International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-11, Issue-4; Jul-Aug, 2025
Journal Home Page: https://ijaems.com/
DOI: https://dx.doi.org/10.22161/ijaems.114.31

Blockchain-based Security Framework for IoT Devices in Industrial Automation: A Comprehensive Review

Karthik Kumar Vaigandla[1], Madhu Kumar Vanteru[2], Ranjith Kumar Siddoju[3]

[1,2]Associate Professor, Electronics and Communication Engineering, Balaji Institute of Technology and Science, Warangal, Telangana, India.
[3]Assistant Professor, Electronics and Communication Engineering, Sree Chaitanya College of Engineering, Karimnagar, Telangana, India.

Received: 11 Jul 2025; Received in revised form: 04 Aug 2025; Accepted: 08 Aug 2025; Available online: 11 Aug 2025

Abstract *— The widespread use of industrial automation Internet of Things (IoT) devices has seen great transformation in operational efficiency and decision-making. But these interconnected environments have nevertheless raised a major concern about their security challenges. Blockchain technology is a promising solution to the challenges of infrastructure because of its decentralized, transparent and tamper proof characteristics. We discuss in this paper how blockchain based security frameworks are being used in IoT devices for industrial automation right now. It first conducts an in depth analysis of existing approaches and their pros and cons before concluding with research gaps. In addition, it explores integration of blockchain with involving technologies for IIoT ecosystems' security.*

Keywords *— **Blockchain, Security, IoT, IIoT, Industrial Automation, Smart Contracts.***

I. INTRODUCTION

The development of Industry 4.0 has brought IoT devices into Industrial Automation allowing real time monitoring, predictive maintenance and control they're Industrial operations. Whilst these benefits are impressive, the interconnection of IoT devices in general opens industrial systems to a wide range of security threats, such as loss of data, unauthorized access, and system disruption. Industrial IoT environments suffer from their scalability, heterogeneity, and resource constraints, and these traditionally common security mechanisms are not sufficient to deal with such problems. Security using blockchain technology is achieved through a decentralized approach to security, including data integrity, authentication and fault tolerance without a central authority [1].

Industrial Internet of Things (IIoT) technologies have witnessed rapid growth and have provided transformative advantages to industrial automation, which has led to smart factories, greater efficiency and smaller operational costs. At the core of this transformation is IIoT devices: sensors, actuators, and controllers producing massive amounts of data enabling real time monitoring and decisions. Yet as more and more devices link to the Internet the complexity, scope of security risk is growing. Consequently, IIoT systems are particularly susceptible to different types of threats such as unauthorized access, data breaches or attacks to device integrity [2]. Industrial sectors, including in manufacturing, energy, logistics and healthcare, are facing serious vulnerabilities that leave them exposed to serious financial loss, operational downtime as well as physical damage in case of an attack.

To address these challenges, blockchain technology has the potential to be something of a silver bullet, providing security for IoT devices in the industrial automation realm. Being decentralized and immutable, Blockchain provides a strong canvas to

ensure data integrity, confidentiality, and authenticity that is exchanged between IoT devices. The removal of central authority centralizes the authority in the blockchain, which improves transparency and accountability in IIoT networks, which is important for the identification of the malicious actors. One of the major security advantages of blockchain, enabling secure and verifiable transactions between devices, makes it a perfect tool to satisfy some, if not all, key security concerns: device authentication, data integrity, and secure communication.

This review goes through the potential advantages blockchain based security framework provides for IoT devices in Industrial automation specifically with respect to security requirements of the IIoT environments. In the review of the current state of blockchain technologies for industrial automation is considered a range of use cases, advantages and thorny issues when using them. Additionally, it presents ideas on the critical components of a blockchain based security system including consensus mechanisms, smart contracts and decentralized identity management, as means of improving IoT devices security. This review identifies existing gaps in the research and specifies future directions to give an overall view of how blockchain can revolutionize IoT security in the industrial automation in order to ensure safe and protected industrial systems.

