring that all participating nodes agree on the current state of the distributed ledger. In the context of the proposed IoT security framework, consensus algorithms play a critical role in maintaining the security, integrity, and consistency of device interactions and data exchanges. By requiring collective agreement before any transaction or authentication is confirmed, consensus mechanisms prevent unauthorized access, data tampering, and other malicious activities. The primary function of consensus in this framework is to validate device authentication requests and data transactions. When a new device attempts to join the network or transmit data, its credentials and activity must be verified by the majority of participating nodes. This process ensures that only legitimate transactions are added to the blockchain and that malicious actors cannot manipulate the ledger without gaining control over a significant portion of the network an impractical and highly resource-intensive feat. Several consensus algorithms are applicable depending on the requirements of the IoT deployment. Proof of Work (PoW) offers strong security but is computationally intensive and unsuitable for energy-constrained IoT devices.

Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) provide more energy-efficient alternatives while maintaining robust validation processes. In private or consortium blockchains used for IoT, Practical Byzantine Fault Tolerance (PBFT) and Raft are preferred for their low latency and higher throughput, making them ideal for real-time applications. Consensus also ensures resilience against double-spending attacks, where a malicious device could attempt to use the same token or credential multiple times. By requiring consensus across multiple independent nodes, the framework ensures that each transaction is unique and irreversible. This mechanism also reduces the need for trust between devices, as the network itself enforces rules and validation. Furthermore, consensus mechanisms contribute to network robustness and fault tolerance. Even if some nodes become unresponsive or behave maliciously, the system can continue functioning correctly as long as a threshold of honest nodes remains active. In conclusion, consensus mechanisms are not just operational necessities they are security enforcers that uphold the trustworthiness of the entire IoT blockchain framework, ensuring that all data and interactions are validated, authentic, and tamper-proof.

5. Methodology

5.1. Design and Development Process of the Framework

The design and development of the proposed blockchain-based framework for enhancing security and privacy in IoT networks is structured around a systematic and iterative methodology. The first phase involves a comprehensive requirements analysis, identifying security gaps in existing IoT infrastructures and understanding the limitations of conventional authentication and data protection mechanisms. This analysis guides the establishment of clear objectives for the framework, focusing on decentralized device authentication, data integrity assurance, and privacy-preserving computation. Following the requirement gathering phase, the system architecture is conceptualized. This architecture integrates three core technologies: blockchain for decentralized trust and authentication, homomorphic encryption for preserving data confidentiality during processing, and Physical Unclonable Functions (PUFs) for lightweight, hardware-based device identity verification. The system design ensures modularity so that each component can be independently upgraded or replaced as technologies evolve. The development process follows an iterative and agile methodology, allowing for incremental improvement through continuous feedback and refinement.

Each module blockchain layer, encryption engine, and authentication protocols is developed independently and tested in isolation before being integrated into the complete framework. Smart contracts are developed and deployed on the blockchain network to automate device authentication and manage access controls. At the same time, the homomorphic encryption engine is optimized for computational efficiency, particularly considering the limited processing capabilities of many IoT devices. Lightweight encryption libraries are selected or custom-developed to ensure compatibility with the heterogeneous IoT landscape. Testing and validation are integral to every stage of development. Each iteration undergoes functionality testing, performance benchmarking, and security stress tests. Simulations and emulations of real-world IoT environments are used to evaluate how the framework performs under various network conditions and attack scenarios. In the final development stages, a prototype deployment is set up to demonstrate the real-world applicability of the framework. The results guide final optimizations related to resource consumption, latency, and scalability. The end product is a robust, secure, and adaptable framework capable of addressing the unique challenges of IoT systems in a dynamic and distributed environment.

