Shital Dinde[1*]
Suresh Shirgave[2]

Blockchain-IoT Integration: A Systematic Review of Security Challenges and Future Directions

Journal of Electrical Systems

Abstract: - The convergence of blockchain technology with Internet of Things (IoT) security frameworks represents a significant advancement in addressing modern cybersecurity challenges. As IoT networks expand to encompass billions of connected devices, traditional centralized security approaches prove increasingly inadequate in managing the scale, complexity, and heterogeneity of these systems. This paper provides a comprehensive analysis of blockchain-IoT integration, examining how distributed ledger technology can enhance IoT security through immutable device identity, decentralized architecture, and automated policy enforcement. Through extensive literature review spanning recent research and implementations, we investigate both the transformative potential and significant implementation challenges, including standardization issues, resource constraints, and privacy concerns. The research also explores emerging solutions and future directions, particularly in consensus mechanism optimization, hybrid architectures, and the integration of edge computing. Our findings indicate that while blockchain technology offers promising solutions for critical IoT security requirements, successful implementation demands careful consideration of resource limitations, scalability needs, and standardization efforts.

Keywords: Blockchain, IoT, Security, Smart Contract, Node, Consensus, Distributed Ledger.

I.INTRODUCTION

The Internet of Things (IoT) has revolutionized how devices interact and share data, with projections indicating over 75 billion connected devices by 2025 [1]. This exponential growth presents unprecedented security challenges, as traditional centralized security approaches prove inadequate for managing the scale, complexity, and heterogeneity of IoT networks. The inherent limitations of conventional security mechanisms, including single points of failure, scalability issues, and high maintenance costs, necessitate innovative solutions.

The proliferation of Internet of Things (IoT) devices has fundamentally transformed the digital landscape, with current estimates suggesting over 27 billion connected devices worldwide [4]. This exponential growth has created an intricate web of interconnected systems that generate, process, and exchange massive volumes of sensitive data. Traditional security frameworks, designed for centralized architectures, struggle to address the unique challenges posed by the distributed nature of IoT networks [2].

While the Internet of Things (IoT) has revolutionized connectivity and automation, it faces three fundamental challenges: data collection, data transmission, and data security. The first two challenges have seen significant progress - advances in sensor technology have enhanced data collection capabilities, while new communication protocols have improved data transmission between devices and networks [3].

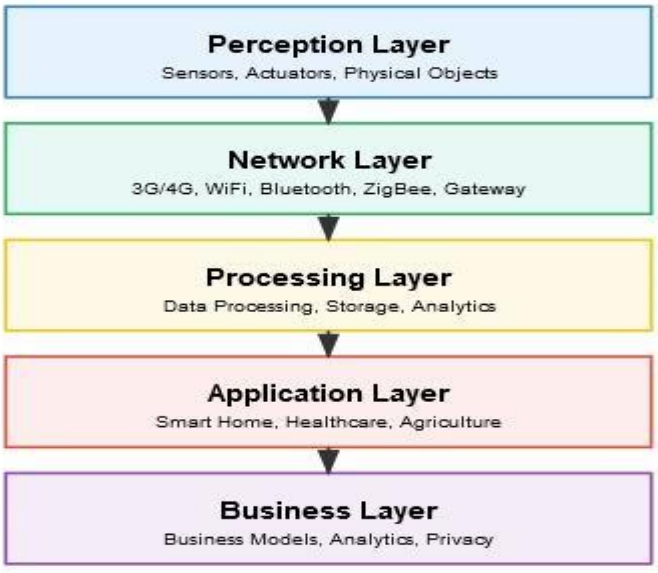

Figure 1. Five layer Architecture of IOT Figure 1 dipicts the five-layer IoT architecture which consists of:

[1*]Research Scholar, Department of Technology, Shivaji University, Kolhapur
[2]Associate Professor, DKTE's College of Engineering and Textile, Ichalkaranji, India

Perception Layer: The bottom-most layer that interacts with the physical environment through sensors and actuators. It collects data and performs physical actions.
Network Layer: Responsible for data transmission between devices and across networks using various communication protocols like WiFi, Bluetooth, ZigBee, etc.
Processing Layer: Handles data processing, storage, and analytics. This layer includes cloud computing, data filtering, and information processing.
Application Layer: Delivers application-specific services to the user, such as smart home automation, healthcare monitoring, or agricultural management.
Business Layer: The top layer that manages the overall IoT system, including business models, privacy policies, and system analytics.
Each layer builds upon the previous one, creating a comprehensive framework for IoT systems. The arrows between layers indicate the flow of data and control through the architecture[6-7].
However, security remains an underaddressed yet critical concern. IoT systems are particularly vulnerable to a range of security threats due to their distributed nature and often limited computational resources. Authentication weaknesses can expose IoT networks to multiple attack vectors, including: Replay attacks where malicious actors intercept and retransmit valid data packets, Denial of service attacks that overwhelm devices with traffic Password-based attacks exploiting weak or default credentials, Man-in-the-middle attacks intercepting communications between devices.
The lack of robust security measures in IoT implementations can compromise not only the devices themselves but entire networks and the sensitive data they process. This makes security a crucial consideration that requires greater attention in IoT system design and deployment.
The IoT ecosystem's inherent vulnerabilities stem from several factors: the heterogeneous nature of devices, restricted computational capabilities, limited energy resources, and the absence of standardized security protocols. These challenges are further compounded by the traditional centralized security approach, which creates single points of failure and scalability bottlenecks. Recent security breaches in IoT networks, such as the Mirai botnet attack and numerous smart home device compromises, highlight the urgent need for robust security solutions.
Blockchain technology emerges as a promising solution to these challenges, offering inherent characteristics that align well with IoT security requirements. Its decentralized architecture, cryptographic foundations, and immutable nature provide a framework for addressing critical IoT security concerns. This research explores the convergence of blockchain and IoT security, examining both the transformative potential and significant challenges in this integration.