At the time the industrial sector has turned to IoT technologies and the need for robust and scalable security solutions has never been bigger. The combination of blockchain based security frameworks is a potential, mature and effective solution to address these requirements as it provides the decentralized trust, increased resilience and transparency at IIoT network level. While technically possible, implementation of blockchain in this domain faces questions that need to be addressed, including technical, operational, and regulatory barriers, these being the subjects to be covered by this review. Reviewing the challenges and solutions to integration of blockchain in obtaining security for IoT devices on industrial automation system can lead to a body of knowledge to support the integration of blockchain in securing IoT devices in industrial automation system.

In this paper, we propose to discuss in detail about blockchain based security framework for IoT devices in industrial automation. It assesses the present picture, acknowledges problems and envisages directions for research and policy work.

II. IOT SECURITY CHALLENGES IN INDUSTRIAL AUTOMATION

The complex interplay of devices, networks and systems makes IoT security in industrial automation a challenging problem. In the IoT ecosystem, industrial automation systems can proactively significantly enhance their security posture by solving these challenges.

Fig.1. Security challenges in IoT

2.1 Data Integrity and Confidentiality

Data integrity and confidentiality in industrial automation are of great importance to ensure operational stability, protection of sensitive data, and data access or manipulation integrity. Suffice it to say, IoT devices produce a ton of sensitive data, making them attractive points of cyber attack. A first priority is to guarantee data integrity and confidentiality when data is transmitted and stored. Data integrity ensures that data is accurate, consistent and that it hasn't been copied, tampered, or damaged while a message is being transmitted or being stored. Wired attackers intercept and modify data that is being transmitted between IoT devices and control systems. During transmission of data some noise or interference in the communication channels corrupt the data [5]. There may be

weaknesses in access controls in industrial systems, causing insiders, or strangers, to be able to modify critical data within such systems. Legacy systems often use outdated and unencrypted protocols, making data vulnerable to tampering. Data confidentiality ensures that sensitive information is accessible only to authorized users and entities. Data transmitted over insecure channels (e.g., HTTP instead of HTTPS) can be intercepted. Weak authentication mechanisms can allow hackers to access sensitive industrial data. Industrial IoT often relies on cloud platforms, which can be targets for data breaches. Attackers can exploit compromised devices to extract sensitive data.

2.2 Device Authentication and Authorization

For a successful industrial automation network, authentication and authorization are necessary to secure the network against unauthorized access and network operation only by trusted devices. These security mechanisms thwart foreign entities accessing until the integrity, reliability, and confidentiality of industrial systems [6]. IoT device needs to authenticate, that is if it is different from what it says it is. Without the proper strong authentication mechanisms, malicious actors can bring rouge devices into the network. So many IoT devices ship with default and often useless username and passwords which attackers can easily break into. Although devices may authenticate a server, the server may not authenticate itself to the device and become susceptible to vulnerabilities. When the number of IoT devices grows, we cannot manage authentication for thousands of devices easily. It decides the extent , above what the device is allowed to operate within the blanket network. If authorization mechanisms are not used properly, it can result in too much, or in no access at all, thereby endangering the security. We often also grant devices blanket access as opposed to having a device restrict itself to roles or functions. In an industrial automation environment, many times devices will join or leave the network and maintaining updated authorization policies becomes difficult. With the abundance of IoT devices comes the need for robust authentication mechanisms to protect against unauthorized access as well as to only allow trusted devices talk within the network. Current deployments of IoT in industrial settings are in remote or unattended locations. Physical tampering with or theft of devices, inserting rogue devices into the network, and not having surveillance and monitoring, are the challenges.