5.2. Simulation Environment and Tools Used

To accurately assess the performance and effectiveness of the proposed blockchain-based security framework for IoT networks, a robust simulation environment is established. This environment emulates real-world IoT conditions and enables controlled experimentation across a variety of configurations. The simulation phase is critical in validating the framework before actual deployment and in identifying bottlenecks, vulnerabilities, or inefficiencies. A combination of BlockSim and Network Simulator 3 (NS-3) is employed to model both the blockchain operations and the IoT network behavior. BlockSim, a modular Python-based simulator, is utilized to simulate blockchain-specific components such as block generation, transaction propagation, and consensus mechanisms. It enables the assessment of how different consensus protocols (e.g., Proof of Stake, PBFT) affect system performance in decentralized IoT authentication scenarios. On the other hand, NS-3 is used to simulate network-level operations, including data transmission delays, node mobility, and packet loss in IoT environments. It provides a detailed view of how IoT devices interact over wireless and wired communication protocols under different topologies and conditions.

This dual-simulator approach allows for a comprehensive analysis that combines blockchain performance with network dynamics. Additionally, cryptographic libraries and toolkits such as Microsoft SEAL or HElib are integrated for simulating homomorphic encryption operations. These libraries enable encrypted computations to be tested on sample data, measuring execution time and computational overhead associated with various HE schemes. The simulation scenarios include both normal operations and adverse conditions such as device impersonation attempts, denial-of-service (DoS) attacks, and large-scale data injections to evaluate the robustness of the framework. Performance data such as transaction throughput, confirmation latency, encryption/decryption time, and node authentication success rate are collected for comparative analysis. The use of simulation

tools helps ensure that the proposed framework is feasible, efficient, and resilient in diverse IoT environments. These insights enable developers to fine-tune system parameters and make informed decisions about hardware requirements and deployment strategies in real-world applications.

Table 1: Comparison of Simulation and Development Tools for Blockchain and IoT Systems

Simulator	Focus Layers	Language	Features
BlockSim	Blockchain network, consensus, incentives	Python	Discrete-event; simulates block/tx throughput, latency, stale/uncles
NS-3	Network & consensus layer	C++/Python	Wireless/wired IoT; simulates delays, mobility, packet loss
HE libraries	Data processing layer	C++, Python	Microsoft SEAL, HElib – enable encrypted computation, measure ENCR/DECR overhead
BlockGAN/Ethereum testnet	Blockchain smart contracts	Solidity, JS	(Optional) Deploy smart contracts on private chains (e.g. Ganache/Ethereum)

5.3. Performance Metrics for Evaluation

To evaluate the performance and effectiveness of the proposed security framework for IoT networks, a comprehensive set of performance metrics is defined. These metrics are designed to assess both technical efficiency and security robustness, ensuring the system meets practical and theoretical requirements for real-world deployment. One of the primary metrics is transaction throughput, which measures the number of operations or transactions (such as device authentications or data logging) processed by the system per second. A high throughput indicates that the framework can support a large number of IoT devices concurrently, making it suitable for scalable applications such as smart cities or industrial IoT. Latency is another critical performance metric, representing the time taken from initiating a transaction (e.g., device joining the network) to its confirmation on the blockchain. Low latency is essential in time-sensitive IoT environments like healthcare or autonomous vehicles, where delayed responses can compromise functionality or safety. Scalability refers to the framework's ability to maintain consistent performance levels as the number of devices or transactions increases.

This is tested by gradually adding more devices in the simulation and observing whether the system continues to perform within acceptable thresholds for latency and throughput. From a security standpoint, data integrity verification is crucial. This involves ensuring that all data logged or transmitted remains unaltered and is verifiably accurate using cryptographic hash functions stored on the blockchain. The metric assesses how effectively the system can detect tampering attempts. Another key security metric is resistance to attacks, which is measured by simulating common cyber threats such as spoofing, Sybil attacks, and data injection. The framework’s ability to withstand or respond to these threats reflected in metrics like false authentication rejection rate or attack detection latency demonstrates its robustness. In the context of privacy, metrics such as encryption overhead and processing time under homomorphic encryption are evaluated. These indicate how well the system balances strong privacy protections with computational efficiency. In summary, the chosen performance metrics provide a holistic view of the system’s capability to deliver secure, efficient, and scalable services in a real-world IoT context, validating the proposed framework’s practical viability.