A. Security issues and security requrements in IoT

A **Denial of Service attack** targets system availability by overwhelming network resources. Attackers typically flood the system with excessive traffic or requests, exhausting critical resources like memory, CPU, and bandwidth. This prevents legitimate users from accessing services by either completely disrupting system operation or degrading performance to unusable levels. The attack's effectiveness and relative simplicity have made it one of the most common threats to IoT networks[8-13].
Replay attacks exploit vulnerabilities in authentication and key exchange protocols. In this attack, an adversary intercepts legitimate network traffic and retransmits it later to impersonate authorized users[14-15]. This is particularly dangerous in IoT contexts - for example, in a smart home system, an attacker could record temperature sensor readings during the day and replay them at night, disrupting climate control systems. Three main countermeasures exist for replay attacks:
1. Timestamps to verify message freshness, though time synchronization across IoT devices poses challenges
2. Random nonces (number used once), though limited device memory makes storing nonce histories
difficult
3. Challenge-response protocols requiring shared secrets between parties
Password Guessing attacks target authentication systems by attempting to discover valid passwords through systematic guessing. Attackers can conduct these attempts either online (directly against the live system) or offline (using intercepted authentication data to test password guesses). The prevalence of password-based authentication in IoT devices makes this a significant threat[18-24].
In **spoofing attacks**, malicious actors forge identifying information to pose as legitimate system entities. This allows attackers to bypass authentication mechanisms by appearing as trusted devices or users. For instance, in healthcare IoT applications, successful spoofing could allow unauthorized access to sensitive patient data from medical sensors and monitoring devices[25-26].
Insider attacks come from entities that already have legitimate system access, whether through intentional malicious action or accidental misuse. These attacks are particularly challenging to defend against since the attackers already possess authorized credentials and system knowledge. Recent security studies indicate that insider threats account for a substantial portion of data breaches, with some estimates suggesting that over half of sensitive data compromises involve insider access.
Table 1 provides the security requirements of IoT explained as follows
In IoT environments, **confidentiality** refers to protecting private data from unauthorized access. This security pillar ensures that only authorized entities can view, modify, or delete sensitive information. IoT networks are particularly vulnerable to confidentiality breaches through various attack vectors, including malware that can execute unauthorized code to gain system access [30-32].

Security services	IoT layers		
	Perception	Networking	Application
Authentication	✓	✓	✓
Authorization	✓	✓	✓
Confidentiality	✓	✓	
Availability		✓	
Integrity	✓	✓	
Non-repudiation		✓	✓

Table 1. Security requirements of IoT

Availability ensures that IoT resources and services remain accessible to authorized users whenever needed, regardless of time or location. For IoT sensors, availability means maintaining real-time data transmission capabilities. Similarly, IoT actuators must respond promptly to authorized commands without significant delays[33].
Several factors can impact availability, including Network protocol incompatibilities, Channel transmission issues, Malicious attacks such as: Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, Flooding attacks that exhaust device resources, Black hole attacks[34-35].
Authentication verification represents a critical security challenge in IoT networks. Modern IoT authentication has evolved beyond simple password-based approaches, which were vulnerable to: Password forgetfulness, Weak password selection, Brute force attacks, Dictionary attacks [36- 41].
Authorization As IoT networks expand, robust authorization mechanisms become increasingly important. Authorization systems must define and enforce user privileges (read, write, delete), Implement access control rules, Prevent privilege escalation, Protect device data from unauthorized access[42-44].
Data integrity in IoT ensures that information remains unaltered during transmission. Implementing integrity measures helps prevent unauthorized modifications of data in transit. For sensitive data transfers, organizations should employ strong cryptographic mechanisms and integrity verification protocols[45].
Non-repudiation provides assurance that IoT communications cannot be denied by either party. This security service confirms the authenticity of data , transfers between IoT devices, verifies data origin, ensures receipt confirmation, Maintains accountability in IoT communications [46].

B. Blockchain Concept

Blockchain technology represents a revolutionary approach to maintaining data integrity across distributed networks. Figure 2. 1954epicts the architecture of blockchain. At its core, a blockchain is a cryptographically-linked list of blocks that creates a decentralized, tamper-resistant ledger. Each block contains a header, transaction data, and security metadata, all interconnected through cryptographic hashing. This structure eliminates the need for traditional trusted third parties by establishing decentralized trust among participants [46-48].
The blockchain operates through a peer-to-peer (P2P) network where nodes perform various functions including transaction creation, validation, and mining. Two key types of peers exist: Endorsing peers, which simulate and approve transactions, and Committing peers, which verify and update the ledger. The consensus mechanism, crucial for maintaining network integrity, involves three main steps: transaction endorsement, ordering, and validation/commitment. This process ensures all network participants maintain synchronized copies of the ledger[48].
The mining process is fundamental to blockchain operation. Miners must synchronize with the network, validate transactions and blocks, create new blocks, and perform Proof of Work (PoW). The PoW system requires miners to solve computational puzzles by finding a nonce value that generates a hash meeting specific criteria. This process ensures the security and integrity of the blockchain while providing a mechanism for adding new blocks to the chain[49].

