Mapana – Journal of Sciences
2025, Vol. 24, No. 2, *117-136*
ISSN 0975-3303 | https://doi.org/10.12723/mjs.73.7

Blockchain-Driven Access Control and Data Protection Framework for Industrial IoT Systems

Yashaswini N* and Sujatha S R†

Abstract

The exponential expansion of Industrial Internet of Things (IIoT) presents major difficulties in guaranteeing strong data security and safe access management over distributed and resource-limited settings. This paper suggests a blockchain-driven architecture combining dynamic access control based on roles with data integrity and confidentiality assurance mechanisms catered for IIoT environments. Three basic levels define the architecture: the IoT layer with intelligent sensors and actuators; the blockchain layer to offer distributed access enforcement and tamper-proof audit trails; and the cloud layer for scalable data storage and processing. Using smart contracts, the system automates access delegation, revocation, and real-time permission changes, hence reducing single points of failure and unwanted access. Compared to centralised systems, experimental evaluation employing Python simulations shows enhanced accuracy, precision, and security at the tradeoff of quite limited throughput. Emphasising privacy, transparency, and resilience, this study provides the basis for reliable, scalable, auditable IIoT infrastructures.

Keywords: Blockchain, Industrial IoT (IIoT), Access Control, Data Protection, Smart Contracts, Role-Based Access Control (RBAC), Data Integrity, Cloud Integration

* Sri Siddhartha Academy of Higher Education, Agalakote, Tumkur, Karnataka, India; yashuyashas99@gmail.com

† Department of Computer Science Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India; sujathasr@ssit.edu.in

1. Introduction

Combining advanced sensing, connectivity, and data analytics technologies to improve automation, operational efficiency, and real-time decision-making, the Industrial Internet of Things (IIoT) offers a transforming paradigm in current industrial ecosystems. The volume of data produced, sent, and kept has skyrocketed as sectors depending more and more on linked devices and systems—from sensors and actuators to controllers and cloud platforms—rely on it. This widespread interconnectedness does, however, also increase the potential of cyberattacks involving illegal access, data breaches, device spoofing, and manipulation of important operational data.

Often becoming bottlenecks because of their reliance on trusted third parties and vulnerability to single points of failure, traditional centralised security systems struggle to accommodate the scale, heterogeneity, and dynamic character of IIoT environments. Blockchain technology becomes a potential enabler of distributed and tamper-proof security systems in this setting. Its natural features—such as distributed consensus, cryptographic hash, and smart contracts—offer strong means for imposing fine-grained access control, guaranteeing data integrity, and preserving transparent audit trails without centralised management. This work investigates the design and implementation of a blockchain-driven access control and data protection architecture especially suited to the particular needs of industrial IoT systems indicated in fig. 1. The suggested framework reduces security vulnerabilities by using permissioned blockchain architectures and programmable smart contracts, so enabling secure device authentication, distributed identity management, and real-time access verification, so preserving system scalability and operational agility and so mitigating security vulnerabilities. Moreover, the article analyses important criteria including latency, throughput, computational cost, and resilience against typical attack routes by means of simulated deployment situations. The results try to show how blockchain may not only improve the security posture of IIoT networks but also enable a trustless environment fit for the future of Industry 4.0.

Figure 1: Blockchain Control Layout for Security Analysis

1.1 The Blockchain-based Cryptography Scheme protects data in Industrial Internet of Things settings

With the use of general information technology, networked physical assets, smart devices, and, in certain cases, cloud or edge computing platforms, the Industrial Internet of Things (IoT) enables a wide range of operations and services to be provided in an industrial setting. The ability to access data in real-time, analyse it, communicate and trade it, and maximise the overall output value are all examples of such processes and services. But there are privacy and security concerns with deploying such systems, so it's important to develop strong privacy and security solutions for IIoT environments. The three main functional systems that make up an IIoT system are the network, platform, and security systems. In contrast, the security system's primary function is to aid in meeting the security needs of various applications, data, networks, controls, and devices through, among other things, the detection, identification, and mitigation of security risks. References [1], [2]. Because the underlying devices in IIoT systems are often power-constrained and have limited storage and computational capabilities, creating solutions to ensure security and privacy can be challenging [3, 4]. So, in most cases, the cloud is used to store and process the data that these IIoT devices perceive, gather, and distribute. Protective measures, such as data encryption, are utilised to lessen the likelihood of data leakage [5], [6]. This may be because of an evil cloud employee, for example. Users or a centralised third-party institution often store and manage the data encryption/decryption key in such techniques. Both methods have their drawbacks. With local key storage, for instance, you risk having only one point of failure or attack vector, and you can lose

access to data or services in the event that the local storage media becomes corrupted—that is, unless you have a backup copy of the key on another storage medium. Trusting a third-party centre (such as a certificate management organisation, or CA) to store and maintain the keys implies putting our faith in that centre to do the correct thing and keep the key secret.

