PUXplore: Multidisciplinary Journal of Engineering, Vol 2, Issue 2, Apr – Jun 2026 || Online (ISSN 3108-2106)

SECURE IOT-BASED AUTOMATIC GATE SYSTEM WITH DECENTRALIZED AUTHENTICATION AND BIBLIOMETRIC ANALYSIS

Alok Pandit[1], Minal Shukla[2], Pooja Sapra[3], Amit Sata[4], Payal Singh[5], Pravin Vadhel[6]

[1,3]Department of Information Technology, PIET, Parul University, Vadodara, Gujarat, India
[2,5,6]Department of Applied Science and Humanities, PIET, Parul University, Vadodara, Gujarat, India
[4]Department of Mechanical Engineering, Marwadi University, Rajkot, Gujarat, India
E-mail: [1]alokpandit2003@gmail.com, [2]shuklaminal19@gmail.com, 3pietithod@paruluniversity.ac.in, [4]amit.sata@marwadieducation.edu.in, [5]payal.singh2875@paruluniversity.ac.in, [6]pravin.vadhel43055@paruluniversity.ac.in
ORCID: [1]https://orcid.org/0009-0003-3575-024X, [2]https://orcid.org/0000-0002-2880-3046, [3]https://orcid.org/0000-0002-3894-2023, [4]https://orcid.org/0000-0002-0945-3095, [5]https://orcid.org/0000-0002-6515-0822, [6]https://orcid.org/0000-0002-0345-2649

Keywords: IoT, Blockchain, Smart Contracts, Security Analytics, Bibliometric Analysis

Abstract
The use of IoT-based automatic gate systems is on the rise in smart cities, healthcare, and transportation sectors; however, centralized authentication systems create single points of failure, scalability issues, and security risks. In this paper, a secure automatic gate system using decentralized blockchain-enabled authentication is proposed. Smart contracts are utilized to implement immutable access control without the need for a central authority. A machine learning-based anomaly recognition framework is incorporated to identify and prevent malicious or anomalous access attempts in real-time. Edge and fog computing concepts are leveraged to minimize latency and improve energy efficiency. In addition, a bibliometric study of peer-reviewed articles (2015-2025) on blockchain-enabled verification is performed using Scopus and Web of Science® datasets. The bibliometric study is carried out in the RStudio® environment using the Bibliometrics package, exploring publication patterns, citation effects, collaboration patterns, and topic evolution. The findings show that research has expanded rapidly since 2018 with a focus on permissioned and hybrid blockchain models. Research gaps in energy efficiency, interoperability, and large-scale deployment of secure IoT access control systems are identified.

1. Introduction
As we build smart cities, we also need smarter gates for the smart city. We don't use the padlocks anymore. In that the gate has the sensors, Wi-Fi chip, and software that allow us to control them remotely and monitor them [1]. In smart cities, smart gates are really needed as we can manage the traffic and people across different connected areas, ensuring that only the right person gets into the right places [2]. The old gates are mechanical; now the new gates will be the Cyber-Physical systems, which means the computer and machine combined gates. We use the Edge intelligence for processing the data right at the gate instead of sending the data to the cloud, so the system will be faster. This is necessary for things like cars or trains so that they can't have to wait for the slow signals [3]. At first, we are using the central server, but in that case, there is a problem that if the server fails, then everything will break so for that we will use Attribute-Based Encryption, this means the user only gets in if their specific attributes like role and ID matches the rules rather than checking a list on a server for that particular person [4]. We are now combining the IoT with the blockchain, so we do not use the central server, meaning that the hackers can't secretly change the access logs [5]. And for the small and weak devices, we try to use lightweight methods like PUFs, which use the physical uniqueness of the computer chip as a key. After all, that also the hackers can also find other ways to trick the system, so it is challenging to prevent it [6]. When we use one central server to control all the gates, we create a single point of failure. As if the server is hacked then the all the gates go offline. The research shows these central systems are easy targets for the hackers, so we need constant Intrusion Detection Systems (IDS) to watch them [7] [8]. To fix the central server problem, we use Blockchain to spread the data across many computers using this way if one node means computer fails then also the system will work. It protects the data and ensures the data is real, which is good [9]. New research suggests that using the Smart Contract the automatic digital agreement and the AI we can automatically spot weird behaviour and also by using the Federation Learning we allows the network to learn from the data without revealing the user's private information's [10]. There are already a lot of the research on the IoT security. However, most of the existing research which don't gives a proper view of how the everything works and connects [11][12]. Most of the old reviews just talk about papers. They don't use the Bibliometrics means using the statistics to analyse publication trends. So, we need to measure the research progress quantitively [13][14]. As with the new tech like 5G coming, we need a structured and evidence-based review to find out what is missing in the current research papers, so we know that what to study next [15][16]. Recent literature has demonstrated the impact of integrating blockchain through IIoT systems to enhance trust, security, and data-driven decision-making in industrial environments, particularly in manufacturing inspection and process optimization [17][18]. While these contributions validate the practical potential of decentralized architectures, the rapid and fragmented growth of related research highlights the need for a comprehensive

bibliometric investigation. Accordingly, this study systematically analyses Web of Science–indexed literature to map the evolution, thematic structure, and research gaps of Web 3.0–based data analytics for IIoT-enabled systems. This review is the combination of all research for keeping the IoT system safe. In this, we specifically understand how the Blockchain helps keep the data private and secure. In this, we also evaluate how machine learning is used to spot hackers even in small and weak devices that don't have much battery power. This also introduces advanced ideas like Zero-trust, which means never trust anyone automatically and Federated Learning, which means learning from data without looking at the private details related to the person. The remaining document is structure as described below. Part 4 represents the basis of automated gate systems driven by IoT, including approaches for authentication. Section 5 describes the review methodology specifying data sources and selection criteria, as well as bibliometric tools. Section 6 presents a classification of IoT- powered gate systems focusing on their architecture designs, authentication methods, blockchain incorporation and intelligent security attributes. Section 7 focuses on the main security challenges and threats associated with centralised and decentralised gate control systems. Section 8 evaluates bibliometric data to understand the knowledge of the research trends and patterns in this domain. Section 9 highlights critical key research gaps identified in the existing literature, whereas Section 10 presents prospective research pathways. Ultimately, Section 11 includes the summary of the major outcomes and addition of the study.