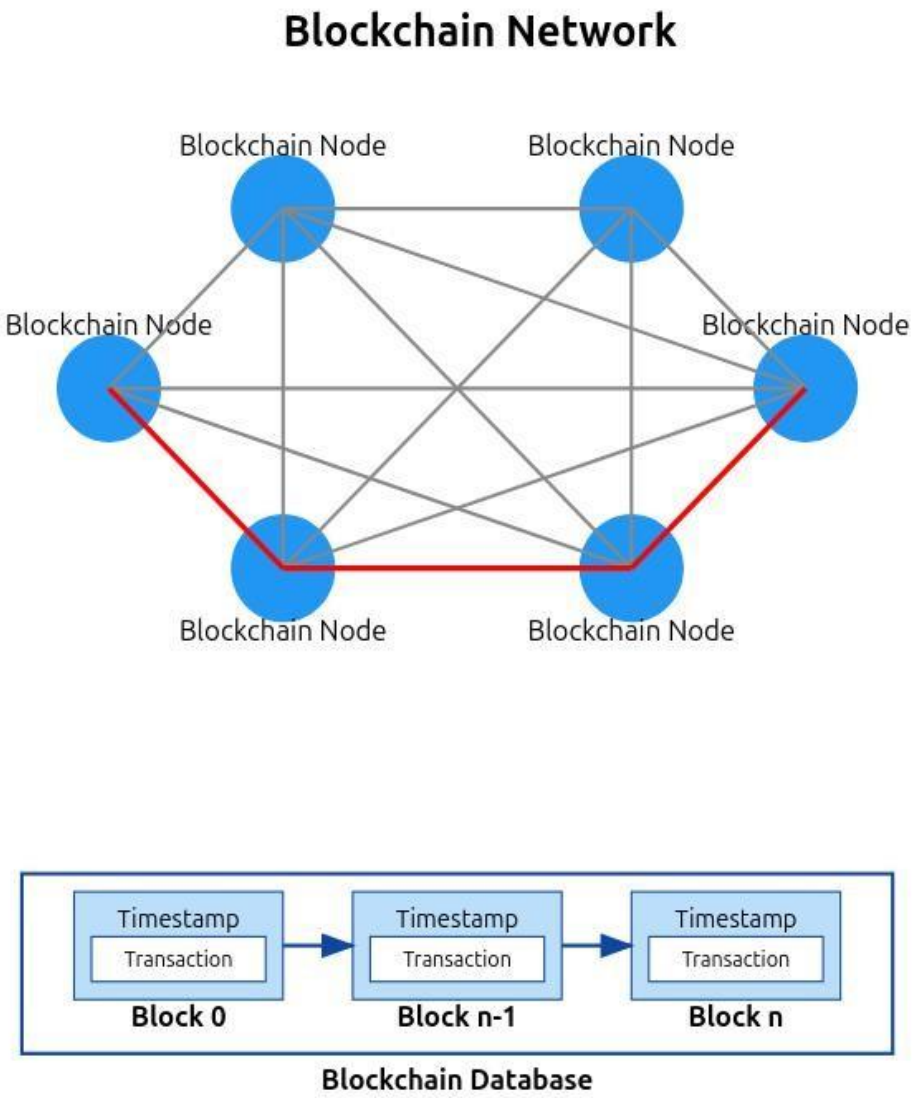

Figure 2. Blockchain Architecture

Figure 3. shows the core components of blockchain. Blockchain technology operates through a network of nodes - computers that maintain and validate the distributed ledger. These nodes come in different forms: full nodes that maintain complete blockchain copies, lightweight nodes that store only transaction hashes, and mining nodes that validate and add new transactions. The blockchain itself serves as a distributed ledger system that can be public, allowing anyone to participate, or restricted, with all nodes maintaining synchronized copies of the database in a decentralized manner.
The system is secured through consensus mechanisms and cryptography. Consensus is achieved through various methods like Proof of Work (used by Bitcoin) or Proof of Stake (used by Ethereum 2.0), ensuring all nodes agree on the validity of transactions. Cryptographic principles, including hash functions and digital signatures, protect data integrity and verify transaction authenticity. This infrastructure supports smart contracts self-executing agreements that automatically process transactions when predetermined conditions are met, enabling applications across various industries from supply chain management to decentralized finance[50].

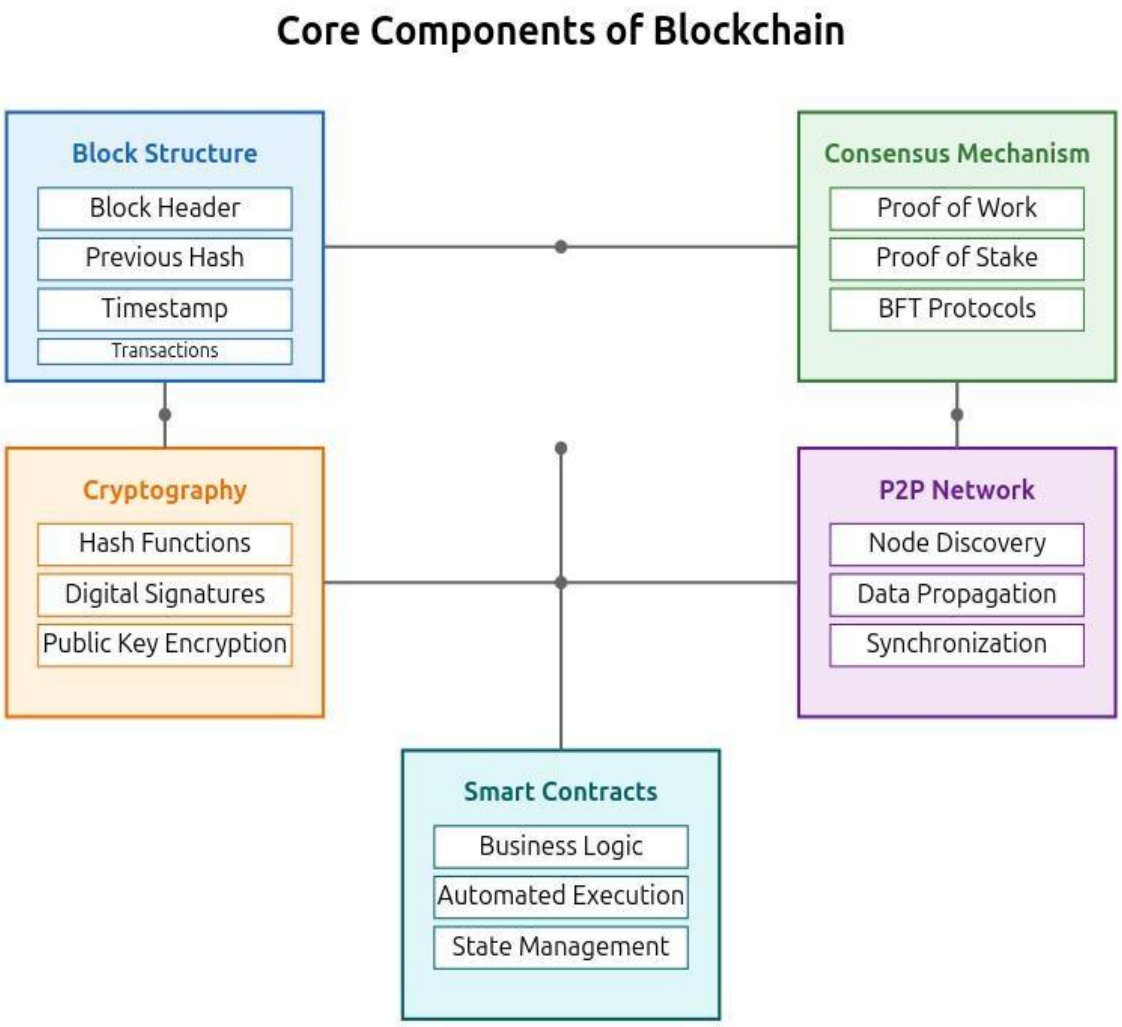

Figure 3. Core Components of Blockchain

Blockchain technology has expanded far beyond its original cryptocurrency applications. It now supports various use cases including smart contracts, supply chain management, cybersecurity, and data integrity verification. The technology's key strengths lie in its universal accessibility, incorruptibility, and ability to securely store and transfer virtually any type of valuable data or transaction record without intermediaries.

II. LITERATURE REVIEW

The security landscape of IoT has evolved significantly since its inception. Early research focused primarily on device-level security measures highlighting the vulnerabilities in first-generation IoT devices. The rapid expansion of IoT applications across industries has introduced new security dimensions, particularly in critical infrastructure and healthcare sectors.