1.2 Blockchain-Enabled Cloud-IoT Environment: Dynamic Secure Access Control and Data Sharing via Trusted Delegation and Revocation

Connectivity between several devices has been made possible by the recent emergence of the Internet of Things (IoT) technology. This has allowed for a variety of applications, including smart homes, smart manufacturing, and smart transportation [7], [8]. A system for managing these devices is required due to the privacy and security concerns linked to this advancement [9]. According to research [10], access control is the most effective method for preventing unwanted and illegal users from gaining access. A number of strategies for controlling who can access what resources have been suggested, but all of them depend on one central authority, making them vulnerable to interference [12]. Network attackers take over the main server and change the access policies to their advantage. Furthermore, the compromised central entity poses significant privacy risks due to the exposed personal information of IoT users, including location and surveillance data [13]. In order to overcome the drawbacks of centralized architectures and meet the needs of large-scale scenarios, blockchain technology enables decentralized access management inside the IoT network [14], [15]. Despite its potential benefits for secure data sharing, multiauthority-based access control raises serious concerns about user privacy in a number of published publications [16], [17], and [18]. By storing the access policies in the blockchain node and making choices based on them, several existing systems incorporate the blockchain to enable decentralized access controls [19]. These methods leverage the blockchain node to delegate processing of the IoT entities' total resource needs [20, 21].

2. Literature Review

The literature reveals that integrating blockchain into IoT systems significantly enhances security by enabling decentralized access control, immutable data storage, and trust less communication. Some major considerations are given below-

B Zhong et.al (2023) [22] claims that BDIT has lately been rather popular in the AEC industry. A critical literature evaluation of BDIT is one approach

to support AEC sector innovation. This paper quantitatively mapped 247 BDIT literatures from 2017 to 2022. Examined in line with the lead of quantitative research were two pivotal phases of BDIT technological development and application. The findings indicate that BDIT's future tech could use information automation and building information management and incorporate knowledge framework and technological integration (e.g., internet of things, blockchain, building information modelling, edge computing, etc.). We discussed many possible future developments, use cases, and challenges including the integration of blockchain with federated learning, digital twins, and cloud-edge-end architecture for a closer examination of BDIT trends. The theoretical and practical references offered by this work would be much appreciated in research on BDIT in the AEC sector.

According to W Tong et.al. (2022) [23], multi-domain IoT was introduced as a method to enhance the network's control and coordination capabilities as a consequence of the widespread use of the Internet of Things (IoT). There are a lot of security concerns with the new multi-domain Internet of Things (IoT), including things like insider attacks and problems with transferring data across domains. To solve the problems of inefficient data flow throughness and costly cross-domain access control in a multi-domain IoT setting, we provide a blockchain-driven data exchange architecture in this paper. This design is built upon a domain-as-a-shard (DaaS) technology-based chaincode-based cross-domain access control system form, which optimises high parallel throughput. Data controllability and distributed storage based on strategy are ensured by many blockchain nodes, specifically responsible for maintaining the access control system. Nodes in this architecture are required to validate the access control technique before data may be exchanged across domains. Setting the Internet of Things domain as a blockchain shard also facilitates parallel processing of data exchange, which substantially boosts throughput. To increase the throughput of blockchain transactions, our method partitions data exchange into smaller pieces and processes each one separately. Our method of security analysis guarantees both the controllability of data across domains and the non-repudiation of access control measures. We found that our model's transaction throughput is about three times more than that of the original Fabric v1.4, according to our extensive Hyperledger Fabric examinations. According to P. Patil et al. [24], blockchain technology is currently garnering significant interest from researchers and scientists due to its many potential applications. These include decentralising wireless networks, access control, data security, and privacy. Blockchain is the preferred solution due to its irreversible nature, while it also offers additional advantages, including peer-to-peer technology, anonymity,

expanded capacity, and improved security. Due to its decentralised nature, blockchain technology presents a promising substitute for trusted third parties in network architectures. Several popular blockchain systems are available, including Hyperledger Fabric, Multichain, Ripple, IBM Blockchain, and Ethereum. Current blockchain-based security solutions for supply chains, healthcare, automobile ad hoc networks, and the Internet of Things (IoT) are detailed and evaluated in the review article provided below. In order to conduct cutting-edge research on blockchain technologies, researchers can refer to the extensive survey of blockchain use cases. With this, they may expand the use of blockchain technology to other areas.

According to AH Sodhro et.al. (2020) [25], a new paradigm shift called Industry 4.0 will usher in the Industrial Internet of Things (IIoT), which will impact various industries. Smaller networks with lower power consumption have a harder time providing security, however, sensor-enabled technologies like wireless sensor networks (WSNs) make this viable in some settings. There is a wide variety of industrial uses for smart devices, driven by the increasing demand for commercial Internet of Things (IoT) devices. Should these devices infringe upon data, severe consequences and data loss would ensue, in contrast to the extent to which commercial IoT devices do so. Thus, the need for secure industrial IoT is being driven by the introduction of smart IoT-based solutions in the healthcare industry and other growing industries that are utilising cutting-edge blockchain security solutions. Consistent updates to Android have made the blockchain-based IIoT system administration more secure. Blockchain technology has opened the door to a new cybersecurity algorithm and architecture that the industrial internet of things (IoT) desperately needs. This system should take advantage of technologies that generate initial and master keys randomly over long-range, low-power wireless networks in order to process and transmit encrypted data rapidly. Three significant contributions are contained in this paper. We begin with the premise of an efficient, secure, and sustainable blockchain-driven algorithm. One view is that the suggested method generates a series of blocks that handle keys in a random fashion, which lessens power consumption, lessens the need for core components, and somewhat increases the amount of bits needed for processing and communication. The second one is an analytical hierarchy process (AHP) based smart decision-making method for the blockchain-driven IIoT system that is trustworthy, safe, concurrent, interoperable, and sustainable. Professionals in the field can improve product yield by using AHP-based solutions to prioritise features like reliability with regard to packet loss ratio, mapping convergence with latency, and interoperability with throughput. Finally, a