2.3 Scalability and Interoperability

Industrial IoT networks are complex and, as such, offer great opportunity and challenge in security for the uniformity of security measures. They also transmit and store enormous masses of sensitive operational data, and breaches are a gaping vulnerability for them. Data breaches and exfiltration. Manipulation or corruption of data impacting decision-making. Non-compliance with data protection regulations. The absence of uniform security standards in IoT devices and protocols creates compatibility and security gaps. The various challenges are difficulty in integrating devices from different vendors securely, use of outdated or proprietary protocols and Inconsistent implementation of security features. As the number of IoT devices grows, ensuring security becomes increasingly challenging. There may be difficulty in managing and monitoring large-scale deployments, increased risk of DDoS attacks and insufficient resources to handle real-time threat detection [7].

2.4 Fault Tolerance and Reliability

System failures or attacks on centralized security architectures can lead to significant operational disruptions. Decentralized approaches are crucial for maintaining reliability and fault tolerance. Industrial automation often involves third-party vendors and systems. The different challenges includes supply chain attacks through compromised components, lack of transparency in vendor security practices and risk of backdoors or malware from external integrations. Many industrial automation systems are built on legacy infrastructure not designed for IoT integration. They are incompatibility with modern security solutions, unpatched vulnerabilities due to outdated software and high cost and complexity of upgrading legacy systems. Industrial systems require low latency and high reliability, often limiting the implementation of heavy security measures. But performance and security comes at a trade of price, the problem of finding real time intrusion detection is hard, and there is a risk of system downtime if a security breach occurs.

III. BLOCKCHAIN TECHNOLOGY: AN OVERVIEW

Decentralized and distributed ledger system that aims to work safely & transparently record transactions across multiple machines. First conceived in 2008 as the foundational technology behind Bitcoin, the first cryptocurrency, by an entity known as Satoshi Nakamoto, it initially emerged as open source in 2009. Blockchain has evolved to include multiple uses and is not only used for digital currencies, but also banking, supply chain management, healthcare and industrial automation.

Block chain essentially refers to a series of blocks, each with a bunch of transactions included. Because these blocks are connected using cryptographic hashes, once a block is integrated into the chain, its contents cannot be changed, without changing all other blocks afterwards in a computationally impossible way [8]. It's lack of immutability makes it highly resistant to fraud, it is essentially impossible to manipulate the blockchain. By consensus, such as Proof of Work (PoW) or Proof of Stake (PoS), blockchain transactions are authenticated, where all participating nodes must agree on the ledgers state.

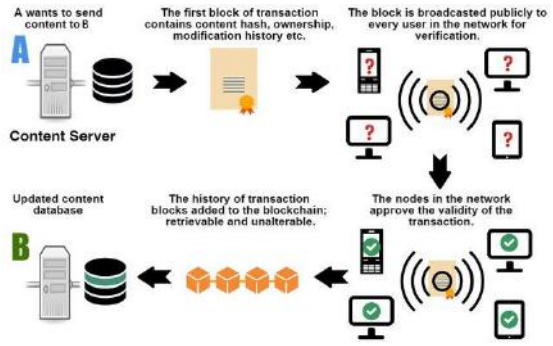

Fig.2. Overview of the blockchain working principle

Because blockchain operates on a peer to peer (P2P) network, it doesn't require the use of middlemen like banks or clearinghouses. It also makes for more transparency and less transaction cost. In addition, by employing state of the art cryptographcz methods, blockchain ensures the privacy as well as the security of participants, who are able to preserve anonymity as they authenticate transactions. Built on blockchain, smart contracts self-executing contracts with terms encoded directly extend its functionality by building automated operations and reducing intermediaries' dependence. There are some benefits to blockchain technology, however, it is facing challenges of scalability, as well as energy consumption (PoW systems specifically) and regulatory uncertainty. Yet advancements, including Layer 2 solutions, green consensus mechanisms and regulatory frameworks, have sought to solve these [9]. As the technology behind blockchain matures, it is having a major impact on industries by way of adding safety, transparency and efficiency to what it has introduced, pointing to blockchain as a transformative force of the digital age.