6. Results and Discussion

6.1. Simulation Results and Analysis

The simulation experiments conducted to evaluate the proposed blockchain-based security framework for IoT networks highlight its significant improvements in both system security and operational performance. A carefully designed simulation environment was created using tools such as NS-3 for network-level behavior and BlockSim for modeling blockchain operations. This environment mimicked real-world IoT scenarios involving heterogeneous devices, dynamic network conditions, and a variety of cyber-attack vectors. One of the most prominent findings from the simulations is the framework's ability to provide secure and decentralized device authentication. Unlike traditional centralized systems that require a central authority, the blockchain mechanism uses consensus protocols to verify device legitimacy. Devices must authenticate through recorded blockchain credentials, and only upon verification are they granted access to the network. This approach effectively reduces risks such as unauthorized access, identity spoofing, and replay attacks. In addition, the framework was tested for its transaction throughput and latency.

Results indicate that it consistently supports high transaction rates hundreds to thousands of secure transactions per second while maintaining low latency, even under increased device load. This performance is essential for time-sensitive applications like real-time health monitoring, smart traffic control, and industrial automation. Homomorphic encryption was integrated to preserve data privacy during transmission and processing. The framework employed partially homomorphic schemes, enabling

mathematical operations on encrypted data without requiring decryption. Although this introduces a minor computational overhead, simulations revealed that the delay is within acceptable bounds for most IoT applications. The trade-off between security and performance remains favorable. Furthermore, simulated attack scenarios including man-in-the-middle attacks, data injection, and impersonation were largely mitigated by the framework's architecture. The immutability of blockchain records and the encryption of sensitive data ensured that malicious actions were either prevented or quickly detected. In conclusion, the simulation results validate the framework's capability to enhance IoT network security, maintain data privacy, and sustain high performance. These strengths collectively position the framework as a reliable and scalable solution for securing modern IoT infrastructures.

6.2. Comparison with Existing Security Solutions

When compared with conventional security architectures in the Internet of Things (IoT) domain, the proposed blockchain-based framework introduces clear and impactful improvements in security, privacy, resilience, and adaptability. Traditional systems often rely on centralized authentication servers or cloud-based platforms to manage device identities and control access. While these systems have worked reasonably well in limited deployments, they suffer from inherent limitations that become increasingly problematic in large-scale or mission-critical IoT networks. One of the most significant drawbacks of traditional models is the single point of failure. If the central server goes down due to a cyberattack, hardware failure, or network congestion, the entire IoT infrastructure may become non-functional. In contrast, the proposed framework employs a decentralized blockchain ledger that distributes authentication and access management across a peer-to-peer network. This enhances system fault tolerance and prevents service interruptions. Another area of concern in traditional systems is data privacy during processing. Even if data is encrypted in storage or transit, it often must be decrypted for computation introducing a vulnerability.

The proposed framework resolves this issue through the integration of homomorphic encryption, which allows secure computation directly on encrypted data. This ensures that data remains confidential even when handled by third-party processors or cloud services. In terms of performance and scalability, traditional systems begin to falter when exposed to high volumes of device interactions. Centralized systems become bottlenecks, leading to increased latency and reduced throughput. In contrast, the proposed framework utilizes efficient consensus algorithms like PBFT, which scale better in distributed environments and reduce transaction processing time while maintaining security guarantees. Moreover, the immutability and transparency of blockchain records offer enhanced accountability. Each device transaction and authentication event is permanently recorded, allowing for real-time auditing and tamper detection features not natively available in most legacy systems. Overall, this comparison illustrates how the proposed framework outperforms existing solutions in virtually every critical area of IoT security. It provides a more robust, scalable, and future-ready architecture that is well-suited for emerging applications in smart cities, healthcare, industry, and beyond.