new cloud-enabled architecture for the IIoT platform is being proposed by eco-friendly tech solutions, which will allow for consistent product monitoring throughout the entire organisation. In addition to providing a solid foundation for anticipating the methodologies and resources that will be utilised to manage the adaptive system from an Industry 4.0 standpoint, the experimental results demonstrate that the suggested approach has a decent shot at being a blockchain-driven IIoT system contender in terms of convergence, interoperability, and reliability.

Prior to their use of the term by Ma et al. (2020) [26], the evolution of IoT technology has yielded tremendously impressive outcomes in recent years. Intelligent administration and operation are made possible by the Internet and a network of interconnected sensors and machines. With traditional centralised IoT data management systems, problems with data trust, security, sustainability, and user privacy are inevitable. This study suggests a blockchain-based system for the secure sharing of IoV data (IoVChain). As part of the intelligent transportation sensor network, it establishes a reliable mechanism of sharing IoV data via smart contracts, as well as automatic registration and fast authentication. The sensitive data, which is kept on the blockchain as ciphertext, undergoes changes during the smart contract's homomorphic encryption and zero-knowledge proof processing. An immutable Merkle-tree-based block stores all of the processing and consumption operations for IoV data, guaranteeing the integrity of the entire network ledger. The IoVChain system eliminates the risk of data loss caused by a single point of failure, guaranteeing that all IoV data stays trustworthy, accessible, and resistant to manipulation in a secure environment that cherishes privacy. This is in contrast to a centralised solution for IoV data management. For the safe and reliable transfer of IoV data, we have utilised the IoVChain scheme, which is based on the consortium blockchain. Lastly, research and testing have proven that the suggested IoVChain system is secure, expandable, and practical for the private exchange of IoV data.

Major research gaps show up as one moves through the research process. One can emphasise the research gap for a Blockchain-Driven Access Control and Data Protection Framework for Industrial IoT (IIoT) Systems as follows:

- Usually employing conventional access control mechanisms like Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), industrial IoT systems These techniques lack the requisite granularity needed to protect private data in dynamic contexts, nevertheless, and are prone to assaults including privilege escalation, illegal access.

- In IIoT systems—where sensitive operational data, machine health information, and proprietary algorithms are exchanged—data integrity and privacy are absolutely vital. Currently centralised data storage and management solutions expose single points of failure and are susceptible to data manipulation, unauthorised access, or attack.
- As IIoT systems grow, so does the count of devices and users. Although blockchain's capacity to offer distributed and decentralised control could help to solve scalability issues, its interaction with current IIoT systems is yet mostly unknown.
- Particularly in real-time operational environments where data flow is continuous and high-volume, blockchain has shown promise in securing financial transactions but its potential for ensuring access control, data protection, and privacy in IIoT environments is yet underexplored.
- Lack of Standardisation and Interoperability: There is nothing of a standardised blockchain framework combining effortlessly with IIoT technologies. Still, a major research void is ensuring compatibility between several IoT devices, platforms, and blockchain systems.

3. Research Objectives

Research on Blockchain-Driven Access Control and Data Protection Framework for Industrial IoT Systems has as its main goals:

- Create a blockchain-based decentralised access control model for IIoT systems that can safely control and provide access depending on dynamic contextual elements such as device kind, role, and operating environment.
- Use cryptographic methods included in blockchain systems to guarantee data integrity, authenticity, and privacy for private information sent between systems and devices, and sensitive industrial data.
- Examining the integration of blockchain technology into current IIoT infrastructures, with an eye towards low latency, high throughput, and scalability in real-time operations without sacrificing performance,
- Using off-chain storage, sharding, or sidechains, propose scalable blockchain solutions able to handle the enormous amount of data and many transactions typical of IIoT systems.

- Create a framework for interoperability across heterogeneous IoT devices, IIoT systems, and blockchain networks, thereby guaranteeing the safe data transfer and access rights across platforms.
- Work towards developing standards and protocols for blockchain-based security solutions that may be generally implemented in IIoT systems to ensure consistency and compatibility across industrial sectors.
- Using blockchain's distributed and tamper-proof character to solve the current access control and data protection gaps, this study intends to improve the security, integrity, and privacy of industrial IoT systems.