3.1 Core Features of Blockchain

- *Decentralization:* It removes the need for a central authority, making single points fail.
- *Immutability:* As a guarantee that data written on the blockchain won't be retrievable and then obsolete.
- *Transparency*: Allows all participants in the network to view transaction records.
- *Security*: Cryptographic mechanisms protect data confidentiality and integrity.

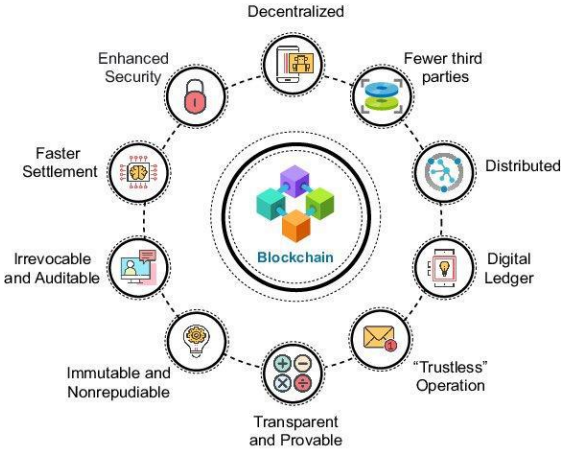

Fig.3. Core features of blockchain

3.2 Consensus Mechanisms

Consensus algorithm is used in blockchain to validate transactions. Common mechanisms include:

- *PoW:* Ensures security through computational effort but is resource-intensive.
- *PoS:* Minimizes energy usage by choosing validators according to their stake.
- *PBFT*: Suitable for private blockchains with high throughput requirements.

3.3 Smart Contracts

The term 'Smart contracts' refers to self executing programs that are stored on the blockchain and executes predefined rules to do something like authentication or access control.

IV. BLOCKCHAIN-BASED SECURITY FRAMEWORKS FOR IIOT

Currently, blockchain technology is being widely adopted as a solid security solution to the IIoT, especially in the aspects of data integrity, device authentication, and security communication. IIoT systems are made up of interconnected devices, sensors and machinery that collectively collect and share critical operational data in industrial settings. However, traditional centralized security models face challenges with scale, complexity and dynamic IIoT networks, making blockchain based models an attractive alternative.

The use of blockchain based security framework exploits the decentralized, immutable and transparent nature of blockchain to secure and trustworthy base operations in IIoT ecosystems. Work done in these frameworks rely on using distributed ledger technology (DLT) to remove probability of exploits occurring in the form of single points of failure. IIoT devices are recording transactions and data exchanges over tamper proof blocks for data integrity and traceability. Beyond, smart contracts can be used to automate and enforce security policies such as granting or revoking device access and make sure devices are indeed in compliance with operational protocols [10].

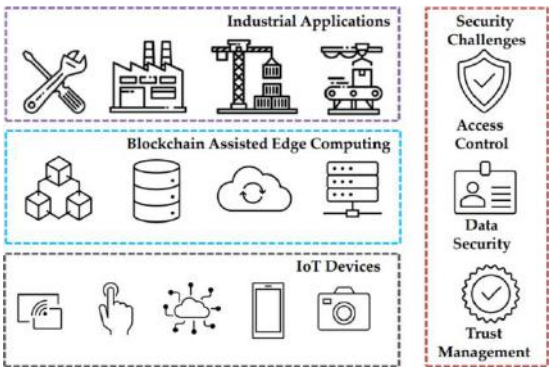

Fig.4. IoT systems and its security challenges

With device authentication and authorization being one of the critical IIoT applications of blockchain. The framework stores unique device identities on the blockchain and only trusted devices can access the network. The consensus mechanisms provide a mechanism to validate that devices are authentic and their activities and in addition prevent unauthorized entities from infiltrating the system. Moreover, the blockchain provides a secure means of sharing data between IIoT devices in encrypted and verifiable transactions so that sensitive information is not susceptible to interception or tampering.

