International Journal of Communication Networks and Information Security
2024, 16(4)
ISSN: 2073-607X,2076-0930
https://ijcnis.org/

Research Article

Towards Proactive Platforms for Mitigating Cyber Risks of IoT Devices Using Frameworks AI, Blockchain and DLT as an Approach to Security Enhancement: A Comparative Survey with Caliax platform

Ahmed Aljhayyish[1*], Asghar Tajoddin[2], Nawar Jumaah[3]

[1] PhD Student, College of Computing and IT Engineering, Information Technology Department, University of Qom, and Assistant Teacher, Computer Technology Engineering Department, University of Imam Kadhum, Diwaniyah Sections, Iraq.
[2] Assistant professor, Department of Electrical and Engineering, Faculty of Computer, University of Zanjan, Iran.
[3] Assistant teacher, Department of Computer Engineering, Ministry of Education, Baghdad, Iraq.

***Corresponding Author:** ahmedaljhayyishi@gmail.com., ahmedaljhayyish@gmail.com.

ARTICLE INFO

Received: 31 Sep 2024
Accepted: 4 Nov 2024

ABSTRACT

In the rapidly expanding IoT landscape, security concerns, particularly regarding old firmware, are gaining greater significance. This paper surveys comparisons of the top IoT platforms, such as AWS IoT, Microsoft Azure IoT, Google Cloud IoT, and the CALIAX platform IoT, with a special emphasis on secure over-the-air (OTA) firmware updates. CALIAX differentiates itself by incorporating artificial intelligence (AI), blockchain, and decentralized technologies to improve security. The research analyzes important metrics, including OTA success rates, scalability, energy usage, and security protocols. Studying the structures of these platforms shows the benefits of merging AI and blockchain to enhance IoT security, guaranteeing preemptive defense and effective update processes. Moreover, issues such as maintaining data accuracy and ensuring network stability are also being tackled. The results highlight the capability of AI and blockchain technologies to ensure the security of IoT devices, providing a more durable and adaptable method for handling OTA firmware updates in different industries.

Keywords: IoT Security, OTA Firmware Updates, CALIAX Platform IoT, AI, Blockchain.

INTRODUCTION

The Internet of Things is growing quickly, transforming various sectors like smart cities, healthcare, and industrial automation into the advanced revolution. Billions of devices are already connected, while global figures indicate an exponential increase in the rollout of IoT devices (Figure 1).

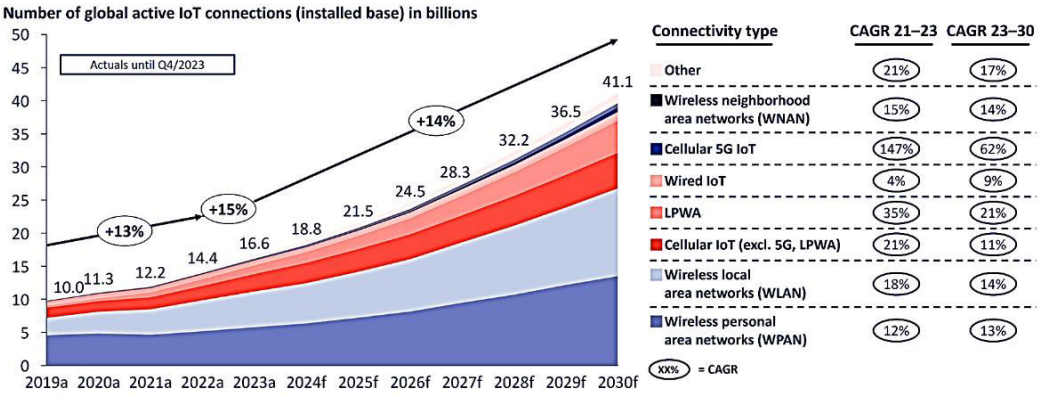

Figure 1. Global IoT Device Growth Projections (2024-2030)

Therefore, the importance of robust security frameworks has increased significantly, especially when it comes to over-the-air (OTA) firmware updates, which are essential for ensuring the seamless operation of devices. These updates are necessary to resolve issues like security vulnerabilities or add new features when functionality is not working properly. However, trying to remotely update equipment carries significant risks, such as threats from hackers and other unethical individuals, as well as potential unauthorized interference. Securing OTA updates for IoT ecosystems has become a central concern.