4. Background Study

The security of the Internet of Things (IoT) is at risk due to the potential exposure of sensitive data during data exchange. While there are a number of problems with centralised access control and selecting a single delegator, the Internet of Things has introduced secure data sharing and access control to assist in alleviating these issues. Additionally, blockchain is integrated with the IoT to improve eco-friendliness. This study offers DSA-Block, a blockchain-based solution for dynamic secure access control that facilitates both secure access control and data sharing, to achieve this goal. In order to verify the identity of users and devices, the Internet of Things (IoT) attributes and user attributes must first be registered with a local domain authority (LDA). This will allow for the generation of private and public keys using the hyperelliptic curve cryptography (HECC) approach. Afterwards, the Internet of Things devices validate the user's authentication and filter requests by requesting messages from the edge nodes (ENs) through a gateway. The filtered requests are sent to the edge server, which uses rock hyraxes swarm optimisation (RHSO) to delegate access from a group of nodes. A consensus based on Trusted Practical Byzantine fault tolerance (PBFT) is used to influence the choice of access control. By utilising a cloud server for secure data storage, differential privacy techniques guarantee the safety of the IoT data. Finally, security is improved by having twin revocations: user attribute revocation and user revocation. Results show that the suggested DSA-Block model outperforms prior works, proving that DSA-Block performs as expected. [27]

5. Methodology Layout

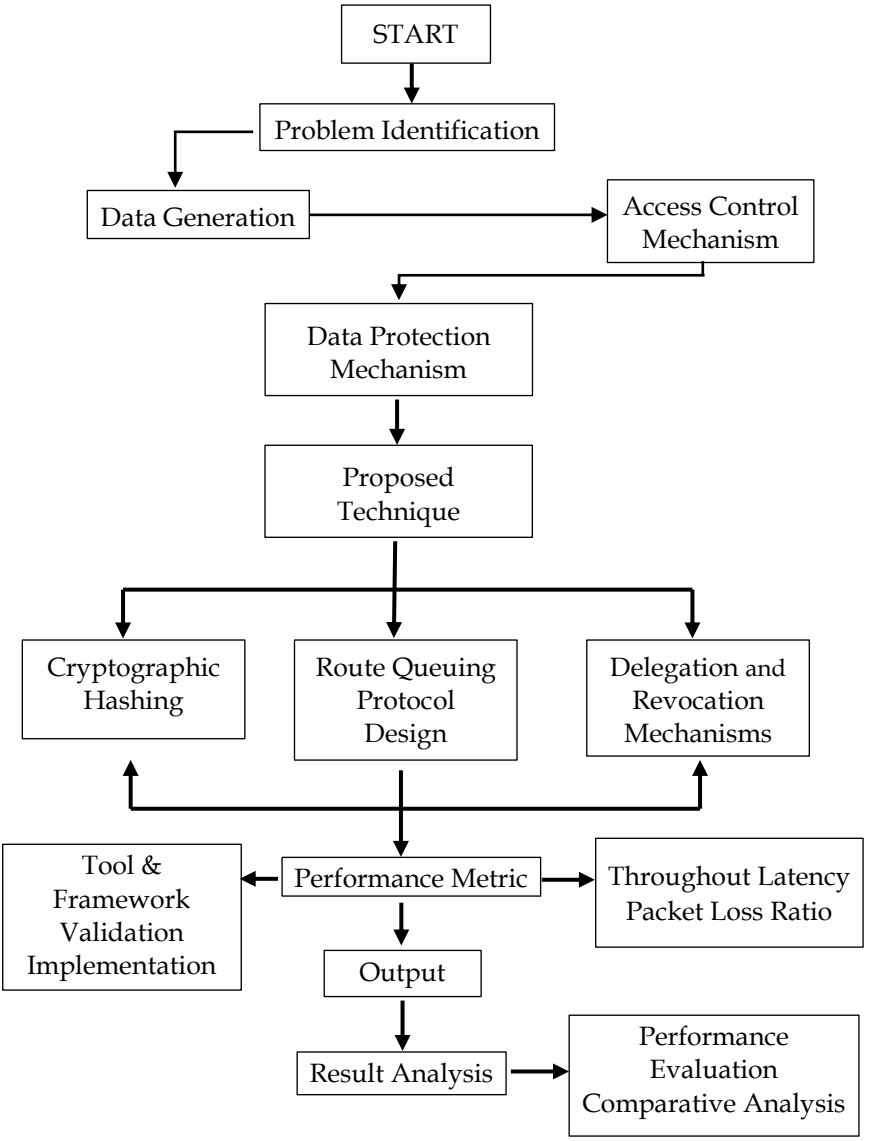

Figure 2: Proposed Methodological layout

Structured into a multi-layered conceptual framework and system architecture that holistically integrates IoT, blockchain, and cloud computing technologies, the proposed method for implementing a Blockchain-Driven Access Control and Data Protection Framework for Industrial IoT Systems shown in fig. 2 is At the IoT level, a network of