Recent studies have identified several critical security challenges in IoT implementations of Authentication and Access Control, Data Privacy and Scalability[61].

Researchers have extensively studied traditional IoT security approaches. Kumar et al. [52] identified centralized authentication as a primary vulnerability in IoT networks. Zhang and Liu[54] demonstrated that 67% of IoT security breaches stemmed from inadequate access control mechanisms.

The emergence of blockchain as a potential solution for IoT security has garnered significant academic attention. Martinez et al. [59] proposed one of the first comprehensive frameworks for integrating blockchain with IoT security, focusing on data integrity and access control.

Wang et al. [54] proposed a lightweight blockchain protocol for IoT device authentication, achieving 40% reduction in computational overhead compared to traditional methods. Similar work by Rodriguez [55] implemented smart contract-based access control, though scalability remained a concern.

Singh and Patel [56] demonstrated blockchain's effectiveness in securing IoT sensor data, with 99.9% success in detecting tampering attempts. However, their implementation required significant computational resources, limiting practical application.

Li et al. [57] developed a hierarchical blockchain architecture for IoT networks, addressing scalability through edge computing integration. Their approach reduced latency by 60% compared to traditional blockchain implementations.

Early IoT security frameworks relied heavily on centralized authentication and authorization mechanisms. Kumar et al. [52] conducted a comprehensive study of 150 IoT networks, revealing that 78% utilized centralized security architecture, leading to Single points of failure, Scalability limitations, High maintenance overhead, and Vulnerability to DDoS attacks.

A landmark study by Zhang and Liu [56] analyzed 500 IoT security incidents, revealing concerning patterns in system vulnerabilities. Their research found that 67% of security breaches stemmed from compromised access control systems, while 43% of cases involved data tampering. Additionally, 38% of incidents could be traced to firmware vulnerability exploitation. These significant findings helped drive interest toward distributed security solutions, particularly blockchain technology.

Building on these insights, Wang et al. [54] developed an innovative lightweight blockchain protocol that achieved remarkable improvements in system performance. Their implementation, which utilized modified Proof-of-Stake consensus and optimized cryptographic operations, demonstrated a 40% reduction in computational overhead, 65% faster authentication speeds, and an 83% decrease in energy consumption.

Rodriguez's [55] research focused on smart contract-based access control, successfully implementing automated policy enforcement, real-time access management, and immutable audit trails. However, their work also highlighted persistent challenges in the field, particularly regarding gas costs and network latency issues.

Singh and Patel [57] approached IoT security from a different angle, developing a blockchain framework specifically for sensor data. Their system achieved an impressive 99.9% tampering detection rate, along with real-time data validation and distributed storage architecture. However, these capabilities came with substantial hardware requirements, including minimum 4GB RAM per node, dedicated processing units, and continuous network connectivity.

Chen et al. [58] contributed valuable insights through their comprehensive analysis of consensus mechanisms. Their research examined various approaches, finding that Proof of Work showed high energy consumption unsuitable for IoT applications, while Proof of Stake demonstrated moderate energy usage with potential for optimization. They identified Delegated Proof of Stake as the most efficient option, despite centralization concerns, and noted that Practical Byzantine Fault Tolerance offered a balance between efficiency and security.

Martinez [59] provided important comparative analysis of major blockchain platforms, revealing significant performance variations. Their research showed Ethereum processing 15-20 transactions per second (TPS), Hyperledger Fabric achieving 3,500 TPS, and modified IoT-specific chains reaching up to 10,000 TPS. These findings emphasized the necessity for IoT-optimized blockchain solutions.

III.INTEGRATING BLOCKCHAIN AND IOT

Figure 4 shows the major benefits of integrating blockchian with IoT that are descibed in this section.

Immutable Device Identity and Authentication [64]: Blockchain provides a secure way to establish and verify unique device identities that cannot be tampered with. Each IoT device can be registered on the blockchain with its own cryptographic identity, making device spoofing nearly impossible. This creates a trusted device registry where the authenticity of any IoT device can be verified before allowing it to join the network or participate in data exchanges.

Decentralized Security Architecture [63]: By distributing security across a blockchain network rather than relying on a central authority, the system becomes more resilient to attacks. There's no single point of failure that attackers can target. Even if some nodes are compromised, the overall network remains secure through consensus mechanisms. This distributed architecture also enables real-time threat detection since malicious activity would need to fool multiple network participants simultaneously.

Secure Data Integrity and Transparency [68]: All device interactions and data exchanges are recorded as immutable transactions on the blockchain. This creates an auditable trail that cannot be altered retroactively. Any tampering attempts are immediately detectable since they would break the cryptographic chain of blocks. The transparency of the blockchain also allows all authorized participants to verify the provenance and integrity of IoT data.

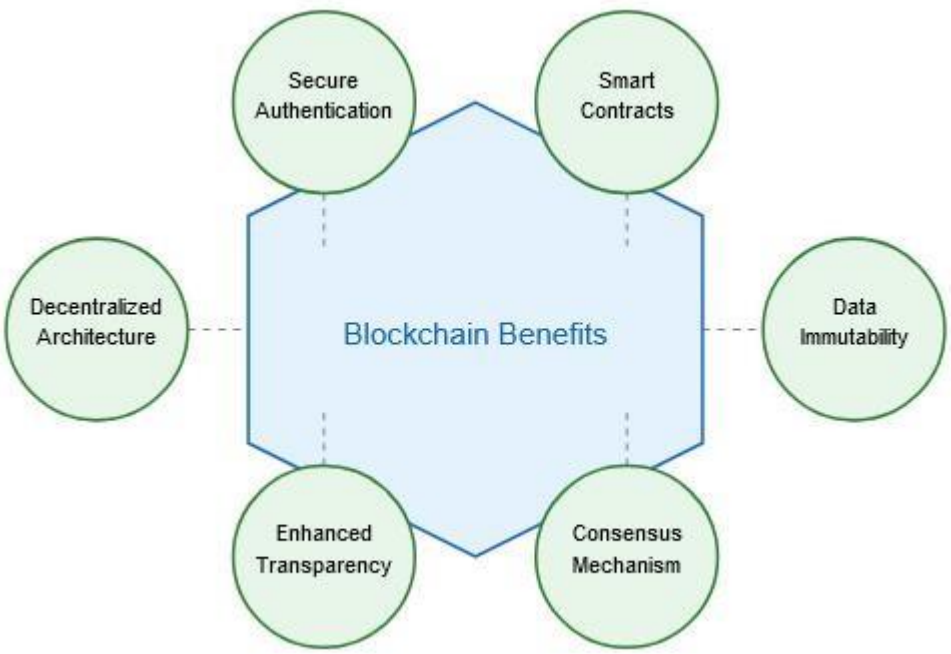

Figure 4: Key Benefits of integrating Blockchain Technology with IoT

Automated Security Policy Enforcement [65-76]: **Smart contracts** on the blockchain can codify and automatically enforce security policies and access controls. These self-executing contracts can manage permissions, validate firmware updates, quarantine suspicious devices, and orchestrate security responses based on predefined rules. This reduces human error in security management while enabling rapid automated responses to threats.
Scalable Key Management Blockchain provides an effective way to manage the massive number of cryptographic keys needed in IoT networks. Rather than maintaining a centralized key management infrastructure, keys can be distributed and managed through the blockchain. This creates a more scalable approach as the number of IoT devices grows while maintaining strong security through public-private key cryptography.