2. Bibliometric

It has been noted that the popularity of Blockchain for IIoT has been increased in the last few years however an integration of Blockchain for IIoT especially for Automatic Gate System is yet to be fully explored. Detailed analysis of prior work-related research and development has been conducted using the two key factors promising databases such as Scopus® and Web of Science®. Meaningful insights achieved from these databases are highlighted they were searched with the keyword related to Blockchain for IIoT, and various types of documents were studied. Methodology is used for this study of bibliometrix analysis on Blockchain for IIoT conducted using open-source platform, RStudio®, and is highlighted in Table 1.

Table 1: Methodology adopted for bibliometric analysis

Bibliometric Analysis on Blockchain for IIoT Using RStudio®		
Scopus	**Database searched for documents published**	Clarivate Web of Science™
2015-2025	**Duration**	2015-2025
Articles, book chapter, review, conference paper, book, editorial	**Type**	Articles, review articles, book chapter, early access, proceeding papers
1027	**Total number**	711
English	**Language**	English

It is observed little research and development work in this domain has been conducted in last few years and seems to have very high potential for contribution. This analysis helped in deciding the direction for development of appropriate Blockchain for IIoT application. Detailed discussion on bibliometric analysis is presented next followed by methodology for development and demonstrative work supporting that methodology.

Overview

Table 2 represents the overview about bibliometric analysis carried out on documents published in both of databases. Distribution of overall documents published in Web of Science® and Scopus® are also shown in Figure 1 and 2. Documents were also merged in order to eliminate repeated documents using program executed on RStudio®, and their distribution is also represented in Figure 3.

Table 2: Overview of bibliometric analysis

Total documents (after removing 607 duplicated and retracted documents)	1131
Total number of sources (i.e., journal, conference, publishers) in which documents were published	348
Annual growth rate (in percentage)	17.6
Average citation per document	~24.5
Total number of authors contributed	2842
International co-authorship (in percentage)	28.03