However, current and potential IIoT blockchain deployments tend to struggle with high computational overhead, scalability limits, and incompatibility with existing IIoT systems [11]. But blockchain advancement efforts such as lightweight consensus algorithms, off-chain data storage and hybrid blockchain architectures will mitigate these problems. Potential solution to IIoT network security challenges can be provided by blockchain based security frameworks. Combining blockchain with IIoT allows industries to realize increased security, transparency, as well as operational efficiency, paving the way for smarter and more resilient industrial systems.

4.1 Architecture of Blockchain-based Frameworks

Specific use cases such as IIoT, financial systems, and supply chains are served by Blockchain based frameworks that are secure, transparent and decentralized frameworks. Other times, they are comprised of multiple layers and components that work together to create what wants to be achieved. Typical frameworks consist of

- *Blockchain Layer*: Stores transaction data securely and enables decentralized communication.
- *IoT Layer*: Comprises IoT devices, gateways, and edge computing nodes.
- *Application Layer*: Provides user interfaces and analytics tools.

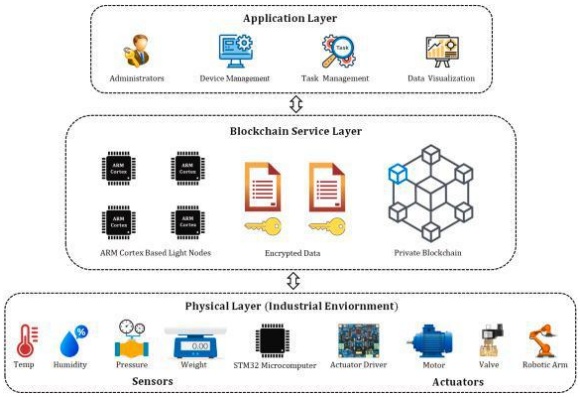

Fig.5. Architecture of Blockchain

4.1.1 Workflow in Blockchain-Based Frameworks

- *Transaction Initiation*: For example, a transaction (e.g, data sharing or smart contract execution) is submitted by a user or device.
- *Validation and Consensus*: Once the consensus is achieved the transaction is broadcasted to the network, validated by the nodes that participate and it will be included in a new block.
- *Block Creation and Storage*: An appended validated block will ultimately be added to the blockchain ledger, which means data immutability and this entire development process is repeatable.
- *Execution of Smart Contracts*: Smart contracts are used to enforce business rules or logic if needed.
- *Data Access and Reporting*: Data or interaction with the blockchain is retrieved by authorized users or systems using APIs or DApps.

4.1.2 Key Benefits of Blockchain-Based Frameworks

- *Security*: Tamper-proof ledger ensures data integrity and confidentiality.
- *Transparency*: Provides an auditable and immutable record of transactions.
- *Decentralization*: Eliminates reliance on a central authority, reducing vulnerabilities.
- *Scalability*: Advanced architectures enable scalability for large networks.

V. INTEGRATION WITH EMERGING TECHNOLOGIES

5.1 Edge Computing

Using Blockchain combined with edge computing reduces the latency and improves real time processing capabilities for IIoT applications. By merging the powerful cryptographic security of data decentralization with the best of real time data processing and edge computing, blockchain merge can be applied as a robust framework for modern digital ecosystem. This means that computational tasks are moved closer towards the data sources, like IoT devices, lowering latency and bandwidth utilization. This is where blockchain comes in to complement, and provide a secure, immutable, and decentralized way of checking data integrity, device authentication, and trustworthy communication across edge networks [12].

However, in traditional cloud centric architectures, data coming from edge devices is sent up to central servers to process and store the data, which creates high latency, scalability issues and potential security issues. The blockchain decentralized the data management process to address this challenge. They securely record transactions or device interactions at the edge in a distributed ledger, and are tamperproof and verifiable. This integration is especially important in the scenario of IIoT with real time decision making and high security standards.