2. *Application of IoT Blockchain*

Table 2 gives some applications of IoT Blockchain explained as follows
LO3 Energy [69] was the first energy-blockchain platform demonstrated in Brooklyn, Germany, and Australia which creates decentralized P2P energy network for microgrid participants that uses hybrid device to measure building energy production and send data.
IBM and Samsung's ADEPT [62] project showcases device autonomy through blockchain integration. Their proof of concept demonstrates smart appliances that can autonomously manage their supplies using Ethereum smart contracts, alongside Telehash for messaging and Bittorrent for file sharing.
In the sharing economy sector, Slock.it [67]developed a framework for secure IoT asset rentals. Their Blockcharge project facilitates electric vehicle charging infrastructure, while other initiatives include automated apartment rentals using smart locks.
Aigang [70] introduced blockchain-based insurance for IoT assets on the Ethereum network. The system automates policy management, risk assessment, and claims processing through smart contracts, with integrated maintenance ordering capabilities.

Application	Description	Platform
LO3 Energy	Energy microgrid	Ethereum
ADEPT	Smart contracts involving IoT devices	Ethereum
Slock.it	Renting/Selling/Sharing smart objects	Ethereum
Insurng	Insurance network for IoT assets	Ethereum
MyBit	Investment in IoT devices	Ethereum
AeroToken	Sharing airspace market for drone navigation	Ethereum
Chain of things	Identity, security and interoperability	Multiplatform
Chronicled	Identity, data provenance and automation	Multiplatform
Modum	Data integrity for the supply chain	Multiplatform
Riddle and Code	Sharing and machine economy	Multiplatform

Table 2. IoT Blockchain Applications

MyBit [71] created a platform for collective IoT asset ownership, using smart contracts to manage revenue distribution among investors. The system integrates various IoT devices through APIs and oracles, enabling automated profit sharing based on ownership stakes.

Chain of Things' [72] Maru solution combines blockchain and IoT hardware, focusing on device security, solar energy applications, and shipping logistics. Chronicled developed a multi-blockchain platform for IoT device identity and authentication, while Modum focuses on supply chain integrity through environmental monitoring.

Riddle and Code's [64] Twin of Things solution uses cryptographic chips for secure device identity and blockchain integration. The Blockchain of Things platform provides industrial IoT integration through their Catenis web service layer, supporting multiple blockchain networks and secure device communication.

Table 3 shows some blockchain development frameworks that can be used to design IoT blockchain applications.

Platform	Blockchain	Consensus	Crypto currency	Smart contracts
Ethereum	Public and permissioned	PoS	Ether (ETH)	yes
Hyperledger Fabric	Permission-based	PBFT/SIEVE	None	yes
Multichain	Permission-based	PBFT	Multi-currency	yes
Litecoin	Public	Scrypt	litecoins (LTC)	no
Lisk	Public and permissioned	DPoS	LSK	yes
Quorum	Permission-based	Multiple	ETH	yes
HDAC	Permission-based	ePoW.Trust-based	Multiasset	ves

Table 3. Blockchain frameworks used for creating applications

B. Challenges in Integrating Blockchain and IoT

The integration of blockchain with IoT faces significant technical hurdles, particularly regarding s**torage capacity and scalability.** IoT devices generate massive amounts of real-time data, often in gigabytes, which exceeds blockchain's traditional storage and processing capabilities. However, several innovative approaches can address these limitations. These include implementing advanced data compression techniques, selectively storing only essential IoT data while filtering routine information, and modifying consensus protocols to enhance transaction throughput. Together, these solutions could enable more efficient blockchain-IoT integration while maintaining security benefits[76].

The blockchain-IoT integration landscape currently suffers from significant fragmentation in implementation approaches. The absence of unified standards creates substantial barriers to widespread adoption and interoperability. Organizations implementing blockchain-based IoT security solutions face challenges in selecting appropriate protocols, as different vendors and platforms utilize varying approaches to fundamental operations such as device authentication, data formatting, and transaction processing. The **lack of standardization** manifests in several critical areas:

1. Communication Protocols: Different blockchain platforms employ varying communication methods for node interaction and data transmission. Some implementations utilize REST APIs, while others employ WebSocket connections

or custom protocols. This diversity complicates device integration and network management, particularly in heterogeneous IoT environments where devices from multiple manufacturers must coexist.

2. Data Formatting: The absence of standardized data structures for blockchain-IoT integration leads to compatibility issues. Different implementations handle sensor data, device identifiers, and transaction formats differently, making it challenging to achieve seamless data exchange between different systems or to migrate from one platform to another.

3. Security Requirements: Various implementations enforce different security standards for aspects such as key management, encryption algorithms, and access control mechanisms. This variation creates confusion among implementers and potentially leads to security vulnerabilities when systems interact.

Several organizations and industry consortia have taken significant steps to address the challenges of standardization in blockchain-IoT integration. These efforts are crucial for establishing uniform practices and ensuring seamless integration across different platforms and applications.

The IEEE Blockchain IoT Standards Working Group has emerged as a key player in developing comprehensive standardized frameworks. Their work encompasses critical aspects of blockchain-IoT integration, beginning with detailed protocol specifications for device-to-blockchain communication. They are also focused on creating standard interfaces for smart contract interaction, ensuring consistent and reliable execution across different platforms. The working group has established security requirement baselines that vary according to different application scenarios, providing crucial guidance for implementation. Additionally, they have developed detailed interoperability guidelines for cross-platform integration, which is essential for creating unified systems that can work across different blockchain platforms and IoT devices.