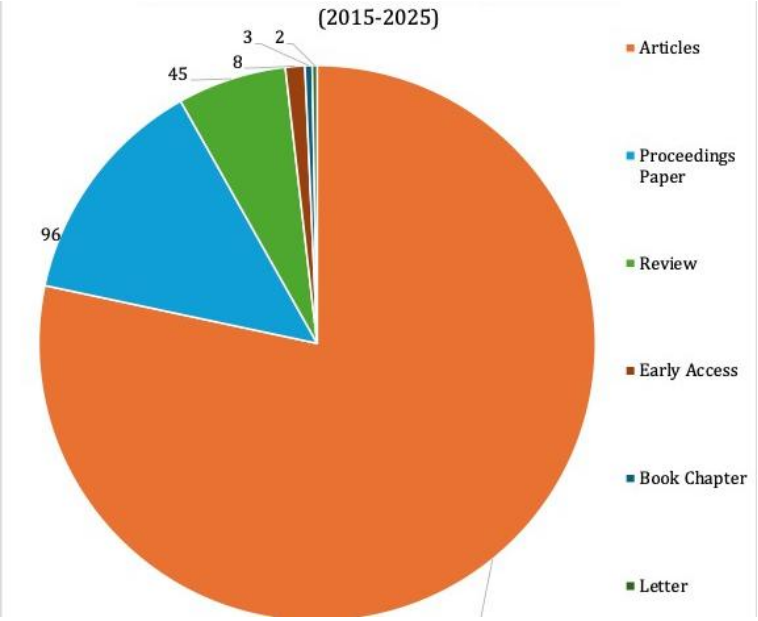

Figure 1: Type of documents published in Web of Science®

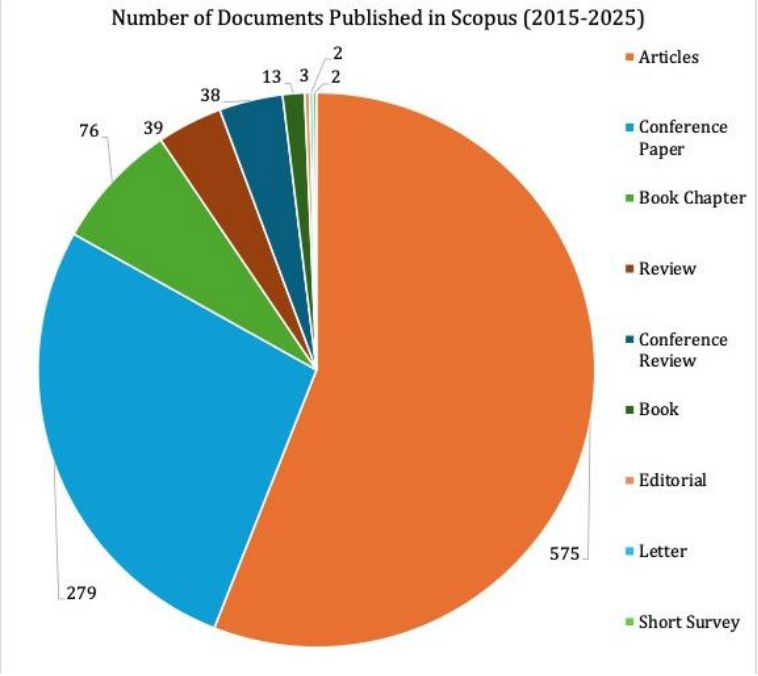

Figure 2: Type of documents published in Scopus®

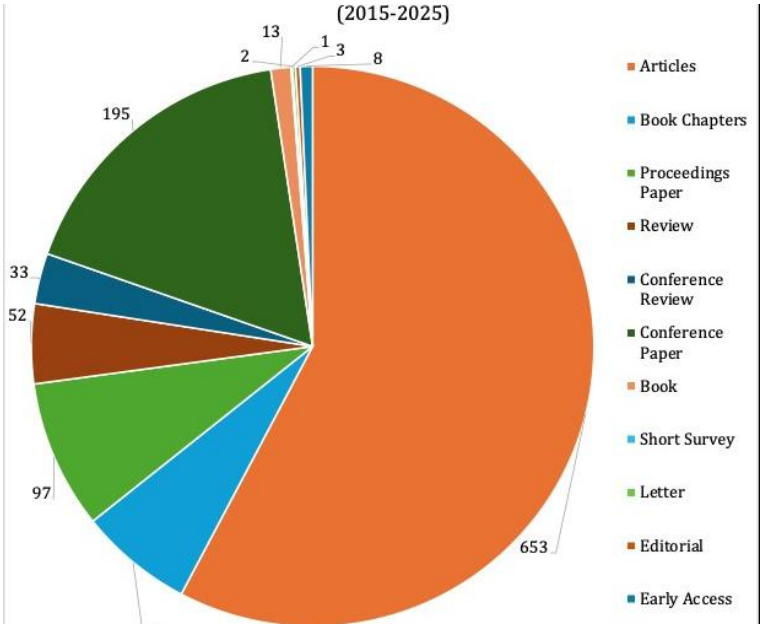

Figure 3: Distribution of documents in merged databases

Year-wise publication is also checked (Figure 4), and it was observed that number of documents published in the domain of Blockchain for IIoT is increased since 2015 with average increasing rate of 16.75%, and nearly 3175 documents published in the year of 2024. However, slight reduction in number of publications happened in the year of 2025 (till December 2025).

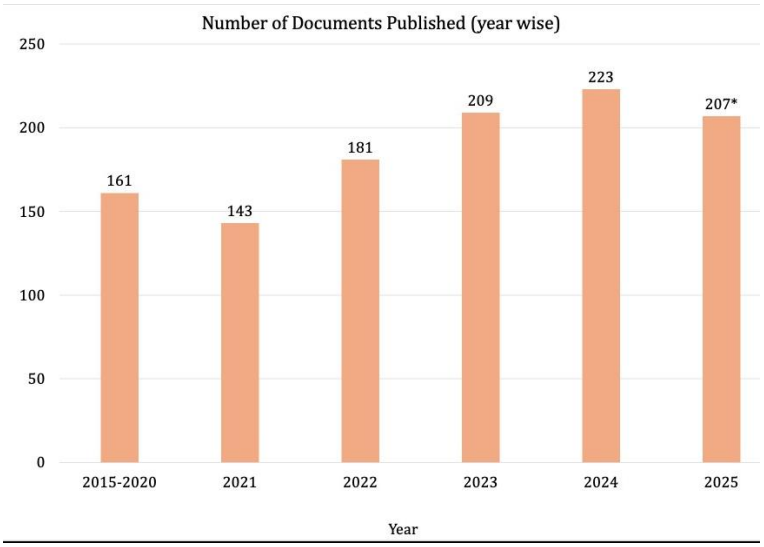

*Figure 4: Year wise publication of documents (*data is till December 2025)*

Major contributors including researchers, their affiliations, countries, sources, etc. are also found out using systematic bibliometric analysis, and is highlighted herewith.

Contributors and Collaboration

Authors conducted remarkable research in the domain of Blockchain in IIoT, and their publication, as well as h-index are represented in Figure 5. Dr. Zhang Y has highest number of documents published (i.e., 26) and h-index (=14) in this domain.

Also, most cited country and their average citations per document are shown in Figure 6. It has been noticed that China has highest rate of citations followed by India, Norway, USA, and UK. However, average citations per article is highest for Lithuania (i.e., 469.4) followed by UK (i.e., 116.70).

Average citations per article is for India is relatively low, and in the range of 20.5.