industrial devices including sensors, actuators, and machines creates data and runs processes needing authorized access. By means of smart contracts, which also guarantee data integrity and preserve an unchangeable and open audit record of all data access and policy updates, the blockchain layer serves as a distributed trust infrastructure regulating access control and ensuring data integrity. By allowing safe data transmission via blockchain integration, the cloud layer—which acts as a link between IoT devices and blockchain—is in charge of data processing and storage chores. Among the important security measures are end-to-end data protection techniques, smart contract-based delegation and revocation systems, and fine-grained access control policies. Based on roles and real-time data, including device state and trust measurements, blockchain Role-Based Access Control (RBAC) dynamically regulates privileges. Smart contracts also allow for delegation mechanisms to enable safe transfer of access privileges among entities and revocation systems to rapidly invalidate access in response to threats or compromises. Advanced encryption methods, including AES and RSA, are used to ensure data confidentiality for data security, while blockchain saves cryptographic hashes to certify data integrity and promote auditability by immutable logs. Depending on the permission model, an appropriate blockchain platform such as Ethereum or Hyperledger is selected at the phase of framework implementation; consequently, smart contracts are generated for efficiently enforcing policies, delegation, and revocation. While safe APIs or gateways allow integration with IoT devices, seamless cloud-blockchain communication provides constant, encrypted data flow and storage. Finally, the framework finishes in a prototype development whereby technologies such as Contiki and Cooja replicate IoT networks and apply blockchain capabilities over Ganache and Truffle. The prototype is then deployed in a simulated industrial environment for real-time validation, performance testing, and refining after ensuring the viability, security, and scalability of the recommended blockchain-based access control and data protection architecture for Industrial IoT systems.

5.1. Technique Used

The proposed method for Industrial IoT (IIoT) systems takes advantage of a distributed access control and data security mechanism built on a blockchain. Natural features of blockchain—immutability, transparency, and decentralisation—are applied in access management and data integrity assurance in an IIoT setting. By means of smart contracts, the framework dynamically grants, alters, and cancels access permissions depending on real-time events, hence enabling the delegation of access rights between trusted entities. Furthermore, utilised to protect data confidentiality and verify integrity all throughout the network are hash methods and

encryption. The distributed character of blockchain guarantees that no one point of failure exists, therefore protecting the system against fraud and attack. Keeping scalability and efficiency, this approach enhances security, transparency, and confidence in managing IIoT access control and data transmission.

5.2. Pseudocode Layout

```
START
// Step 1: System Initialisation
Initialize BlockchainNetwork()
Initialize IoTDevices()
Initialize CloudInfrastructure()
Deploy SmartContracts()
// Step 2: Role Assignment and Access Control Setup
FOR each User IN System:
   AssignRole(User)
   DefinePermissions(Role)
   StoreAccessControlPolicy(Role, Permissions, Blockchain)
// Step 3: Data Generation from IoT Devices
WHILE Device is Active:
   Data = ReadFromSensor(Device)
```

```
   EncryptedData = Encrypt (Data, EncryptionKey)
   Hash = GenerateHash(EncryptedData)
   StoreHashOnBlockchain(Hash)
   SendToCloud(EncryptedData)
// Step 4: Access Request Handling
WHEN AccessRequest is Received:
   IF VerifyAccessRights(User, Resource) == TRUE:
      GrantAccess(User, Resource)
      LogAccess(User, Resource, Timestamp, Blockchain)
   ELSE:
      DenyAccess(User)
```

```
// Step 5: Delegation Mechanism
IF DelegationRequest is Initiated:
   IF User is Trusted:
      GenerateDelegationToken(User, Delegatee)
      StoreDelegationRecord (Delegatee, Resource, Blockchain)
   ELSE:
      DenyDelegation()
// Step 6: Revocation Protocol
IF SecurityBreachDetected OR RevokeRequestInitiated:
   RevokeAccess(User, Resource)
   UpdateSmartContract(User, Revoked=True)
   LogRevocation(User, Resource, Blockchain)
// Step 7: Data Integrity Verification
FOR each RetrievedData:
   RetrievedHash = RetrieveHashFromBlockchain(DataID)
   ComputedHash = GenerateHash(EncryptedData)
   IF RetrievedHash == ComputedHash:
      ConfirmIntegrity()
   ELSE:
      RaiseAlert("Data Tampering Detected")
// Step 8: Audit and Monitoring
SchedulePeriodicAudit()
FOR each AuditLog in Blockchain:
   AnalyzeLog(Log)
   ReportSuspiciousActivities()
END
```

[*Blockchain allows the pseudocode to provide a distributed and safe architecture for Industrial IoT systems. It addresses system setup, role-based access control, safe data encryption and hashining, access validation, dynamic delegation and revocation with smart contracts. It also guarantees data integrity and keeps an unchangeable audit trail for study and monitoring****].***

6. Implementation and Result Layout

While integrating IoT devices and cloud services for safe data exchange, the implementation consists in deploying smart contracts on a blockchain platform (e.g., Ethereum or Hyperledger) to manage access control, delegation, and revocation. Access latency, transaction throughput, security breach response time, and auditability guide evaluation of results to confirm system performance and scalability.