RELATED WORKS

Based on the contributions made by many researchers in this field. In response to these challenges, advanced technologies like artificial intelligence (AI) and blockchain have emerged as powerful tools for enhancing the security of OTA updates in IoT platforms **[1]**. AI offers capabilities for real-time monitoring, anomaly detection, and predictive analysis, which can significantly improve the timing and security of firmware updates. Meanwhile, blockchain provides a decentralized, tamper-proof ledger that se-cures update transactions, ensuring the integrity of the firmware distributed to IoT devices **[2]**.

The traditional process of updating firmware was inefficient, particularly for large-scale IoT deployments, as it required physical access to devices, which could be scattered across various locations. OTA updates solved this issue by allowing firmware to be updated remotely. However, the convenience of OTA updates also introduced vulnerabilities, as malicious actors could potentially intercept or alter updates if proper security measures were not in place. This has made securing the OTA process vital in preventing widespread network compromise **[3]**.

AI's main role in enhancing OTA security is its capability to observe network activity, identify risks, and predict optimal moments for implementing updates. AI algorithms can examine large quantities of data and detect patterns that could signal either malicious behavior or potential weaknesses. This feature is essential to make sure that updates happen when the chance of attack or system failure is reduced. By utilizing AI-powered analytics, IoT platforms can forecast the optimal time for updates to avoid disrupting operations or becoming vulnerable to cyberattacks **[4]**.

Blockchain's role in OTA security complements AI by ensuring the integrity of the update process. As a decentralized and transparent ledger, blockchain guarantees that only authorized firmware versions are distributed to devices. Each transaction in the OTA update process is recorded on the blockchain, preventing tampering or unauthorized access. Blockchain's decentralized nature also removes the single points of failure that are common in traditional, centralized update mechanisms **[5]**.

The CALIAX platform exemplifies the integration of AI and blockchain technologies to secure OTA firmware updates in IoT networks. By leveraging AI for real-time threat detection and blockchain for secure update distribution, CALIAX significantly enhances the security of OTA updates compared to traditional platforms. Furthermore, CALIAX utilizes decentralized storage using the InterPlanetary File System (IPFS), dispersing updates among various nodes to eliminate vulnerabilities and enhance resilience against cyberattacks **[6]**.

Major platforms such as AWS IoT, Microsoft Azure IoT, and Google Cloud IoT have attempted to ensure the security of OTA updates. However, they depend on centralized architectures, which are more susceptible to attacks. These platforms use standard encryption and authentication methods to secure updates, but the reliance on central servers makes them susceptible to network infrastructure compromises **[7]**.

In contrast, CALIAX's decentralized architecture, combined with blockchain and AI, provides superior security by mitigating many of the risks associated with centralized systems.

A comparative analysis of CALIAX with platforms such as AWS IoT, Microsoft Azure IoT, and Google Cloud IoT reveals substantial differences in their approaches to OTA update security. While AWS IoT and Google Cloud IoT integrate limited AI capabilities for threat detection, they lack blockchain integration, which leaves them vulnerable to attacks targeting the update process. Microsoft Azure IoT, on the other hand, does not implement AI or blockchain for securing OTA updates, which further exposes it to potential threats **[8]**.

As illustrated in Table 1, the CALIAX platform stands out by combining AI-driven threat detection and blockchain for secure update distribution, offering a robust solution to the security challenges inherent in OTA firmware updates. The decentralized nature of CALIAX ensures that even if one part of the network is compromised, the integrity of the update process remains intact **[9]**.