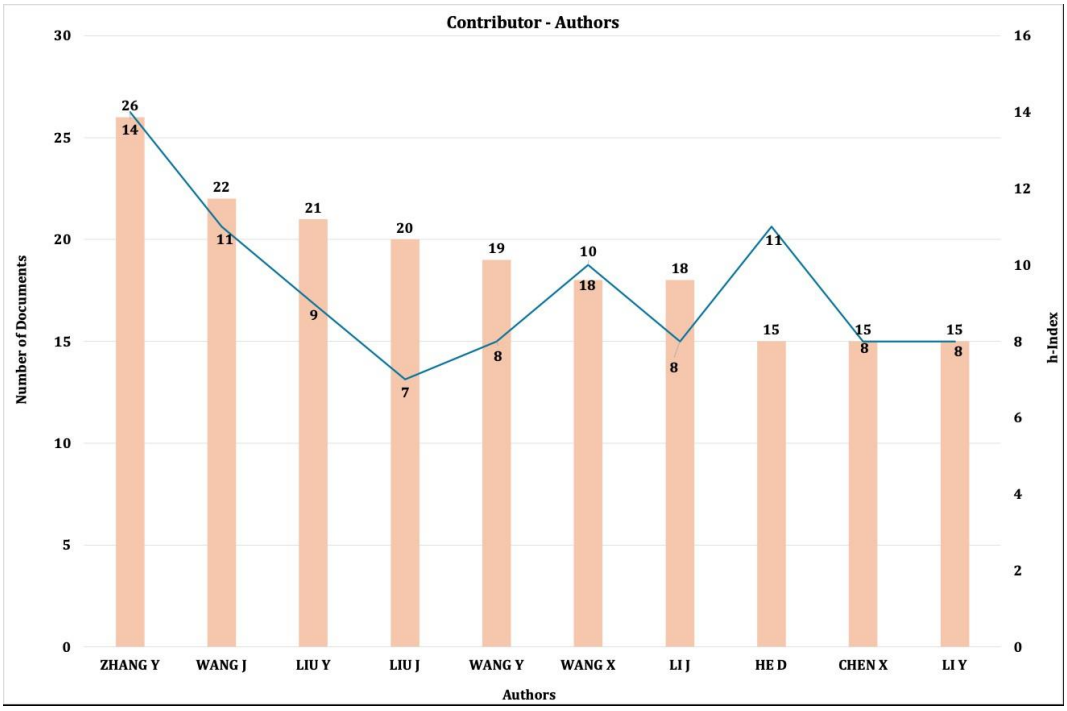

Figure 5: Top 10 Authors, and Their h index

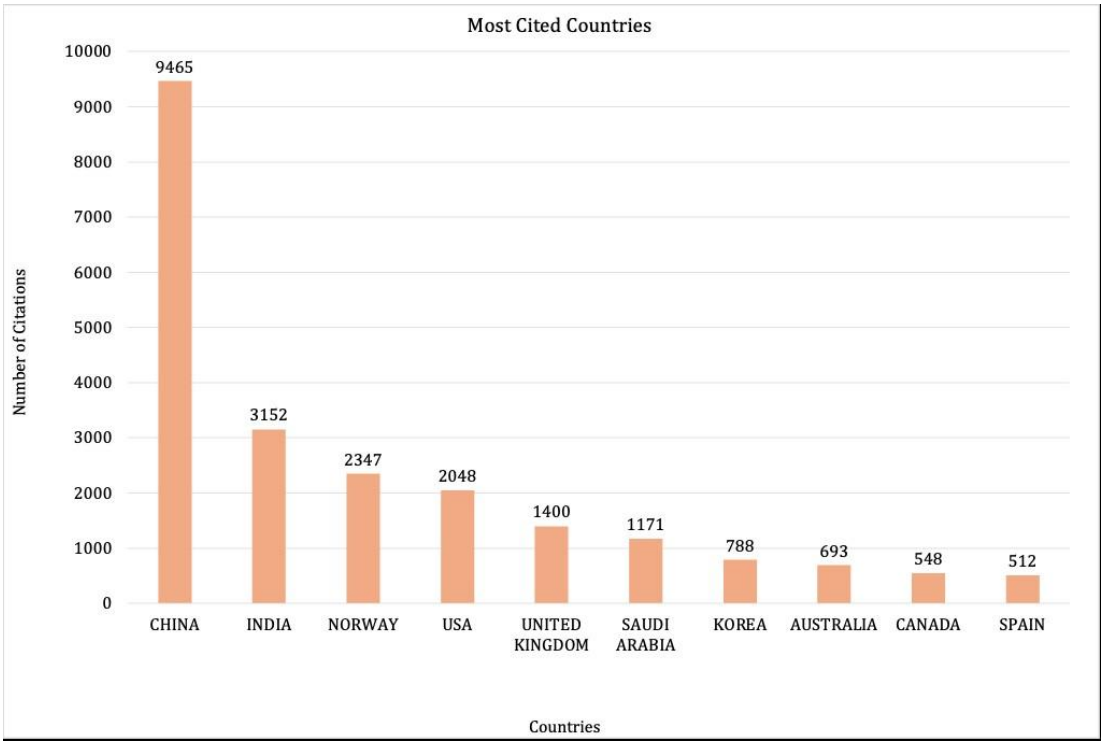

Figure 6: Most cited Countries

Specific three-field plot is generated highlighting authors, affiliated institutes and countries to highlight contribution, and is illustrated in Figure 7. It is observed that Dr Wang J from Anhui University – China has remarkably contributed in this domain.

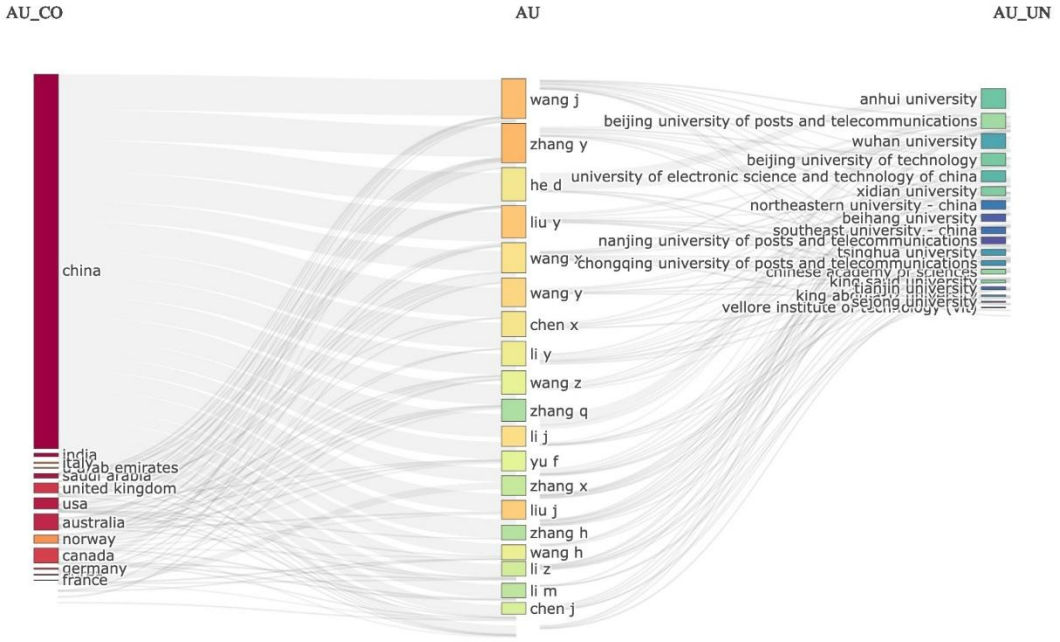

Figure 7: Three field plot highlighting institutes, authors and countries working in this domain