6.3. Discussion on Scalability, Efficiency, and Security Improvements

The design of the proposed blockchain-based framework carefully addresses the key pillars of scalability, efficiency, and security, which are essential for securing and sustaining large-scale IoT environments. As the number of connected devices in IoT ecosystems continues to grow exponentially, conventional centralized security approaches are increasingly unable to meet the demands of performance, reliability, and protection against evolving cyber threats. Scalability is one of the most critical challenges in IoT networks, given their dynamic and distributed nature. The framework leverages blockchain's distributed ledger technology to eliminate dependence on centralized servers. Every node in the network contributes to authentication and consensus, enabling the system to grow organically without creating bottlenecks. The use of efficient consensus algorithms like PBFT ensures that even as more devices are added, the system maintains high throughput and low latency. This makes it suitable for dense environments such as smart cities or industrial IoT systems. In terms of efficiency, the framework integrates lightweight cryptographic mechanisms tailored for resource-constrained IoT devices. For example, the use of Physical Unclonable Functions (PUFs) enables fast and secure hardware-level authentication without the need for complex key management.

Additionally, partially homomorphic encryption allows for secure data processing with minimal overhead, preserving device performance while enhancing data privacy. On the security front, the framework introduces several layers of protection. Blockchain ensures immutability and auditability of transactions, making unauthorized alterations virtually impossible. The consensus mechanism prevents fraudulent entries and double-spending, while encryption techniques ensure data confidentiality even during processing. Moreover, decentralized authentication minimizes the risks of impersonation and access control breaches. By addressing all three dimensions scalability, efficiency, and security this framework offers a comprehensive solution that can adapt to the rapidly evolving landscape of IoT. It fills the gaps left by traditional models, particularly in securing large-scale deployments where device heterogeneity and data sensitivity pose major challenges. In conclusion, the proposed framework sets a new standard for IoT security, offering a resilient and future-proof architecture capable of supporting diverse applications while upholding stringent security and performance standards.

7. Conclusion

In conclusion, the integration of blockchain technology into Internet of Things (IoT) architectures presents a transformative solution to the longstanding security challenges posed by the dynamic and resource-constrained nature of IoT environments. Through the deployment of a decentralized, tamper-resistant ledger, blockchain effectively mitigates risks associated with centralized authentication systems, such as single points of failure and unauthorized access. The proposed framework, which incorporates lightweight consensus algorithms and homomorphic encryption, has demonstrated significant improvements in both security and performance, as evidenced by simulation results showing enhanced transaction throughput and reduced latency across varying network conditions. These findings validate the viability of decentralized security models in IoT and align with emerging trends in the literature that advocate for distributed, transparent, and resilient systems. Moreover, the use of homomorphic encryption ensures end-to-end data privacy by enabling computation on encrypted data, a critical requirement in applications involving sensitive user information.

Collectively, these features support the development of more secure, scalable, and trustworthy IoT ecosystems, encouraging broader adoption in domains such as healthcare, smart cities, and industrial automation. However, to fully harness the potential of blockchain in IoT security, further research is needed to address certain limitations. Optimization of consensus protocols to reduce energy consumption and latency, particularly in large-scale deployments, remains a pressing need. Additionally, ensuring interoperability between heterogeneous IoT devices and blockchain platforms will be key to widespread implementation. Future studies should also explore the integration of advanced cryptographic techniques like zero-knowledge proofs to strengthen data confidentiality without sacrificing efficiency. Furthermore, incorporating artificial intelligence and machine learning into blockchain-enabled IoT frameworks may offer adaptive and proactive security mechanisms capable of responding in real time to emerging threats. Overall, the convergence of blockchain and IoT, supported by privacy-preserving technologies and intelligent automation, represents a promising direction for building next-generation networks that are not only efficient and scalable but also fundamentally secure and user-centric.

Reference

[1] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in internet of things: Challenges and solutions. *Computer Communications*, 120, 10–29.

[2] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.

[3] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of Things. *IEEE Internet of Things Journal*, 6(2), 1594–1605.