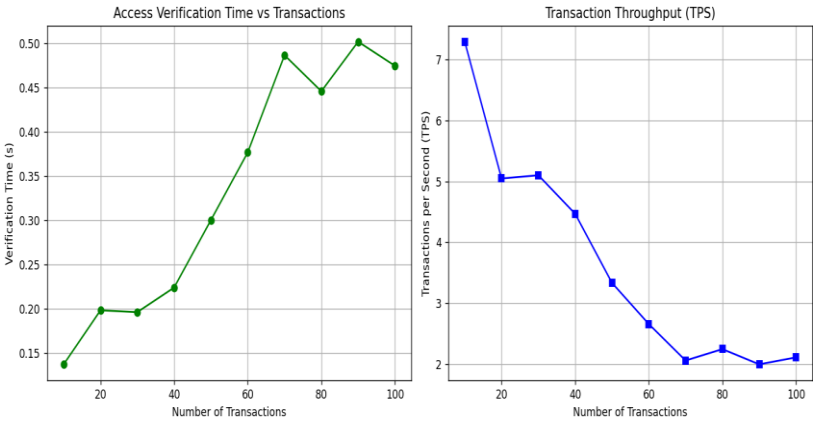

Figure 3: Access Verification and Throughput Considerations for Security Analysis

The efficiency and scalability of access control operations in an Industrial IoT (IIoT) environment are illustrated by analysing significant criteria like access verification time and transaction throughput (TPS), thereby displaying the blockchain performance graph displayed in Fig. 3 simulation. As seen in the first subplot, access verification time somewhat increases with the volume of access requests, reflecting the computational cost and network latency imposed by blockchain activities, including consensus verification and smart contract execution. This trend remains quite linear for modest to moderate transaction volumes, indicating a constant and manageable latency profile, which is crucial for time-sensitive industrial applications. The second subplot displays the transaction throughput, therefore revealing the concurrent access requests processing capability of the blockchain system. The TPS first grows as the system efficiently manages small transaction loads, but with rising transaction volume, the throughput starts to plateau or perhaps reduce due to the overhead in block production, gas cost limits, or chain resource contention. This study underlines the significance of selecting a blockchain platform (e.g., Ethereum or Hyperledger) that can control the scalability and performance requirements of IIoT systems while ensuring robust security and auditability. It also emphasises the importance of enhancing smart contracts and considering off-chain processing techniques, such as

idechains, for upcoming scalability enhancements in pragmatic implementations.

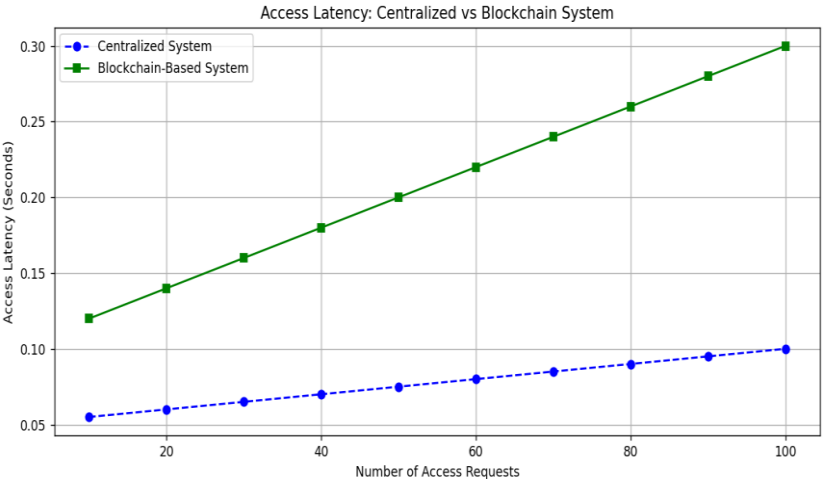

Figure 4: Access latency considerations for Security Analysis

The representation shown in Figure 4 shows how both centralised and blockchain-based access control systems behave as access demand rises. Because of its simple and easy access verification mechanism—which does not depend on distributed consensus processes—the centralised system consistently shows lower latency. The capacity of the centralised system to tolerate a constant and predictable increase in latency as the volume of access requests increases shows how well it handles controlled circumstances. By comparison, the latency increases in the blockchain-based system are more evident. This is resulting from the well-known time-consuming character of the safe and distributed authorisation processes, which comprise block validation, smart contract execution, and consensus protocols. Blockchain technology presents improved data security, transparency, and tamper-resistance—all of which are vital for industrial IoT applications—that trade off with higher latency, particularly when loads are higher. Because of their increased trust, auditability, and security—even if centralised systems provide faster reaction times—this study shows that blockchain solutions are better for uses that value data protection and decentralised control over latency overhead.