Collaborative research plays very important role especially in this domain. It was observed that 19.42% of documents has international co-authorship, and overview of collaboration between various countries is shown in Figure 8.

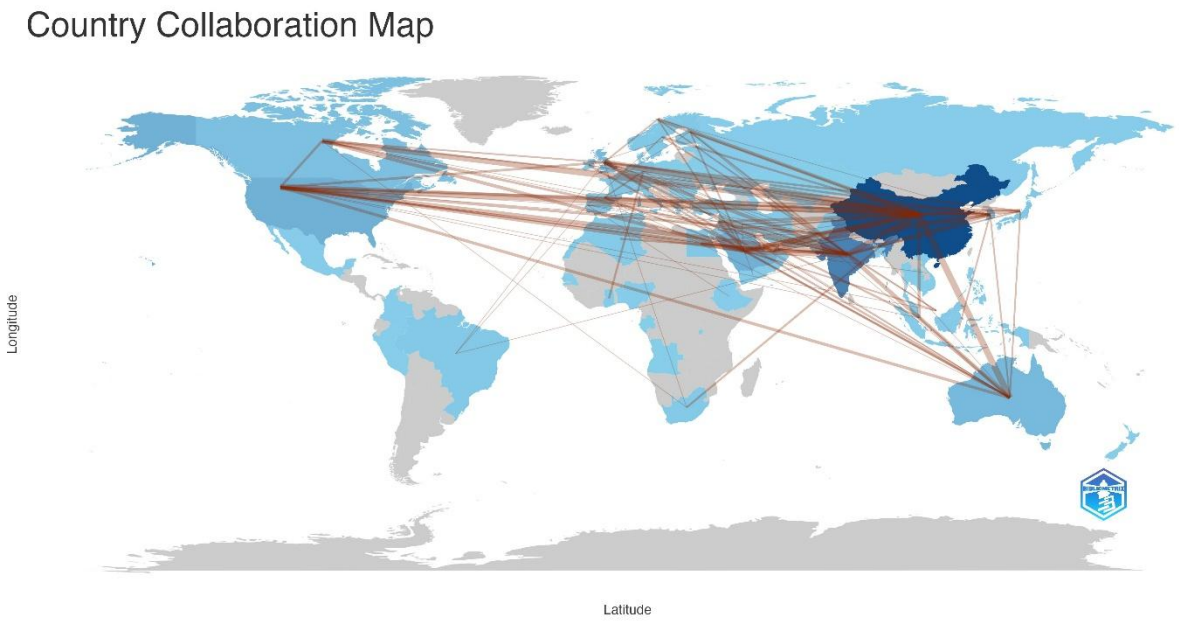

Figure 8: Collaboration between various countries for research in the domain of Image Processing for Manufacturing

China has developed strong collaboration with USA for 35 documents and with Australia for 33 documents. India has published 31 documents with Saudi Arabia; 23 with China; and 13 with USA. However, collaboration of India with Korea,

Canada, Germany, etc. can be strengthen in this domain. Detailed technical literature highlighting application of Blockchain in IIoT is summarized next.

3. Prior Work

In smart gates, we need the sensors to see the world, the sensors detect cars, motion, or ID cards using the magnetic or chemical sensing [19]. The sensors send the collected data to the controller, which is a small computer, and the controller uses the logic or AI to decide instantly if the gate should open or not [20]. Once the controller decides to open the gate, it tells the Actuators. The actuators are the motors or hydraulics that physically push the gate open or closed [21]. The interaction between the sensor and the controller is handled by MQTT. This works like sending a short text message instead of a large email, so it is fast and good for our system [22]. The controller sends the data to the wider network using wireless tech like ZigBee, Bluetooth, or LoRa, depending on how far the signal needs to go and how much battery is available [23]. To ensure that devices from different brands work smoothly together, standard communication protocols are used [24]. Earlier gate systems required on the main server for every entry request. Now, to overcome the rise and delays, we used AI to monitor abnormal behaviour instantly. Similarly, in medical IoT (IoMT), systems the Deep Learning are used to predict a cyberattack before it happens, instead of handling them after execution [25]. Instead of storing all data in a central server, we used multiple servers to reduce the security attacks and hackers' difficulty. Bio-Rollup used zero-knowledge proofs to protect biometric identification of the user with reveal the original data [26]. IPFS is used to store data in multiple parts instead of one location, which increases the privacy protection and system security of the robot as well as IoT network in PrivShieldROS [27]. AI can decide whether a user is valid or not by using blockchain-based smart contracts [28]. Similarly, in factories, these contracts are allowed to update the machine software securely without using a central server to approve every step [29]. Once a record is saved in blockchain, it cannot be deleted or updated. This method is used to protect online exam papers from hackers and cheaters [30]. Blockchain is also used in online stores to verify that the products are real or a copy [31]. It is also applied in a waste management system to track the disposal processes accurately and to make integrity of the data across all systems [32]. In Edge and Fog computing, data processing is performed closer to the gate hardware. Instead of sending all requests to the server, decisions are made locally, but only essential requests are sent to the server; this makes faster decisions, reduces time, and saves on load [33]. New 6G technology combined with Fog computing helps medical devices (IoMT) save battery. It allows devices to trust each other without needing to constantly talk to a heavy cloud server [34]. Security features improved by hardware bolster this integration with FPGA-powered zero-trust stream encryption demonstrating that assigning cryptographic operations to edge or fog nodes can achieve ultra-low latency and high-throughput secure communications suitable, for widespread 6G-NB-IoT access scenarios [35]. At the network layer, cross-layer security systems utilising SDN, NFV, and AI offer synchronised defence across edge, fog, and cloud environments, facilitating adaptable policy enforcement, anomaly identification, and secure network slicing within 5G/6G frameworks that support contemporary gate systems [36]. Federated learning allows devices to learn from data collections without sharing private files. By using secure aggregation, devices can make security decisions on-device, keeping user information private [37]. Models such as Zen Guard operate on the basic principle of never trusting any user by default. Instead of a single password check, Zen Guard regularly check the user behaviour and environment [38]. Security systems are using AI to handle a new type of attack. Models using LSTM-Attention show how AI can find threats while blockchain maintains a permanent record. This ensures that when a threat is found, it is verified and logged forever on the chain [39]. Similarly, scalable deep neural network-based Attack detection models exhibit accuracy in identifying harmful behaviours, in IoT environments [40]. During a security breach, the legally valid logs allow the system to check the status without doubt [41].