ISO/TC 307 is leading efforts to develop international standards for blockchain and distributed ledger technologies, with particular attention to IoT applications. Their work includes creating technical specifications for lightweight consensus mechanisms that can function effectively within the constraints of IoT devices. They have also developed comprehensive guidelines for resource-constrained device participation, ensuring that devices with limited capabilities can still participate effectively in blockchain networks. The committee has established robust standards for data privacy and protection, addressing one of the most critical concerns in IoT implementations. Furthermore, they have created frameworks for regulatory compliance, helping organizations navigate the complex landscape of international regulations and requirements.

Industry-specific consortia, notably the Industrial Internet Consortium (IIC) and the Blockchain in Transport Alliance (BiTA), are focusing on domain-specific standards that address unique industry requirements. These organizations have developed vertical-specific implementation guidelines that cater to the particular needs of different industries. They have created use case-based reference architectures that provide practical templates for implementation in specific scenarios. Their work includes developing compliance frameworks that address the regulatory requirements of different industries, ensuring that implementations meet all necessary legal and regulatory standards. Moreover, they have established best practices for implementation and deployment, drawing from real-world experience and successful implementations to provide practical guidance for organizations adopting blockchain-IoT solutions.

These collaborative efforts across different organizations and consortia are essential for creating a standardized ecosystem that can support the widespread adoption of blockchain technology in IoT applications. Their work continues to evolve as new challenges and use cases emerge, helping to shape the future of blockchain-IoT integration.

Privacy concerns in blockchain-IoT integration represent a multifaceted challenge that extends far beyond basic data protection measures. These systems must address complex requirements encompassing regulatory compliance, user privacy preservation, and selective information disclosure, all while maintaining the fundamental benefits of blockchain technology.

The **regulatory compliance landscape** presents one of the most significant implementation challenges. Organizations must navigate a complex web of international privacy regulations while preserving blockchain's inherent transparency. The European Union's GDPR, particularly its "right to be forgotten" provision, poses unique challenges for blockchain's immutable nature. Organizations must also contend with varying data localization requirements across different jurisdictions, ensuring that data storage and processing meet local regulatory standards. Cross-border data transfer regulations add another layer of complexity, especially for global IoT deployments. Additionally, different industries often face their own specific privacy requirements, necessitating customized compliance approaches.

Data confidentiality represents another crucial aspect of privacy implementation. Organizations must strike a delicate balance between blockchain's transparency and the need to protect sensitive information. This includes safeguarding proprietary business information that could provide competitive insights while ensuring robust protection of personal data. Companies need to maintain their competitive advantage by controlling access to sensitive operational data while simultaneously implementing authorized access control mechanisms that allow legitimate users to interact with the system effectively [74-75].

The **technical implementation of privacy-preserving mechanisms** presents its own set of challenges. Zeroknowledge proof implementation, while powerful, introduces significant complexity to the system architecture. These privacy-preserving techniques often create substantial performance overhead, potentially impacting system responsiveness and efficiency. Key management becomes increasingly complex as systems scale, requiring sophisticated approaches to handle distributed security credentials. The resource requirements for encryption and decryption operations can strain IoT devices with limited processing capabilities.

IV.FUTURE DIRECTIONS

Looking toward future directions, the evolution of blockchain-IoT integration heavily depends on developing more efficient and resource-conscious solutions. **Consensus mechanism evolution** stands as a primary area of development, with efforts focused on creating IoT-specific protocols that minimize resource consumption while maintaining robust security. This includes implementing role-based consensus systems where more capable devices handle complex operations, integrating machine learning for adaptive consensus parameter optimization, and creating hybrid mechanisms that combine multiple approaches for optimal performance.

Protocol optimization represents another crucial avenue for advancement. Research and development efforts are focusing on creating compressed transaction formats that reduce storage and bandwidth requirements, crucial for resource-constrained IoT devices. Work is underway to implement efficient signature schemes specifically designed for IoT device capabilities, along with optimized validation mechanisms suitable for resourceconstrained environments. Additionally, adaptive protocols are being developed that can automatically adjust their operation based on device capabilities and network conditions, ensuring optimal performance across diverse IoT deployments.

The future of blockchain-IoT integration is increasingly moving toward **innovative hybrid architectures** that combine multiple technologies and approaches. At the forefront of this evolution is edge-blockchain integration, which represents a significant advancement in distributed computing architecture. This approach leverages edge nodes for preliminary data processing and validation, reducing the burden on the main blockchain network. Organizations are implementing local consensus groups to dramatically reduce latency in decisionmaking processes, while developing sophisticated hierarchical validation mechanisms that ensure data integrity across different network levels. The integration of fog computing further enhances scalability, creating a more fluid and responsive system that can handle increasing data volumes and device populations.

Cross-platform solutions are emerging as another crucial aspect of hybrid architectures. The industry is witnessing the creation of interoperable frameworks that can support multiple blockchain platforms simultaneously, breaking down traditional silos between different blockchain implementations. Developers are working on sophisticated cross-chain communication protocols that enable seamless data and value transfer between different blockchain networks. The implementation of unified identity management systems is streamlining user and device authentication across platforms, while standardized data exchange formats are ensuring consistent information flow throughout hybrid systems.

The **integration of emerging technologies** is set to revolutionize blockchain-IoT systems further. Artificial Intelligence and Machine Learning are being incorporated to enhance system capabilities significantly. These technologies enable automated security policy management, reducing human intervention in routine security operations. Intelligent threat detection and response systems can identify and counter security threats in real-time, while predictive maintenance and optimization algorithms ensure system reliability. Dynamic resource allocation powered by AI ensures optimal system performance under varying load conditions.

Quantum-safe security represents another crucial frontier in blockchain-IoT evolution. As quantum computing advances, the development of quantum-resistant cryptographic algorithms becomes increasingly important for long-term security. Organizations are implementing quantum-safe signature schemes to protect against future quantum attacks, while creating hybrid classical-quantum security approaches that leverage the best of both worlds. The industry is actively preparing for post-quantum blockchain architectures, ensuring systems will remain secure even as quantum computing capabilities advance.

Sustainability has emerged as a critical consideration in future blockchain-IoT implementations, encompassing both environmental and operational aspects. Environmental considerations are driving the development of energy-efficient consensus mechanisms that significantly reduce power consumption. Organizations are implementing green computing practices across their blockchain-IoT networks, while optimizing resource usage to minimize environmental impact. These efforts are complemented by focused initiatives to reduce the overall carbon footprint of blockchain-IoT systems.