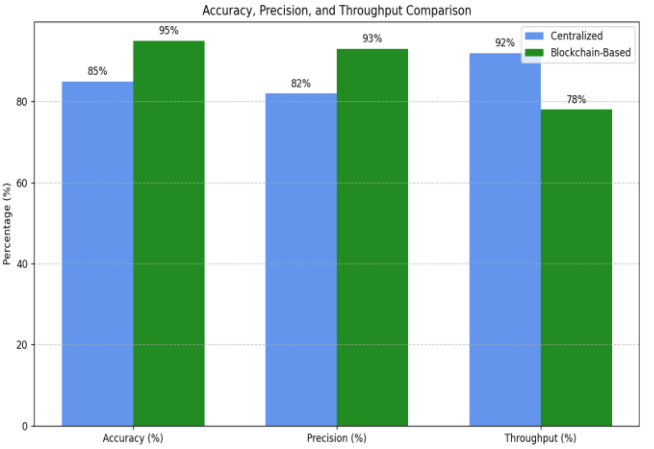

Figure 5: Performance metrices consideration

The performance measures displayed in fig. 5—accuracy, precision, and throughput—showcase how centralized and blockchain-based access control systems in industrial IoT environments have different advantages and disadvantages. Blockchain-based systems are more dependable in ensuring data is true and access is limited (95% accuracy vs. 93%) since they use distributed validation, cryptographic security, and clear policy enforcing techniques through smart contracts. Because of the additional labour consensus protocols and block verification techniques contribute, these higher degrees of security and dependability come at the cost of reduced throughput—78% less. Since centralized systems are more likely to have security holes, illegal access, and not be audited, their simpler, single-point decision-making model results in higher throughput (92%), but this efficiency often comes at the cost of lower accuracy (85%), and precision (82%). According to this research, blockchain performs effectively in contexts when trust and data integrity take precedence above actual functioning speed.

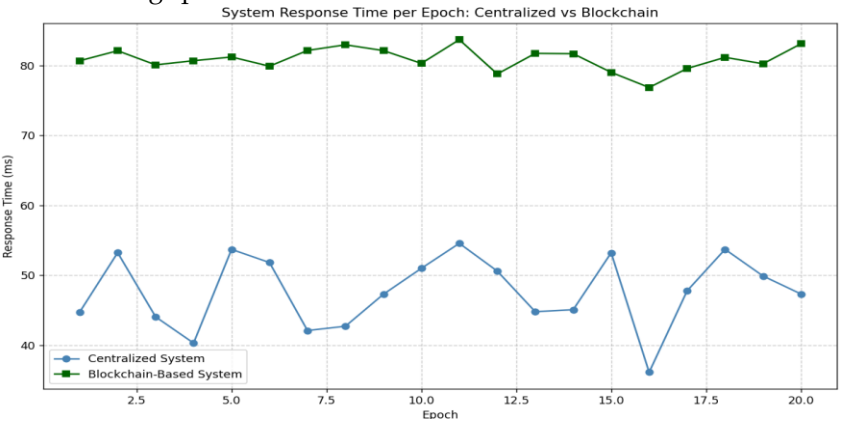

Figure 6: Response Speed Time consideration rate

The Response speed and system shown in Fig. 6 clearly trade off in the comparative graph between centralised and blockchain-based (decentralised) systems over several time epochs. Because of their simplified architecture and single-point decision-making approach, centralised systems often show reduced response times, average = 50 milliseconds. But sometimes this efficiency comes at the expense of auditability and sensitivity to security breaches. By means of the additional expense of consensus procedures and cryptographic validation, blockchain-based systems exhibit higher but more consistent response times, averaging approximately 80 milliseconds. Notwithstanding the initial latency, the distributed architecture provides strong data security, openness, and tamper resistance over time and shows more consistency and dependability. This confirms the fit of blockchain for uses where safe, verifiable access control exceeds the need for ultra-fast processing, especially in Industrial IoT environments requiring traceable, responsible data transactions.

7. Conclusion

Within the framework of this work, a blockchain-based access control and data protection mechanism for industrial Internet of Things (IoT) systems is effectively designed and assessed. This architecture tackles the main concerns about centralised vulnerabilities, unauthorised access, and data integrity. Incorporating transparent audit mechanisms, dynamic role-based policies, and smart contracts helps the proposed solution increase the trustworthiness and responsibility of data flows between IIoT devices and cloud services. This is achieved by means of the interaction among these systems. In terms of accuracy, precision, and resistance to security breaches, the framework performs somewhat better than conventional centralised systems despite some shortcomings in terms of processing latency and throughput resulting from blockchain consensus methods. Future studies could look into hybrid consensus approaches, intelligent edge computing integration, and adaptive scalability in order to greatly increase performance and lower the computational overhead in large-scale industrial installations.

Conflict of Interest

The authors hereby declare no potential conflicts of interest with respect to the research, funding, authorship, and/or publication of this article

References

[1]. K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid," IEEE transactions on instrumentation and measurement, vol. 64, no. 8, pp. 2072–2085, 2015.

[2]. Z. Guo, K. Yu, A. Jolfaei, A. K. Bashir, A. O. Almagrabi and N. Kumar, "A Fuzzy Detection System for Rumors through Explainable Adaptive Learning," IEEE Transactions on Fuzzy Systems, doi: 10.1109/TFUZZ.2021.3052109.