4. Methodology

We distributed tasks among multiple agents to hasten the process and avoid complete system collapse in case of one-part failure. Smart gates can communicate with the linked car via low-power communication methods such as LoRa or ZigBee, making it possible to open automatically. Contemporary systems have shifted from PFID cards that can be easily replicated to biometrics, but biometric information theft poses a privacy threat. To counter this, Zero-Knowledge Proofs confirm identity without disclosing biometric information, and wearables facilitate continuous authentication by monitoring distinct patterns such as heartbeat in real-time. Decentralized authentication systems based on blockchain technology utilize Ethereum, smart contracts, and cloud storage to eliminate the chance of a one point of failure. In this system, smart contracts are combined with AI models such as RNNs to analyse user behaviour rather than just passwords to allow entry only if the activities seem normal. The output of intrusion detection is also stored in the blockchain, providing transparency and trust through the permanent storage of warnings if a hacker is identified. Because blockchain consensus is slow, reinforcement learning is proposed to modify voting rules to make the system faster when traffic is high. Explainable federated blockchain systems integrate privacy-preserving AI, smart contracts, and decentralized storage such as IPFS to securely authenticate users and safeguard private healthcare information. These systems are both fast and accurate, making them ideal for real-time smart gate access control. Other studies have found that hybrid approaches such as CNN-LSTM are capable of handling large multi-source data and identifying different types of attacks, making them suitable for large-scale gate implementations. Lightweight solutions such as SAE-GRU are also capable of identifying complex patterns of botnet attacks while consuming low resources, making them ideal for smart city security. Additionally, solutions such as

HCAP are capable of predicting attacks in advance, allowing for early defensive measures. In UAV networks, federated learning ensures data is decentralized and maintains confidentiality by preventing the exchange of sensitive information. In contemporary IoT gate systems, faster cellular communications enhance both responsiveness and security. Although Wi-Fi and LPWAN enable low-power communication, 5G is susceptible to attacks such as jamming and spoofing, thus promoting the application of machine learning-based anomaly detection and physical-layer security techniques. Cross-layer security architectures that combine SDN, NFV, and AI further enhance 5G/6G security by facilitating fast threat detection and synchronized security enforcement across layers. Hardware technologies such as FPGAs further enhance security by encrypting information significantly faster than software, thus ensuring secure transmission in 6G IoT systems without consuming much battery power. Furthermore, clustering devices in 6G healthcare systems enhances energy efficiency by preventing unnecessary transmissions while ensuring secure and reliable connectivity. Among the most significant risks to smart gates is the presence of hackers who attempt to create identities or copy devices to gain access. Conventional security networks are prone to spoofing attacks, and hence, Physical Unclonable Functions (PUFs) are recommended to create a unique fingerprint on a chip that cannot be replicated. Blockchain technology also enhances security by providing a decentralized entry system that cannot normal user behaviour to rapidly identify and prevent malicious commands. Zero-Trust networks also provide an additional security layer by continuously authenticating user behaviour even after gaining access. Hackers can also record signals for gaining remote access and use them later, while MitM attacks allow attackers to monitor and modify transmission among nodes and central servers. Basic software programs are also ineffective in identifying these risks, but deep learning algorithms can detect hidden delays and signal patterns. The traditional methods of blockchain are too slow to verify access in real- time. To overcome this issue, some research proposes the use of AI to dynamically change the rules of consensus to enable faster response rates during peak network traffic. Smart contracts with AI can also verify access faster, and Layer-2 technology reduces storage requirements by performing complex calculations off the blockchain. Hybrid AI-blockchain models enable real-time surveillance with efficient networks. Nevertheless, even secure networks can reveal personal identity information during the login process. To overcome this problem, Attribute-Based Encryptions (CP-ABE) enables access verification without disclosing private information. Decentralized platforms such as IPFS further minimize risks compared to single-server networks. Federated Learning also enables collaboration between multiple devices for security tasks without exchanging sensitive user data. Since many IoT gate sensors devices have limited battery life and processing capacity, edge computing assists by processing data locally with reduced latency and power consumption. Moreover, efficient clustering techniques in 6G networks ensure high security with low energy consumption. Employing FPGA chips for encryption purposes is more efficient compared to software-based approaches and offers high security even for small devices.