Operational sustainability represents the final piece of this evolutionary puzzle. The development of selfmanaging networks is reducing operational overhead and improving system reliability. Organizations are implementing automated maintenance procedures that can identify and resolve issues without human intervention. Scalable architecture designs ensure systems can grow efficiently to meet increasing demands, while the integration of sustainable business models ensures long-term viability. These developments in operational sustainability are crucial for the widespread adoption of blockchain-IoT solutions across different industries and use cases.

Together, these advancements in hybrid architectures, emerging technology integration, and sustainability approaches are shaping the future of blockchain-IoT systems, creating more efficient, secure, and environmentally conscious solutions that can meet the growing demands of our interconnected world.

V. CONCLUSION

The integration of blockchain technology with IoT security frameworks offers promising solutions for critical security challenges while presenting notable implementation complexities. While blockchain provides robust mechanisms for device authentication, data integrity, and decentralized access control through its inherent characteristics of immutability and distributed consensus, successful implementation must address significant hurdles including IoT device resource constraints, network scalability requirements, and lack of standardization. Emerging solutions such as hybrid architectures combining edge computing with blockchain and IoT-optimized consensus mechanisms show potential in overcoming these challenges. As IoT ecosystems continue to expand, the focus must remain on developing standardized frameworks

and innovative approaches that balance robust security with practical implementation considerations, ultimately working toward more secure and efficient IoT networks that can meet the growing demands of our interconnected world.

REFERENCES

[1] "Strategy analytics: internet of things now numbers 22 billion evices but where is the revenue? strategy analytics online newsroom." https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-nownumbers-22-billion-devices-where (accessed Feb. 23, 2020).

[2] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of things- IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," International journal of engineering science and computing, vol. 6, 2016.

[3] O. Vermesan and P. Friess, Internet of ;ings: Converging Technologies for Smart Environments and Integrated Ecosystems, River publishers, Denmark, 2013.

[4] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117.

[5] J. Rivera, R. van der Meulen, Forecast alert: internet of things—endpoints an associated services, worldwide, 2016, Gartner (2016).

[6] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: a review," Journal of Big Data, vol. 6, no. 1, 111 pages, 2019.

[7] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: a comprehensive survey," Sensors, vol. 18, no. 9, 2796 pages, 2018.

[8] S. Prabhakar, "Network security in digitalization: attacks and defence," International Journal of Research in Computer Applications and Robotics, vol. 5, no. 5, pp. 46–52, 2017.

[9] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internetscale IoT exploitations," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, 2019.

[10] H. C. Hasan, F. N. Yusof, and M. Daud, "Comparison of authentication methods in internet of things technology," International Journal of Computer and Systems Engineering, vol. 12, no. 3, pp. 231–234, 2018.

[11] A. Ahmed, R. Latif, S. Latif, H. Abbas, and F. A. Khan, "Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review," Multimedia Tools and Applications, vol. 77, no. 17, p. 21947–21965, 2018.

[12] K. C. Archana and N. Harini, "Mitigation of spoofing attacks on IOT home networks," International Journal of Engineering and Advanced Technology, vol. 9, no. 1S, pp. 240–245, 2019.

[13] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, "Preventing DoS attacks in IoT using AES," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 3–11, pp. 3–11, 2017.

[14] H. C. A. van Tilborg and S. Jajodia, Encyclopedia of Cryptography and Security, Springer US, Boston, MA, 2011.

[15] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.

[16] S. Behrooz and S. Marsh, "A trust-based framework for information sharing between mobile health care applications," Trust Management X, in Proceedings of the IFIP International Conference on Trust Management, pp. 79–95, Darmstadt, Germany, July 2016.

[17] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," in Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), pp. 811–817, Dubai, United Arab Emirates, December 2017.

[18] M. Azrour, Y. Farhaoui, and M. Ouanan, "Cryptanalysis of farash et al.'s SIP authentication protocol," International Journal of Dynamical Systems and Differential Equations, vol. 8, no. 1/2, 2018.

[19] M. Azrour, Y. Farhaoui, and A. Guezzaz, "Experimental validation of new SIP authentication protocol," in Big Data And Networks Technologies, Y. Farhaoui, Ed., vol. 81, pp. 1–11, Springer International Publishing, Cham, 2020.

[20] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, "New enhanced authentication protocol for internet of things," Big Data Mining and Analytics, vol. 4, no. 1, pp. 1–9, 2021.

[21] P. K. Roy, K. Parai, and A. Hasnat, "User authentication with session key interchange for wireless sensor network," in Methodologies and Application Issues of Contemporary Computing Framework, J. K. Mandal, S. Mukhopadhyay, P. Dutta, and K. Dasgupta, Eds., Springer Singapore, Singapore, pp. 153–165, 2018.

[22] J. Moon, T. Song, D. Lee, Y. Lee, and D. Won, "Cryptanalysis of chaos-based 2-party key agreement protocol with provable security," in Advances in Human Factors in Cybersecurity, D. Nicholson, Ed., vol. 593, pp. 72–77, Springer International Publishing, Cham, 2018.

[23] K. Park, S. Lee, Y. Park, and Y. Park, "An ID-based remote user authentication scheme in IoT," Journal of Korea Multimedia Society, vol. 18, no. 12, pp. 1483–1491, 2015.

[24] J. Ryu, H. Lee, H. Kim, and D. Won, "Improvement of Wu et al.'s three-factor user authentication scheme for wireless sensor networks," , 2018.

[25] K. Somasundaram and K. Selvam, "Iot - attacks and challenges," International Journal of Engineering and Technical Research (IJETR), vol. 8, no. 9, pp. 9–12, 2018.