[3]. H. Li, K. Yu, B. Liu, C. Feng, Z. Qin and G. Srivastava, "An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things," IEEE Journal of Biomedical and Health Informatics, 2021, doi: 10.1109/JBHI.2021.3075995.

[4]. K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3567–3569, aug 2018.

[5]. K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, "Secure Artificial Intelligence of Things for Implicit Group Recommendations", IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.

[6]. L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, "Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness", IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.

[7]. S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-based access control for AWS Internet of Things and secure industries of the future," IEEE Access, vol. 9, pp. 107200–107223, 2021.

[8]. Y. Liu et al., "Capability-based IoT access control using blockchain," Digital Commun. Netw. vol. 7, no. 4, pp. 463–469, 2021. [Online]. Available: https://www.sciencedirect. com/science/article/ pii/S2352864820302844

[9]. 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.

[10]. L. Liu, H. Wang, and Y. Zhang, "Secure IoT data Outsourcing with aggregate statistics and fine-grained access control," IEEE Access, vol. 8, pp. 95057–95067, 2020.

[11]. Q. Yang, M. Zhang, Y. Zhou, T. Wang, Z. Xia, and B. Yang, "A noninteractive attribute-based access control scheme by blockchain

for IoT," Electronics, vol. 10, no. 15, p. 1855, 2021. [Online]. Available: https: //www.mdpi.com/2079-9292/10/15/1855

[12]. A. Kousalya, K. Sakthidasan, and A. Latha, "Reliable service availability and access control method for cloud assisted IoT communications," Wireless Netw., vol. 27, pp. 881–892, Feb. 2021.

[13]. K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT Healthcare applications," Comput. Commun., vol. 180, pp. 31–47, Dec. 2021. [Online]. Available: https://www.sciencedirect.com/science/article /pii/S0140366421003054

[14]. Z. Li, J. Hao, J. Liu, H. Wang, and M. Xian, "An IoT-applicable access control model under double-layer blockchain," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 68, no. 6, pp. 2102–2106, Jun. 2021.

[15]. U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Clust. Comput., vol. 23, pp. 2067–2087, Feb. 2020.

[16]. S. Xiong, Q. Ni, L. Wang, and Q. Wang, "SEM-ACSIT: Secure and efficient multiauthority access control for IoT cloud storage," IEEE Internet Things J., vol. 7, no. 4, pp. 2914–2927, Apr. 2020.

[17]. S. Banerjee et al., "Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment," J. Inf. Security Appl., vol. 53, Aug. 2020, Art. no. 102503. [Online]. Available: https://www.sciencedirect.com/ science/article/pii/S2214212619310178

[18]. M. Dammak, S.-M. Senouci, M. A. Messous, M. H. Elhdhili, and C. Gransart, "Decentralized lightweight group key management for dynamic access control in IoT environments," IEEE Trans. Netw. Service Manag., vol. 17, no. 3, pp. 1742–1757, Sep. 2020.

[19]. P. Chinnasamy, P. Deepalakshmi, A. K. Dutta, J. You, and G. P. Joshi, "Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in AI-enabled IoT system," Mathematics, vol. 10, no. 1, p. 68, 2022. [Online]. Available: https://www.mdpi.com/ 2227-7390/10/1/68

[20]. N. Tapas, F. Longo, G. Merlino, and A. Puliafito, "Experimenting with smart contracts for access control and delegation in IoT," Future Gener. Comput. Syst., vol. 111, pp. 324–338, Oct. 2020. [Online]. Available: https://www. sciencedirect.com/science/article/pii/S0167739X18326979

[21]. S. Pal, T. Rabehaja, M. Hitchens, V. Varadharajan, and A. Hill, "On the design of a flexible delegation model for the Internet of Things using blockchain," IEEE Trans. Ind. Informat., vol. 16, no. 5, pp. 3521–3530, May 2020

[22]. Zhong, Botao, Xing Pan, Lieyun Ding, Qiang Chen, and Xiaowei Hu. "Blockchain-driven integration technology for the AEC industry." Automation in Construction 150 (2023): 104791.

[23]. Tong, Wei, Xuewen Dong, Yulong Shen, Xiaohong Jiang, and Zhiwei Zhang. "A blockchain-driven data exchange model in multi-domain IoT with controllability and parallelity." Future Generation Computer Systems 135 (2022): 85-94.

[24]. Patil, Pradnya, M. Sangeetha, and Vidhyacharan Bhaskar. "Blockchain for IoT access control, security and privacy: a review." Wireless Personal Communications 117, no. 3 (2021): 1815-1834.

[25]. Sodhro, Ali Hassan, Sandeep Pirbhulal, Muhammad Muzammal, and Luo Zongwei. "Towards blockchain-enabled security technique for industrial internet of things based decentralized applications." Journal of Grid Computing 18, no. 4 (2020): 615-628.

[26]. Alshehri, Suhair, Omaimah Bamasaq, Daniyal Alghazzawi, and Arwa Jamjoom. "Dynamic secure access control and data sharing through trusted delegation and revocation in a blockchain-enabled cloud-IoT environment." IEEE Internet of Things Journal 10, no. 5 (2022): 4239-4256.