5. Research Gap

Many studies discuss about AI and blockchain connection, but most are still limited to idea-based or low-level experiments in present, with few tested in real-world environments. Blockchain also demands bulk storage capacity and processing high power, making it difficult for low-power IoT devices, even with secondary layer support. Current security testing often uses simple attack models and old datasets, while real attackers use self-adjusting AI-based methods. Compatibility between devices from different companies is another major challenge, especially with new-generation systems. Although edge and fog computing improve real-time processing, blockchain is often treated as an additional component rather than a main system for decentralized trust. Overall, simple blockchain methods combined with AI for secure, real-time IoT applications remain an unsolved problem.

6. Conclusion

This paper proposes a secure IoT-based automatic gate automation system framework, supported by a bibliometric analysis of peer-reviewed studies, showing the shift from centralized access control systems to decentralized systems. The results validate the growing use of blockchain technology, smart contracts, machine learning models, and edge/fog computing to overcome security, privacy, trust, and scalability issues. Blockchain authentication systems efficiently remove single-point failure issues and identity fraud by using decentralized verification and cryptographic enforcement. Machine learning algorithms improve system resilience by facilitating real-time identification of anomalous access patterns and novel attack patterns. Edge and fog computing systems greatly improve response times and minimize energy consumption, making them ideal for real-time gate control applications. However, some open issues still remain unaddressed, such as the lack of real-word deployment, blockchain energy efficiency, interoperability between heterogeneous IoT devices, and inadequate testing against sophisticated cyber-attacks. It is essential to address these issues to make the proposed system more practical. In summary, this paper identifies the key research trends and gaps, forming a basis for the development of scalable, intelligent, and secure next-generation access control systems.

7. References

[1] W. Serrano, "Smart or intelligent assets or infrastructure: Technology with a purpose," Buildings, vol. 13, no. 1, p. 131, 2023, doi: 10.3390/buildings13010131.
[2] K. T. Chui, B. B. Gupta, J. Liu, V. Arya, N. Nedjah, A. Almomani, and P. Chaurasia, "A survey of Internet of Things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions," Information, vol. 14, no. 7, p. 388, 2023, doi: 10.3390/info14070388.
[3] A. Bourechak, O. Zedadra, M. N. Kouahla, A. Guerrieri, H. Seridi, and G. Fortino, "At the confluence of artificial intelligence and edge computing in IoT-based applications: A review and new perspectives," Sensors, vol. 23, no. 3, p. 1639, 2023, doi: 10.3390/s23031639.
[4] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu, and Z. Hu, "Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment," J. Cloud Comput., vol. 12, no. 1, p. 61, 2023, doi: 10.1186/s13677-023-00444-4.
[5] J. Lee, M. Kim, K. Park, S. Noh, A. Bisht, A. K. Das, and Y. Park, "Blockchain-based data access control and key agreement system in IoT environment," Sensors, vol. 23, no. 11, p. 5173, 2023, doi: 10.3390/s23115173.
[6] D.-Z. Sun, Y.-N. Gao, and Y. Tian, "On the security of a PUF-based authentication and key exchange protocol for IoT devices," Sensors, vol. 23, no. 14, p. 6559, 2023, doi: 10.3390/s23146559.
[7] P. Mahadevappa et al., "A secure edge computing model using machine learning and IDS to detect and isolate intruders," MethodsX, vol. 12, Art. no. 102597, 2024, doi: 10.1016/j.mex.2024.102597.
[8] U. Tariq and T. A. Ahanger, "Employing SAE-GRU deep learning for scalable botnet detection in smart city infrastructure," PeerJ Comput. Sci., vol. 11, Art. no. e2869, 2025, doi: 10.7717/peerj-cs.2869.
[9] Q. Arshad et al., "Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges," Complex Intell. Syst., vol. 9, pp. 6155–6176, 2023, doi: 10.1007/s40747-023-01058-8.
[10] T. Bhardwaj and K. Sumangali, "An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data," Sci. Rep., vol. 15, 2025, doi: 10.1038/s41598-025-04083-4.
[11] A. Alfahaid et al., "Machine learning-based security solutions for IoT networks: A comprehensive survey," Sensors, vol. 25, no. 11, p. 3341, 2025, doi: 10.3390/s25113341.
[12] H. Meziane and N. Ouerdi, "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems," Sci. Rep., vol. 13, 2023, doi: 10.1038/s41598-023-46640-9.
[13] E. Rodríguez, B. Otero, and R. Canal, "A survey of machine and deep learning methods for privacy protection in the Internet of Things," Sensors, vol. 23, no. 3, p. 1252, 2023, doi: 10.3390/s23031252.
[14] C. V. Kifor and A. Popescu, "Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies," Sensors, vol. 24, no. 18, p. 6139, 2024, doi: 10.3390/s24186139.
[15] M. Harvanek et al., "Survey on 5G physical layer security threats and countermeasures," Sensors, vol. 24, no. 17, p. 5523, 2024, doi: 10.3390/s24175523.
[16] B. Alturki et al., "IoMT landscape: Navigating current challenges and pioneering future research trends," Discover Appl. Sci., vol. 7, no. 26, 2025, doi: 10.1007/s42452-024-06351-w.
[17] N. Yousef, A. Sata, M. Shukla, S. Jarboui, and D. Mobarsa, "Blockchain-integrated IoT device for advanced inspection of casting defects," Scientific Reports, vol. 15, p. 5300, 2025, doi: 10.1038/s41598-025-86777-3.
[18] D. Mobarsa, A. Sata, M. Shukla, and P. K. Dutta, "Blending blockchain with manufacturing for developing smart and secure process: A review, framework and implementation," in Proc. 9th Int. Congr. on 3D Printing Technologies and Digital Industry, Cluj-Napoca, Romania, Sep. 18–19, 2025.
[19] W. Jiang, C. Liu, W. Liu, and L. Zheng, "Advancements in intelligent sensing technologies for food safety detection," Research, vol. 8, Art. no. 0713, 2025, doi: 10.34133/research.0713.
[20] I. Essamlali, H. Nhaila, and M. El Khaili, "Advances in machine learning and IoT for water quality monitoring: A comprehensive review," Heliyon, vol. 10, Art. no. e27920, 2024, doi: 10.1016/j.heliyon. 2024.e27920.
[21] J. W. Lai, "Research on prediction algorithm of effluent quality and development of integrated control system for wastewater treatment," Sci. Rep., vol. 15, no. 19257, 2025, doi: 10.1038/s41598-025-03612-5.
[22] A. Chai et al., "DUA-MQTT: A distributed high-availability message communication model for the industrial Internet of Things," Sensors, vol. 25, no. 16, p. 5071, 2025, doi: 10.3390/s25165071.
[23] V. Iordache et al., "Integrating connected vehicles into IoT ecosystems: A comparative study of low-power, long-range communication technologies," Sensors, vol. 24, no. 23, p. 7607, 2024, doi: 10.3390/s24237607.
[24] W. Azariah et al., "A survey on open radio access networks: Challenges, research directions, and open source approaches," Sensors, vol. 24, no. 3, p. 1038, 2024, doi: 10.3390/s24031038.
[25] M. F. Ali et al., "HCAP: Hybrid cyber-attack prediction model for securing healthcare applications," PLOS One, vol. 20, no. 5, Art. no. e0321941, 2025, doi: 10.1371/journal.pone.0321941.
[26] J. Yun, Y. Lu, X. Liu, and J. Guan, "Bio-rollup: A new privacy protection solution for biometrics based on two-layer scalability-focused blockchain," PeerJ Comput. Sci., vol. 10, 2024, doi: 10.7717/peerj-cs.2268.
[27] T. Wang et al., "PrivShieldROS: An extended robot operating system integrating Ethereum and interplanetary file system for enhanced sensor data privacy," Sensors, vol. 24, no. 10, p. 3241, 2024, doi: 10.3390/s24103241.