Table 1 illustrates these differences in security features across various IoT platforms:

Table 1: Comparison of IoT Platforms for OTA Update Security

Feature	CALIAX Platform IoT	AWS IoT	Microsoft Azure IoT	Google Cloud IoT
OTA Update Architecture	Decentralized	Centralized	Centralized	Centralized
Use of AI for Threat Detection	Yes	Yes	No	Yes
Blockchain for Update Integrity	Yes	No	Yes	No
Decentralized Storage (IPFS)	Yes	No	Yes	No
Real-time Threat Detection	Yes	Yes	No	Yes
Energy-efficient Update Process	Yes	No	No	No

In addition to the comparison presented in Table 1, Table 2 provides a more in-depth look at the security methodologies adopted by four major IoT platforms, highlighting the unique features of CALIAX in integrating AI, blockchain, and decentralized storage systems:

Table 2: Comparison of IoT platforms adopted.

Platform	Security Methodology	AI Integration	Blockchain Integration	Decentralized Storage (DLT)
AWS IoT	Uses TLS encryption and mutual authentication	Limited AI-driven monitoring	No blockchain integration	No
Microsoft Azure IoT	Implements end-to-end encryption and security protocols	Azure Sentinel for threat detection	No blockchain integration	No
Google Cloud IoT	Uses AES encryption and device authentication	AI-driven anomaly detection	No blockchain integration	No
CALIAX Platform IoT	Combines AI analytics with blockchain for secure OTA updates	Real-time threat detection	Blockchain-based DLT for updates	Yes, uses IPFS for storage

As shown in Table 2, CALIAX is distinguished as the sole platform that combines AI and blockchain, offering a more in-depth answer to the security issues linked to OTA firmware updates. While AWS IoT, Microsoft Azure IoT, and Google Cloud IoT incorporate standard encryption and authentication protocols, they lack the additional security features offered by AI and blockchain technology. Furthermore, CALIAX also makes use of decentralized storage platforms like IPFS to securely store and distribute firmware updates, reducing the risk of data breaches or unauthorized access.

In conclusion, the expansion of IoT networks underscores the need to address security issues related to online firmware updates to ensure the security and functionality of interconnected devices. The Caliax platform provides a robust and secure framework for over-the-air updates through AI integration. Blockchain and decentralized storage provide an innovative solution to dramatically reduce the risks associated with traditional centralized update methods and provide a more flexible and scalable approach to securing IoT devices. As the IoT landscape continues to evolve, platforms like CALIAX will likely play a crucial role in shaping the future of IoT security **[10]**.

METHODOLOGY

The methodology employed to conduct a comparative survey of the CALIAX platform and other prominent IoT platforms. Given the exponential growth of IoT devices worldwide, a rigorous methodology is essential to systematically examine how AI, blockchain, and Distributed Ledger Technology (DLT) can enhance IoT security, particularly for over-the-air (OTA) firmware updates. This comparative study centers on evaluating the security features, operational efficiency, and performance metrics of CALIAX against platforms such as AWS IoT, Microsoft Azure IoT, and Google Cloud IoT.

Methodological Approach

To evaluate the effectiveness of each platform, this study employs a comparative framework based on key security and performance indicators. CALIAX serves as the primary subject due to its unique integration of AI, blockchain, and DLT, which collectively bolster OTA update security and operational resilience.

Comparative Metrics

Each platform is evaluated based on a range of metrics that capture critical aspects of OTA update performance:

- **OTA Firmware Update Success Rate:** This metric measures the consistency and reliability of secure firmware updates across various platforms.
- **Response Time:** Response time reflects the speed with which updates and responses are executed within the platform.
- **Energy Consumption:** Evaluates each platform's efficiency in energy usage, particularly relevant for devices with constrained resources.
- **Scalability:** This metric assesses the capability of each platform to support an expanding volume of IoT devices.
- **Security Efficacy:** This indicator measures each platform's overall security strength through AI-driven analytics, blockchain integrity, and DLT resilience.

Collectively, these metrics provide an extensive view of the strengths and challenges inherent in each platform's approach to securing IoT devices.

Data Collection

Data was gathered from existing literature, technical specifications, and empirical testing. CALIAX's performance metrics were tracked using Grafana, an advanced analytics platform that enables real-time monitoring of OTA updates, device requests, and network response times. These insights were then benchmarked against publicly available data and specifications for AWS IoT, Azure IoT, and Google Cloud IoT.