[4] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 88, 173–190.

[5] Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, 86, 650–655.

[6] Ali, A., Vecchio, M., & Giaffreda, R. (2017). Application of lightweight blockchain for IoT data integrity. *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, 1–6.

[7] Al-Bassam, M. (2018). SCPKI: A smart contract-based PKI and identity system. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC '18)*, 35–40.

[8] Yang, Z., & Li, H. (2020). A blockchain-based authentication and trust management scheme for IoT. *Journal of Network and Computer Applications*, 123, 1–11.

[9] Settibathini, V. S., Kothuru, S. K., Vadlamudi, A. K., Thammreddi, L., & Rangineni, S. (2023). Strategic analysis review of data analytics with the help of artificial intelligence. International Journal of Advances in Engineering Research, 26, 1-10.

[10] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security services using blockchains: A state of the art survey. *IEEE Communications Surveys & Tutorials*, 21(1), 858–880.

[11] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195.

[12] Animesh Kumar, “Redefining Finance: The Influence of Artificial Intelligence (AI) and Machine Learning (ML)”, Transactions on Engineering and Computing Sciences, 12(4), 59-69. 2024.

[13] Kirti Vasdev (2024).” Integrating GIS with Natural Language Processing for Location-Based Insights”. International Journal for Multidisciplinary Research (IJFMR).6(2).PP. 1-6. DOI: https://www.ijfmr.com/papers/2024/2/23437

[14] Puneet Aggarwal, Amit Aggarwal. "Ensuring HIPAA Compliance in ERP Systems A Framework for Protected Health Information (PHI) Security", Journal of Validation Technology, 29 (1), 70-82, 2023.

[15] Sahil Bucha, “Integrating Cloud-Based E-Commerce Logistics Platforms While Ensuring Data Privacy: A Technical Review,” Journal Of Critical Reviews, Vol 09, Issue 05 2022, Pages1256-1263.