[28] S. Swetha and J. P. P. M., "A novel dilated weighted recurrent neural network-based smart contract for secure sharing of big data in Ethereum blockchain using hybrid encryption schemes," PeerJ Comput. Sci., vol. 11, 2025, doi: 10.7717/peerj-cs.2930.
[29] M. Alabadi and A. Habbal, "Next-generation predictive maintenance: Leveraging blockchain and dynamic deep learning in a domain-independent system," PeerJ Comput. Sci., vol. 9, 2023, doi: 10.7717/peerj-cs.1712.
[30] H. A. Nahi, S. M. Hashim, and D. J. Kreem, "Blockchain for baccalaureate examination sheets protection in Iraq," Indonesian J. Electr. Eng. Comput. Sci., vol. 29, no. 2, pp. 1183–1191, 2023, doi: 10.11591/ijeecs. v29.i2. pp1183-1191.
[31] K. W. Goh et al., "Blockchain-based online virtual store (BOVS): A secure framework for managing machine-created elements in business process management," J. King Saud Univ.–Comput. Inf. Sci., vol. 37, p. 276, 2025, doi: 10.1007/s44443-025-00240-x.
[32] K. Bułkowska, M. Zielińska, and M. Bułkowski, "Implementation of blockchain technology in waste management," Energies, vol. 16, no. 23, p. 7742, 2023, doi: 10.3390/en16237742.
[33] D. Rajagopal and P. K. T. Subramanian, "AI augmented edge and fog computing for Internet of Health Things (IoHT)," PeerJ Comput. Sci., vol. 11, Art. no. e2431, 2025, doi: 10.7717/peerj-cs.2431.
[34] R. Yuvarani et al., "Energy-aware cluster head optimization and secure blockchain integration for heterogeneous 6G-enabled IoMT networks," Sci. Rep., vol. 15, no. 30009, 2025, doi: 10.1038/s41598-025-15462-2.
[35] W. C. Tsai, "FPGA-based implementation of zero-trust stream data encryption for enabling 6G-NB-IoT massive device access," Sensors, vol. 24, no. 3, p. 853, 2024, doi: 10.3390/s24030853.
[36] Z. Allaw, O. Zein, and A.-M. Ahmad, "Cross-layer security for 5G/6G network slices: An SDN, NFV, and AI-based hybrid framework," Sensors, vol. 25, no. 11, p. 3335, 2025, doi: 10.3390/s25113335.
[37] W. Yao, T. Zhou, Y. Han, and X. Wang, "Verifiable secure aggregation scheme for privacy protection in federated learning networks," Discover Computing, vol. 28, no. 175, 2025, doi: 10.1007/s10791-025-09676-1.
[38] A. Hassan et al., "ZenGuard: A machine learning-based zero trust framework for context-aware threat mitigation using SIEM, SOAR, and UEBA," Sci. Rep., vol. 15, no. 35871, 2025, doi: 10.1038/s41598-025-20998-4
[39] Q. Zhang et al., "Blockchain-powered LSTM-attention hybrid model for device situation awareness and on-chain anomaly detection," Sensors, vol. 25, no. 15, p. 4663, 2025, doi: 10.3390/s25154663.
[40] M. A. Hossain, "Deep learning-based intrusion detection for IoT networks: A scalable and efficient approach," EURASIP J. Inf. Secur., vol. 2025, no. 28, 2025, doi: 10.1186/s13635-025-00202-w.
[41] P. Reedy, "Interpol review of digital evidence for 2019–2022," Forensic Sci. Int.: Synergy, vol. 6, 2023, doi: 10.1016/j.fsisyn.2022.100313.