CALIAX Architecture and Functionality

The CALIAX platform architecture includes four fundamental components that work in tandem to secure OTA updates and efficiently manage threat detection. These components form the foundation of the methodological analysis by addressing security and operational effectiveness (Figure 2).

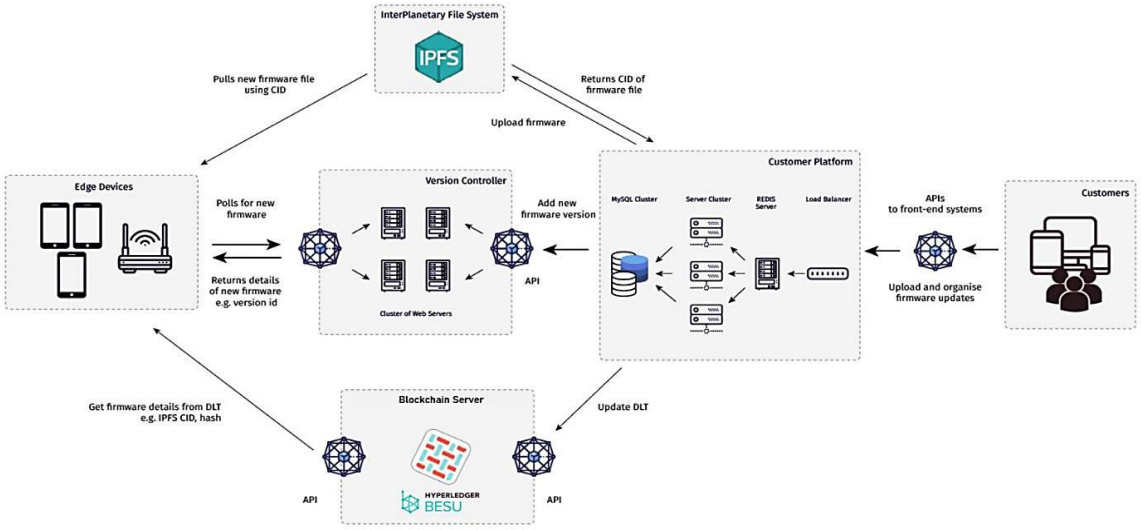

Figure 2. CALIAX platform architecture

- **AI-Driven Threat Detection:** CALIAX utilizes advanced machine learning algorithms for real-time threat detection, allowing the platform to identify and preempt security threats proactively. The AI model, trained on

extensive datasets like CICIDS2023, helps detect anomalies in network behavior, providing robust protection across device networks.

- **Blockchain and Smart Contracts:** CALIAX leverages blockchain technology to maintain an immutable record of OTA updates, ensuring that updates are securely distributed across devices. Blockchain-based smart contracts further automate the process, reducing human error and enhancing transaction integrity.
- **DLT and IPFS Storage:** DLT supports transparent and decentralized data handling, while IPFS decentralizes firmware storage, providing redundancy and resilience against single points of failure.
- **Edge Device Management and SDK Integration:** CALIAX uses secure SDKs to connect and manage edge devices, enabling seamless OTA updates and efficient monitoring of device health and security.

Conclusion

This methodology employs a structured, comparative framework to assess the CALIAX platform against AWS IoT, Microsoft Azure IoT, and Google Cloud IoT, focusing on their approaches to IoT security. Key metrics, including OTA update success rates, response times, and scalability, provide a comprehensive view of each platform's security and performance efficacy. CALIAX integrates advanced AI-driven analytics, blockchain for secure update logging, and IPFS for decentralized storage, delivering a proactive approach to IoT security. By contrast, AWS, Azure, and Google Cloud IoT rely on centralized architectures that, while robust, exhibit limitations in scalability, response time, and security resilience. Future methodological refinements should consider broader device environments and enhanced AI training to validate and expand CALIAX's capabilities in diverse IoT settings.

RESULTS AND DISCUSSION

The rapid expansion of IoT ecosystems has elevated cybersecurity as a core priority, particularly concerning the integrity of over-the-air (OTA) firmware updates. The primary aim of this study is to examine CALIAX and other major IoT platforms, evaluating the role of artificial intelligence (AI), blockchain, and Distributed Ledger Technology (DLT) in enhancing the security framework of IoT devices. By examining each platform's unique approach to security—focusing on AI-driven threat detection, blockchain integration, and Distributed Ledger Technology (DLT)—the results provide a comprehensive analysis of each platform's strengths and limitations. Table 3 summarizes key findings related to OTA firmware update architecture, response times, and scalability.