Through the confluence of blockchain with edge computing, devices can securely communicate with one another and authenticate themselves, without relying on centralized authorities such as a human. As an example of this, smart contracts can be based on blockchain and can automate and enforce such access control policies at the edge, such that only authorized devices or users can access sensitive systems. Furthermore, it also helps in sharing data between edge nodes transparently and audibly log of interactions, and this raises the trust in the collaborative ecosystem like smart cities or the connected healthcare system. However, the integration of blockchain with edge computing suffers from computation overhead of blockchain operations and the resource constraints of the edge devices. To address these problems, solutions such as lightweight consensus mechanisms (e.g., Proof of

Authority) and hybrid architectures that offload critical blockchain function to more capable nodes, are being developed. Combing blockchain and edge computing opens up a powerful security, transparency, and efficiency-enhancing weapon in decentralized systems. With this integration poised to help advance applications ranging from autonomous vehicles, to industrial automation and to next generation smart infrastructures, it promises to become indispensable.

5.2 Artificial Intelligence (AI)

Putting blockchain data through an AI algorithm which detects anomalies and can predict potential security threats improves proactive defense. The combination of blockchain with AI enables powerful synergy by improving data security, transparency, and decision making within most applications. Blockchain's intrinsic decentralized and immutable characteristics are leveraged to solve many of the challenges surrounding AI, like data provenance, sourcing of trust, and participatory transparency, while AI helps optimize functions like consensus mechanisms, and fraud identification. Together, these technologies' solutions are more secure, more reliable, and more efficient.

Some great benefits of this integration are data integrity. Vast amounts of high quality data are needed to train and make decisions in AI systems, and determining authenticity and origin of data can be difficult. The data used by AI models is proven accurate and reliable due to blockchain's tamper proof record of data provenance [13]. In healthcare, finance and supply chain management, this is important because data integrity is critical.

Improving transparency and accountability of AI algorithm is another important advantage for others. And many AI systems fall into the category of "black box" systems, a reality which makes it difficult to understand or audit their decision making processes. With the ability to record AI Decisions and process on the blockchain, organizations can create an irreplicable audit trail that increases trust and ensures that regulations are followed. It is particularly useful for autonomous vehicles, credit scoring and legal decision making.

AI also helps Blockchain by optimising its functioning. Blockchain can be further secured using AI to analyze the blockchain data and detect anomalies or any fraudulent activities. Moreover, AI can improve consensus mechanisms that would scale and improve the blockchain networks. For example, machine learning algorithms can forecast and counteract any network bottlenecks that may already exist, in real time. While there is much promise to integrating blockchain and AI, as with all de-centralized technologies there are inherent hurdles such as the computational requirements for both and the integration with infrastructures being used. But lightweight blockchain protocols and edge AI are helping these problems.

Blockchain AI integration has the potential to be revolutionary by combining the trust and security of blockchain with the intelligence and efficiency of AI. It is creating a powerful combination that is reshaping industries in order to provide smarter and more secure solutions to an array of applications.

5.3 5G Connectivity

5G networks' high-speed and low latency communication complements blockchain's capability, allowing the seamless industrial automation. Blockchain integration with 5G connectivity has the prospect to revolutionize industries by delivering greater security, better efficiency and greater scalability for next generation networks as 5G provides faster data transfer speeds, lower latency and scales support massively connected devices - applications like autonomous vehicles, smart cities and industrial automated products. But, with more devices and data flows, security, data privacy and network management problems also increase. To overcome this challenge, Blockchain can offer a decentralized, secure and transaparent solution for the management of the complex interactions within 5G networks [14].

Augmenting blockchain with 5G has one of the biggest advantages as it boosts the security. Blockchain's decentralized properties mean there are no single points it can be attacked from. It can be applied to secure authentication of devices, identity managing and the verification of transactions among devices in a 5G enabled ecosystem. This assures that only the allowed devices can access the network and thereby reduces the risk of cybercrime, data breach, and also fraudulence. Blockchain can also serve as a

secure and tamper proof ledger for network transactions and data exchange, then providing yet another layer of trust and transparency.