[26] S. Panchiwala and M. Shah, "A comprehensive study on critical security issues and challenges of the IoT world," Journal of Digital Information Management, vol. 2, no. 4, pp. 257–278, 2020.
[27] S. Holger, "Insider threat report," Cybersecurity Insiders, Accessed: Aug. 13, 2020.
[28] I. B. M. X-Force® Research, Cyber Security Intelligence Index, Accessed: Jun. 02, 2017.
[29] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and L. Qiao-min, "An efficient authentication and access control scheme for perception layer of internet of things," Applied Mathematics & Information Sciences, vol. 8, no. 4, pp. 1617–1624, 2014.
[30] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, "Preventing DoS attacks in IoT using AES," J. Telecommun. Electron. Comput. Eng. JTEC, vol. 9, no. 3–11, pp. 3–11, 2017.
[31] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloudIoT applications," Journal of Information Security and Applications, vol. 42, pp. 95–106, 2018.
[32] M. Azrour, Y. Farhaoui, and M. Ouanan, "A server spoofing attack on Zhang et al. SIP authentication protocol," Int. J. Tomogr. SimulationTM, vol. 30, no. 3, pp. 47–58, 2017.
[33] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: a review," Journal of Big Data, vol. 6, no. 1, 111 pages, 2019.
[34] M. Domb, "Smart home systems based on internet of things," in Internet of ;ings (IoT) for Automated and Smart Applications, IntechOpen, London, UK, 2019.
[35] T. Shah and S. Venkatesan, "Authentication of IoT device and IoTserver using secure vaults," in Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 819–824, New York, NY, USA, August 2018.
[36] M. Rana, A. Shafiq, I. Altaf et al., "A secure and lightweight authentication scheme for next generation IoT infrastructure," Computer Communications, vol. 165, pp. 85–96, 2021.
[37] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," IEEE Access, vol. 8, pp. 139244–139254, 2020.
[38] A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," IEEE Syst. J.vol. 99, pp. 1–9, 2020.
[39] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," Computer Networks, vol. 185, Article ID 107731, 2021.
[40] S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "PFLUA-DIoT: a pairing free lightweight and unlinkable user access control scheme for distributed IoT environments," IEEE Syst. J.vol. 99, pp. 1–8, 2020.
[41] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4425–4435, 2020.
[42] M. Wu, J. Chen, and R. Wang, "An enhanced anonymous password-based authenticated key agreement scheme with formal proof," IJ Network Security, vol. 19, no. 5, pp. 785–793, 2017.
[43] C.-W. Liu, C.-Y. Tsai, and M.-S. Hwang, "Cryptanalysis of an efficient and secure smart card based password authentication scheme," in Recent Developments in Intelligent Systems and Interactive Applications, F. Xhafa, S. Patnaik, and Z. Yu, Eds., vol. 541, pp. 188–193, Springer International Publishing, Cham, 2017.
[44] A. Jebrane, A. Toumanari, N. Meddah, and M. Bousseta, "A new efficient authenticated and key agreement scheme for sip using digital signature algorithm on elliptic curves," Journal of Telecommunications and Information Technology, vol. 2 pp. 62–68, 2017.
[45] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: challenges and solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601–628, 2018.
[46] S. Hong, "Authentication techniques in the internet of things environment: a survey," International Journal of Security and Networks, vol. 21, no. 3, pp. 462–470, 2019.
[47] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, 2019.
[48] S. Perera, S. Nanayakkara, M. Rodrigo, S. Senaratne, and R. Weinand, "Blockchain technology: Is it hype or real in the construction industry?" Journal of Industrial Information Integration, vol. 17, 2020.
[49] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, 2008.
[50] H. Ru, et al., "A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges," IEEE Communications Surveys & Tutorials, 2022
[51] H. Ke, X. Zhang, Y. Mu, F. Rezaeibagha, and X. Du, "Lsb: A lightweight scalable blockchain for iot security and anonymity," Scalable and redactable blockchain with update and anonymity, vol. 546, pp. 25–41, 2021.
[52] Kumar, R., Singh, A., & Patel, D. (2019). Security Vulnerabilities in Centralized IoT Authentication Systems: A Comprehensive Analysis of 150 Networks. Journal of Network Security, 15(4), 278-293.
[53] Zhang, H., & Liu, K. (2020). Analysis of IoT Security Incidents: A Study of 500 Breach Cases. IEEE Internet of Things Journal, 7(3), 2089-2102.
[54] Wang, J., Zhang, L., & Chen, Y. (2021). Lightweight Blockchain Protocol for IoT Networks: Implementation and Performance Analysis. IEEE Transactions on Systems, Man, and Cybernetics, 51(6), 3456-3470.
[55] Rodriguez, M. (2022). Smart Contract-Based Access Control for IoT Networks: Challenges and Solutions. International Journal of Blockchain Technology, 4(2), 123-138.

[56] Singh, R., & Patel, V. (2021). Blockchain Framework for Secure IoT Sensor Data: Implementation and Analysis. IEEE Access, 9, 45678-45692.
[57] Li, X., Wang, R., & Thompson, J. (2022). Hierarchical Blockchain Architecture for IoT Networks Using Edge Computing. Journal of Network and Computer Applications, 185, 103076.
[58] Chen, H., Liu, J., & Anderson, T. (2021). Comparative Analysis of Consensus Mechanisms for IoT Blockchain Networks. IEEE Communications Surveys & Tutorials, 23(2), 1156-1181.
[59] Martinez, R. (2022). Performance Evaluation of Blockchain Platforms for IoT Applications. Blockchain: Research and Applications, 3(2), 100045.
[60] Kim, S., & Park, J. (2023). Storage Optimization Techniques for Blockchain-IoT Integration. Journal of Systems Architecture, 128, 102355.
[61] Souhayla Dargaoui1, Mourade Azrour1, Ahmad El Allaoui, Azidine Guezzaz, Abdulatif Alabdulatif, Abdullah Alnajim, Internet of Things Authentication Protocols: Comparative Study, Computers, Materials & Continua 2024, 79(1), 65-91. https://doi.org/10.32604/cmc.2024.047625
[62] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, in: Empowering the Edge-Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value, 2015.
[63] S. Gan, An IoT Simulator in NS3 and a Key-Based Authentication Architecture for IoT Devices using Blockchain, Indian Institute of Technology Kanpur, 2017.
[64] Chain of things, 2018. Available online: https://www.blockchainofthings.com/ .
[65] Filament, 2018. Available online: https://filament.com/ .
[66] modum, 2018. Available online: https://modum.io/ .
[67] G. Prisco, Slock. It to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy, 2016. Available online: https://bitcoinmagazine.com/articles/slock-it-to-introduce-smart-locks-linked-to-smart-ethereumcontracts-decentralize-the-sharing-economy-1446746719/
[68] M.A. Khan, K. Salah, Iot security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. (2017).
[69] LO3ENERGY, 2017. Available online: https://lo3energy.com/ .
[70] Aigang, 2017. Available online: https://aigang.network/ .
[71] My bit, 2017. Available online: https://mybit.io/ .
[72] Chronicled, 2017. Available online: https://chronicled.com/.
[73] Riddle and Code, 2017. Available online: https://www.riddleandcode.com .
[74] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: INFOCOM, 2010 Proceedings IEEE, San Diego, California, USA, Ieee, 2010, pp. 1–9.
[75] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and iot: a big picture, Future Gener. Comput. Syst. 49 (2015) 58–67.
[76] I. Eyal, A.E. Gencer, E.G. Sirer, R. Van Renesse, Bitcoin-NG: a scalable blockchain protocol, in: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59.