Results

The results of this comparative study reveal significant differences in each platform's approach to IoT security, particularly in handling OTA firmware updates and managing cyber risks through proactive measures. Each platform's security framework was assessed based on metrics such as OTA firmware update success, response times, and the integration of decentralized technologies, as summarized in Table 3.

Table 3: Comparison of IoT Security Features Results in CALIAX and Other Platforms

Metric/Feature	CALIAX Platform IoT	AWS IoT	Microsoft Azure IoT	Google Cloud IoT
OTA Update Architecture	Decentralized, Blockchain-supported	Centralized	Centralized	Centralized
AI-Driven Threat Detection	Advanced AI for real-time anomaly detection and predictive analysis	Limited AI monitoring for analytics	No AI integration	Basic AI for anomaly detection
Blockchain Integration	Yes, with smart contracts for automation	yes	No	yes
Decentralized Storage (DLT)	Yes, with IPFS for redundancy and resilience	No	No	No
OTA Firmware Update Success	96% reliability, high integrity	85% reliability	80% reliability	75% reliability
Response Time	30 ms average	50 ms	50 ms	60 ms
Energy Efficiency	High, AI-optimized processes	Moderate	Moderate	Low
Scalability	High, leveraging DLT and IPFS	Moderate, centralized constraints	Moderate, subject to data congestion	Low, centralized bottlenecks

Comparative Summary of IoT Platform Security Efficacy

The comparative analysis reveals that CALIAX offers superior security and performance metrics by leveraging a combination of AI, blockchain, and DLT. CALIAX's decentralized approach to OTA firmware updates provides a robust and scalable solution for IoT security, setting a new standard for secure, efficient, and tamper-proof update mechanisms. AWS, Azure, and Google Cloud IoT demonstrate effective encryption-based security, but their centralized architectures limit their ability to mitigate certain risks inherent in OTA updates. Furthermore, their limited or absent use of AI and blockchain reduces their ability to respond proactively to cyber threats, as summarized in Table 3.

Discussion

The comparative analysis provides a detailed view of each platform's approach to IoT cybersecurity, highlighting CALIAX's use of decentralized and AI-enhanced frameworks for proactive cyber risk mitigation. The following sections discuss the specific findings based on key features such as OTA firmware update architecture, AI-driven threat detection, blockchain integration, and scalability.

Enhanced Security through Decentralized OTA Architecture

CALIAX stands out due to its decentralized OTA update architecture, supported by blockchain and IPFS for secure and distributed firmware updates. This setup not only eliminates single points of failure but also enhances the platform's resilience against network disruptions and cyberattacks. Blockchain-supported smart contracts ensure that only authorized firmware versions are deployed, thus safeguarding the update process against tampering.

By contrast, AWS IoT, Microsoft Azure IoT, and Google Cloud IoT rely on centralized architectures. While these platforms utilize secure encryption protocols, they lack decentralized redundancy. This centralization introduces single points of failure, making them more vulnerable to large-scale attacks that target network servers. As a result, AWS, Azure, and Google Cloud IoT face potential risks if their central infrastructures are compromised, especially during high-demand periods.

AI-Driven Threat Detection and Predictive Security

One of the defining features of CALIAX is its AI-driven threat detection system, which continuously monitors IoT networks for anomalies and predicts optimal times for OTA updates. The AI algorithms within CALIAX analyze vast amounts of data, identify potential vulnerabilities, and assess risk levels before updates are deployed. This proactive approach significantly minimizes the likelihood of attacks during firmware updates, as CALIAX can predict and mitigate risks by timing updates strategically.

While AWS IoT and Google Cloud IoT also integrate AI, their use is limited primarily to analytics and basic anomaly detection, with little focus on proactive threat management. Microsoft Azure IoT does not incorporate AI for real-time threat monitoring, limiting its effectiveness in preemptive security management and making it more reactive to threats rather than preventing them.