Moreover, blockchain makes it easier to manage network resources. Bandwidth, management becomes tricky and Quality of Service (QoS) more complex with growing number of devices in 5G network. According to Bisgaard, blockchain's smart contracts can execute the allocation and management of network resources according to certain conditions, which eliminates the requirement of manual interference and enhances the operation of the network. This is also possible by Blockchain: to support Decentralized and dynamic pricing models for network services that would allow users to pay for services in real time.

In addition, blockchain boosts the potential of 5G with regard to IoT, where billions of IoT devices will have to communicate securely and in a scalable manner. From a data exchange perspective, blockchain can form the backbone for the secure exchange of IoT data amongst IoT devices in a 5G network while at the same time guaranteeing data integrity, privacy and communication across devices [15]. But blockchain integration with 5G networks remains a challenge, as 5G networks require high computation from blockchain consensus mechanism and blockchain integration with different blockchain platforms need interoperability. To make the integration more feasible these issues, solutions such as lightweight consensus algorithms and hybrid blockchain architectures are developed. Using 5G connectivity in combination with the blockchain ensures that the network management deployed is secure, efficient and scalable and leaves open the path for full potential of next generation applications. The integration of autonomous vehicles and smart cities is only starting and the possibilities are endless in everything from audio systems to food delivery.

5.4 Cybersecurity

The integration of blockchain with cybersecurity provides a powerful solution to address the increasing threats and vulnerabilities in digital systems. Blockchain's decentralized, immutable, and transparent nature enhances traditional cybersecurity measures by ensuring data integrity, securing communications, and enabling decentralized authentication and access control. In today's interconnected world, where cyberattacks are becoming more sophisticated and pervasive, this integration offers a robust defense mechanism to safeguard sensitive data and prevent unauthorized access [16].

One of the key advantages of combining blockchain with cybersecurity is its ability to ensure data integrity. Blockchain provides a tamper-proof ledger, making it nearly impossible for attackers to alter or manipulate data once it is recorded. This is particularly valuable in industries where data integrity is critical, such as finance, healthcare, and supply chains. Blockchain can also be used to securely store logs of system events and network transactions, creating an immutable audit trail that can be analyzed for signs of malicious activity.

Another significant benefit is in the area of identity and access management. Blockchain enables decentralized identity management, where users control their own identities using cryptographic keys. This reduces the risk of identity theft, phishing, and unauthorized access. Blockchain-based solutions, such as self-sovereign identities, ensure that user credentials are stored securely and that authentication processes are transparent and tamper-resistant [17].

Blockchain can also help mitigate DDoS attacks and other forms of network disruption. By decentralizing the flow of data and distributing it across a network of nodes, blockchain makes it more difficult for attackers to target a single point of failure. Additionally, blockchain can be integrated with smart contracts to automatically enforce security policies, detect anomalies, and respond to threats in real time, further enhancing the system's ability to defend against cyber threats.

However, integrating blockchain with cybersecurity is not a walk in the park. Consensus algorithms may be computationally expensive, or blockchain networks may be overly scaled for a high traffic environment. For this, while lightweight blockchain protocols and hybrid solutions which integrate blockchain with conventional approaches of security are being made.

By integrating blockchain, traditional security frameworks gain both decentralized, verified and

immutable solutions to prevent fraud, maintain data integrity as well as improve identity management. Together, this combination has the potential to secure digital assets, and mitigate against many cyber threats.

VI. RESEARCH GAPS AND FUTURE DIRECTIONS

For the past few years, we have seen a lot of attention paid to the integration of blockchain with IIoT for secure use cases. But unfortunately, there are still some research gaps which need future improvements in order to further exploit the application of blockchain as a means in securing IoT devices in industrial automation.

- Scalability Challenges : Scalability requires the development of lightweight consensus mechanisms well-adapted to IIoT environments.
- Real-time Performance : Research continues on optimizing blockchain frameworks for real time industrial applications.
- Interoperability Standards : Standardized protocols can improve adoption if we define them for integrating blockchain with heterogeneous IIoT systems.
- Energy Efficiency : For industrial deployment, blockhain operations need to be sufficiently sustainable and the energy consumption should be minimized.