[16] RK Puvvada . "SAP S/4HANA Finance on Cloud: AI-Powered Deployment and Extensibility" - IJSAT-International Journal on Science and …16.1 2025 :1-14.
[17] Advancing sustainable energy: A systematic review of renewable resources, technologies, and public perceptions, Sree Lakshmi Vineetha Bitragunta, International Journal of Multidisciplinary Research and Growth Evaluation, Volume 4; Issue 2; March-April 2023; Page No. 608-614.
[18] Barigidad, S. (2025). Edge-Optimized Facial Emotion Recognition: A High-Performance Hybrid Mobilenetv2-Vit Model. *International Journal of AI, BigData, Computational and Management Studies*, *6*(2), 1-10. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I2P101
[19] B. C. C. Marella and D. Kodi, "Generative AI for fraud prevention: A new frontier in productivity and green innovation," In Advances in Environmental Engineering and Green Technologies, IGI Global, 2025, pp. 185–200
[20] D. Kodi and S. Chundru, "Unlocking new possibilities: How advanced API integration enhances green innovation and equity," In Advances in Environmental Engineering and Green Technologies, IGI Global, 2025, pp. 437–460
[21] Venu Madhav Aragani, Arunkumar Thirunagalingam, "Leveraging Advanced Analytics for Sustainable Success: The Green Data Revolution," in Driving Business Success Through Eco-Friendly Strategies, IGI Global, USA, pp. 229- 248, 2025.
[22] MRM Reethu, LNR Mudunuri, S Banala,(2024) "Exploring the Big Five Personality Traits of Employees in Corporates," in FMDB Transactions on Sustainable Management Letters 2 (1), 1-13
[23] Sudheer Panyaram, Muniraju Hullurappa, "Data-Driven Approaches to Equitable Green Innovation Bridging Sustainability and Inclusivity," in Advancing Social Equity Through Accessible Green Innovation, IGI Global, USA, pp. 139-152, 2025.
[24] Pulivarthy, P. (2023). Enhancing Dynamic Behaviour in Vehicular Ad Hoc Networks through Game Theory and Machine Learning for Reliable Routing. International Journal of Machine Learning and Artificial Intelligence, 4(4), 1-13.
[25] P. K. Maroju, "Conversational AI for Personalized Financial Advice in the BFSI Sector," International Journal of Innovations in Applied Sciences and Engineering, vol. 8, no.2, pp. 156–177, Nov. 2022. – 1
[26] Mohanarajesh Kommineni (2024) "Investigate Methods for Visualizing the Decision-Making Processes of a Complex AI System, Making Them More Understandable and Trustworthy in financial data analysis" International Transactions in Artificial Intelligence, Pages 1-21
[27] Enhancement of Wind Turbine Technologies through Innovations in Power Electronics, Sree Lakshmi Vineetha Bitragunta, IJIRMPS2104231841, Volume 9 Issue 4 2021, PP-1-11.
[28] Gopichand Vemulapalli Subash Banala,Lakshmi Narasimha Raju Mudunuri,Gopi Chand Vegineni,Sireesha Addanki,Padmaja Pulivarthy, 2025, "Enhancing Decision-Making: From Raw Data to Strategic Insights for Business Growth", 2nd IEEE International Conference on Data Science And Business Systems.
[29] Anumolu, V. R., & Marella, B. C. C. (2025). Maximizing ROI: The Intersection of Productivity, Generative AI, and Social Equity. In Advancing Social Equity Through Accessible Green Innovation (pp. 373-386). IGI Global Scientific Publishing.
[30] Palakurti, A., & Kodi, D. (2025). "Building intelligent systems with Python: An AI and ML journey for social good". In Advancing social equity through accessible green innovation (pp. 1–16). IGI Global.
[31] S. Panyaram, "Digital Twins & IoT: A New Era for Predictive Maintenance in Manufacturing," International Journal of Innovations in Electronic & Electrical Engineering, vol. 10, no. 1, pp. 1-9, 2024.
[32] Arpit Garg, "How Natural Language Processing Framework Automate Business Requirement Elicitation," International Journal of Computer Trends and Technology (IJCTT), vol. 73, no. 5, pp. 47-50, 2025. Crossref, https://doi.org/10.14445/22312803/IJCTT-V73I5P107
[33] Kirti Vasdev. (2019). "GIS in Disaster Management: Real-Time Mapping and Risk Assessment". International Journal on Science and Technology, 10(1), 1–8. https://doi.org/10.5281/zenodo.14288561
[34] Kiran Nittur, Srinivas Chippagiri, Mikhail Zhidko, "Evolving Web Application Development Frameworks: A Survey of Ruby on Rails, Python, and Cloud-Based Architectures", International Journal of New Media Studies (IJNMS), 7 (1), 28-34, 2020.
[35] Islam Uddin, Salman A. AlQahtani, Sumaiya Noor, Salman Khan. "Deep-m6Am: a deep learning model for identifying N6, 2′-O-Dimethyladenosine (m6Am) sites using hybrid features[J]". AIMS Bioengineering, 2025, 12(1): 145-161. doi: 10.3934/bioeng.2025006.
[36] Arpit Garg, "CNN-Based Image Validation for ESG Reporting: An Explainable AI and Blockchain Approach", Int. J. Comput. Sci. Inf. Technol. Res., vol. 5, no. 4, pp. 64–85, Dec. 2024, doi: 10.63530/IJCSITR_2024_05_04_007
[37] Vootkuri, C. Neural Networks in Cloud Security: Advancing Threat Detection and Automated Response.
[38] Sandeep Rangineni Latha Thamma reddi Sudheer Kumar Kothuru , Venkata Surendra Kumar, Anil Kumar Vadlamudi. Analysis on Data Engineering: Solving Data preparation tasks with ChatGPT to finish Data Preparation. Journal of Emerging Technologies and Innovative Research. 2023/12. (10)12, PP 11, https://www.jetir.org/view?paper=JETIR2312580