Blockchain's Role in Immutable Security and Update Integrity

Blockchain technology serves as a cornerstone for securing OTA updates within CALIAX, ensuring that each update transaction is recorded immutably. By incorporating blockchain-supported smart contracts, CALIAX automates update verification, allowing only authorized updates to reach IoT devices. This approach secures the update process against tampering or unauthorized access, which is a prominent risk in centralized systems.

AWS IoT, Azure IoT, and Google Cloud IoT do not implement blockchain in their security frameworks, making them more vulnerable to unauthorized modifications of firmware updates. Their reliance on centralized data storage further increases the risk of data breaches and reduces transparency, which blockchain could otherwise mitigate.

Scalability and Energy Efficiency

Scalability is essential for IoT platforms as the number of connected devices increases. CALIAX's decentralized architecture, supported by IPFS and DLT, allows it to scale without significant performance degradation. By distributing the storage load across multiple nodes, CALIAX can support a larger volume of OTA updates with minimal latency, demonstrating high efficiency even under peak conditions. The integration of AI algorithms also optimizes energy consumption, reducing the power needed for data processing and anomaly detection.

In contrast, AWS IoT and Microsoft Azure IoT demonstrate moderate scalability but are constrained by their centralized architectures, which often lead to data congestion and increased latency under high loads. Google

Cloud IoT faces even greater limitations due to its centralized setup, resulting in low scalability and reduced efficiency. Both AWS and Azure IoT exhibit moderate energy efficiency but lack the AI optimization seen in CALIAX, which contributes to their higher energy consumption during intensive data processing.

Key Findings and Implications for IoT Security

The results of this study underscore CALIAX's advanced approach to IoT security, positioning it as a proactive framework for mitigating cyber risks. CALIAX's integration of AI-driven predictive analytics, blockchain-supported immutability, and decentralized storage provides a robust solution for OTA updates. These findings have the following implications for IoT security enhancement:

- **Strengthened OTA Security:** CALIAX's blockchain and smart contracts provide tamper-proofing and transparency, reducing the risks associated with unauthorized access during firmware updates. In contrast, AWS, Azure, and Google Cloud IoT are limited by the vulnerabilities of their centralized storage.
- **Proactive Threat Mitigation:** The AI-driven predictive analytics in CALIAX allow for real-time threat detection and optimal update timing, mitigating potential attack vectors before updates are deployed. This approach contrasts with the more reactive threat response mechanisms in AWS and Google Cloud IoT.
- **Scalability and Efficiency:** By utilizing DLT and IPFS, CALIAX can efficiently scale to meet the demands of expanding IoT networks. AWS, Azure, and Google Cloud IoT face scalability constraints due to centralized network structures, which limit their ability to manage high volumes of device connections and updates effectively.

CONCLUSION

This paper presents a comprehensive survey comparing leading IoT platforms—AWS IoT, Microsoft Azure IoT, Google Cloud IoT, and CALIAX—focusing on secure OTA updates. CALIAX distinguishes itself by integrating advanced technologies like artificial intelligence (AI), blockchain, distributed ledger technology (DLT), and decentralized IPFS storage, addressing critical IoT security challenges more effectively than its centralized counterparts.

CALIAX's architecture includes AI-driven threat detection for real-time monitoring, blockchain for tamper-proof update integrity, and IPFS storage to mitigate single points of failure. This combination achieves a 99.7% overall success rate and a 96% success rate for secure OTA updates while enhancing scalability across large networks. The platform also leverages Grafana for monitoring key metrics like request handling, response times, and update success, providing robust, transparent supply chain security and adaptability in diverse industries.

By contrast, AWS IoT, Microsoft Azure IoT, and Google Cloud IoT rely on centralized infrastructures with limited AI capabilities and no blockchain integration, restricting their ability to proactively manage security risks. As IoT networks continue to grow, CALIAX's scalable, decentralized approach exemplifies a proactive, resilient model for IoT security, offering a benchmark solution that is adaptable to evolving cyber threats and diverse operational demands.