Blockchain brings among them significant potential security improvement to IIoT environments, and however, the research gaps remain. To take these blockchain based security frameworks further will require them to address issues such as scalability, interoperability, privacy, real time security and resource constraints. Consequently, future research can explore the full potential of the blockchain to give us secure, efficient, reliable security solutions for industrial automation if we concentrate on these challenges.

VII. CONCLUSION

Blockchain technology has potential to increase IoT devices security also in industrial automation. The key to solving some of the problems with data integrity, authentication and fault tolerance is the architecture which is decentralized, with features like immutability and smart contracts. Although great progress has been made, scaling, interoperability, and energy efficiency remain as challenges. There are gaps to be addressed in future research and the synergies with emerging technologies to unlock the full potential of blockchain in IIoT ecosystems should be once investigated.

REFERENCES

[1] Rahman, A., Kundu, D., Debnath, T., Rahman, M., & Islam, M. J. (2024). Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities. *arXiv preprint arXiv:2405.12550*.

[2] Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., & Muyeen, S. M. (2024). Enhancing security of internet of robotic things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. *Internet of Things*, 101357.

[3] Vaigandla, K. K., Karne, R., Siluveru, M., & Kesoju, M. (2023). Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications. *Mesopotamian Journal of CyberSecurity*, *2023*, 73-84.

[4] Kumar, S., Kumar, M., Azmea, C. N., & Vaigandla, K. K. (2024). BCSDNCC: A Secure Blockchain SDN framework for IoT and Cloud Computing. *International Research Journal of Multidisciplinary Technovation*, *6*(3), 26-44.

[5] Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, *16*(23), 10177.

[6] Nazir, A., He, J., Zhu, N., Anwar, M. S., & Pathan, M. S. (2024). Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain. *Cluster Computing*, 1-26.

[7] Goyal, N., Veeraiah, V., Namdev, A., Anand, R., Gupta, A., & Shilpa, S. (2024, March). IoT based Blockchain System for Security from Identity Theft in Industrial Automation. In *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies* (pp. 1-4). IEEE.

[8] El Madhoun, N., & Hammi, B. (2024, January). Blockchain technology in the healthcare sector: overview and security analysis. In *2024 IEEE 14th annual computing and communication workshop and conference (CCWC)* (pp. 0439-0446). IEEE.

[9] Huan, N. T. Y., & Zukarnain, Z. A. (2024). A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. *IEEE Access*.

[10] Zanbouri, K., Darbandi, M., Nassr, M., Heidari, A., Navimipour, N. J., & Yalcın, S. (2024). A GSO-based multi-objective technique for performance optimization of blockchain-based industrial Internet of things. *International Journal of Communication Systems*, *37*(15), e5886.

[11] Xiao, N., Wang, Z., Sun, X., & Miao, J. (2024). A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alexandria Engineering Journal*, *86*, 631-643.

[12] Nguyen, T., Nguyen, H., & Gia, T. N. (2024). Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. *Journal of Network and Computer Applications*, 103884.

[13] Kuznetsov, A., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the integration of artificial intelligence and blockchain technology: a perspective about security. *IEEE Access*.

[14] K. K. Vaigandla, "Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis," 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India, 2022, pp. 27-31, doi: 10.1109/ICIPTM54933.2022.9753990.

[15] Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2024). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4329.

[16] Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D. S. (2024). Tides of Blockchain in IoT Cybersecurity. *Sensors*, *24*(10), 3111.

[17] R. Yadav, Ritambhara, K. K. Vaigandla, G. S. P. Ghantasala, R. Singh and D. Gangodkar, "The Block Chain Technology to protect Data Access using Intelligent Contracts Mechanism Security Framework for 5G Networks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 108-112, doi: 10.1109/IC3I56241.2022.10072740.