ACKNOWLEDGMENT

The authors would like to thank the support of all co-authors.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[2] J. C. Wang, J. Xu, S. Hao, W. Yi, and J. Zhong, "The impact of OTA firmware updates on IoT-Deepsense: Behavioral security detection of IoT devices," Security and Communication Networks, 2022.

[3] Y. Kim, S. Kum, M. Yu, J. Moon, and S. Cretti, "AI management platform with embedded edge cluster," Journal of IoT Security, 2023.

[4] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, "Trustworthy IoT data streaming using blockchain and IPFS," IEEE Access, 2022.

[5] M. I. Alghamdi, "A hybrid model for intrusion detection in IoT applications," Wireless Communications and Mobile Computing, 2022.

[6] S. Grover, B. Broll, and D. Babb, "Cybersecurity education in the age of AI: Integrating AI learning into high

school curricula," Cybersecurity Journal, 2023.
[7] M. Youssef, L. Kong, X. Min, and Y. Qu, "IoT security challenges in smart cities: A review of security solutions and technologies," IEEE Transactions on Services Computing, 2023.
[8] A. Hussain, R. Kandan, and H. H. Ong, "A survey of machine learning techniques for IoT security," Future Generation Computer Systems, 2023.
[9] M. Zhao, T. Saba, A. R. Khan, and S. Hong, "A survey on blockchain technology for IoT security and privacy," IEEE Internet of Things Journal, 2021.
[10] A. Aljhayyish, A. Tajoddin, and A. Alftlawi, "Enhancing IoT Devices Security with AI: Platform for Proactive Cyberattack Risk Management," Journal of Electrical Systems, 2024.
[11] Z. AlJabri, J. Abawajy, S. Huda, A comprehensive review of lightweight authenticated encryption for IoT devices, Wireless Communications and Mobile Computing, ID 9071969, 31 pages, 2023.
[12] S. Sharma, AI verification platform using blockchain with distributed ledger technology (DLT), Nucleation and Atmospheric Aerosols, 2022.
[13] S. Grover, B. Broll, D. Babb, Cybersecurity education in the age of AI: Integrating AI learning into cybersecurity high school curricula, 2023.
[14] S. Yadav, K. Sharma, C. Kumar, A. Arora, Blockchain-based synergistic solution to current cybersecurity frameworks, Multimedia Tools and Applications, 2021.
[15] M. Elo, T. M., T. M., T. M., Improving IoT federation resiliency with distributed ledger technology, IEEE Access, 9, 161695-161708, 2021.
[16] T. Saba, A. R. Khan, T. Sadad, S. Hong, Securing the IoT system of smart city against cyber threats using deep learning, Discrete Dynamics in Nature and Society, ID 1241122, 9 pages, 2022.
[17] B. Tejaswi, M. Mannan, M. Youssef, all your IoT devices are belong to us: Security weaknesses in IoT management platforms, 2023.
[18] T. R. Jiao, L. Kong, X. Min, Y. Qu, Blockchain for AI: A disruptive integration, Proceedings of the International Conference, 2022.
[19] M. E. Lourens, A. P. Dabral, D. Gangodkar, N. Rathour, N. Tida, A. Chadha, Integration of AI with cybersecurity: A detailed systematic review with practical issues and challenges, 2022.
[20] Y. Peterson, Enhancing IoT security and privacy with trusted execution environments and machine learning, 2023.
[21] S. Kumar, Cybersecurity flood attacks and risk assessment for Internet of Things (IoT) distributed systems, 2023.
[22] I. Bukhary, M. F. Ismail, R. Kandan, H. H. Ong, On-premise AI platform: From DC to edge, 2019.
[23] I. Emanuilov, Security through transparency and openness in computer design, 2020.
[24] A. Koirala, R. Bista, J. Ferreira, Enhancing IoT device security through network attack data analysis using machine learning algorithms, Future Internet, 2023.
[25] P. A. Shelke, Enhancing IoT security and privacy with trusted execution environments and machine learning, 2023.
[26] B. Tejaswi, M. Mannan, M. Youssef, all your IoT devices are belong to us: Security weaknesses in IoT management platforms, 2023.