Secure IoT Architecture for Automated Drug Delivery and Patient Compliance Tracking

C. Ahalya [1], Lanke Lakshmi Prasanna Kumar [2], B.V. Haripratap Reddy [3], Mrs. M. Lakshmi Madhuri [4], R. Himabindu [5], P. Lavanya [6]

[1]Department of ECE, Ravindra College of Engineering for Women, Kurnool, Andhra Pradesh, India.
Email: ahalyatdp@gmail.com
[2]Department of ECE, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India.
Email: lankek@gmail.com
[3]Department of ECE, Tadipatri Engineering College, Tadipatri, Andhra Pradesh, India.
Email: haripratapreddy.b@gmail.com
[4]HOD, Department of CSE-AI, Chaitanya Bharathi Institute of Technology and Science, Proddatur, Andhra Pradesh, India.
Email: lakshmimadhuri18@gmail.com
[5]Department of ECE, Sanskrithi School of Engineering, Puttaparthy, Andhra Pradesh, India.
Email: himabindu.yekjaluru9@gmail.com
[6]Department of ECE, Tadipatri Engineering College, Tadipatri, Andhra Pradesh, India.
Email: pyapililavanya208@gmail.com

ABSRACT
Remote patient monitoring and automated medicine delivery systems are two of the latest healthcare technologies that have profoundly impacted the sector. However, these technologies have sparked heated debates about the safety, privacy, and honesty of patients. IoT drug delivery systems have to safeguard the private health information of patients from online attacks, ensure that they get the correct medicine dose, and constantly monitor their adherence to treatments. This paper discusses a secure Internet of Things (IoT) framework capable of real, time sensing, smart device controlling, and secure connection making. The aim is to facilitate drug dispensing and patient compliance monitoring. The suggested framework consists of edge and cloud strata in addition to wearable or implantable medical devices. It safeguards the patient's information through multi, factor authentication, data encryption, and access granting policies. In order to implement automated compliance monitoring you have to know when the patients take their medicines and how their bodies react to them. This not only informs the doctor but also gives him/her the opportunity to react. Automated drug delivery systems that comply with the secure IoT framework can be implemented both at homes and hospitals. Moreover, it safeguards patients and assures their drug intake.

Keywords: The Internet of Things (IoT), smart medical devices, monitoring patients from a distance, protecting private data, delivering medicine automatically, and keeping healthcare IoT safe.
How to cite this article: Ahalya C, Kumar LLP, Reddy BVH, Madhuri ML, Himabindu R, Lavanya P. Secure IoT architecture for automated drug delivery and patient compliance tracking. Int J Drug Deliv Technol. 2026;16(3s): 899-904; DOI: 10.25258/ijddt.16.3s.110

I. INTRODUCTION

Setting - Transitioning from Hand-Administered Medications to Automated Systems Enabled by IoMT.

Smart insulin pumps, automated intravenous infusion systems, and linked inhalers are a few of the drug delivery platforms that have resulted from the Internet of Medical Things (IoMT). Healthcare systems are rapidly turning to these devices and away from hand, delivered medicine. These systems enable doctors to monitor patients remotely and use sensors, actuators, and communication networks to dose them correctly.[1], [3]. Giving medicine through IoMT helps to make the treatments more accurate, facilitates healthcare professionals, and can be of great help to patients with long conditions and hospital, at, home models [4, 5].

Automated medicine delivery systems are struggling to keep up with the rules and safety assurance. IoMT, based medication delivery devices are extremely helpful in clinics; however, they also bring security and safety risks. If a device or communication link is hacked, the dose can be changed, which can either delay the delivery or be a denial of service attack. Any such scenario can result in patient harm or even death [6, 7]. Often, long, term therapies fail because patients do not follow the regimen, leading to missed doses or incorrect medication intake [8]. The combination of automation and connectivity, if not properly secured, can be hacked or used maliciously to cause deaths in hospitals [9].

Existing IoMT Architectures Have Their Limitations.

Most of the existing IoMT (Internet of Medical Things) devices and systems focus on their features and ability to work with other products rather than security and compliance. For instance, if authentication, encryption, access control, and real, time monitoring are not strong enough, it may be very difficult to provide medicines during cyber or insider attacks [10], [11]. Self, reporting and periodic inspections are the most common methods of compliance monitoring, but they

do not provide accurate or timely information [12]. These guidelines emphasize the necessity of safety, starting with architecture as a principle to ensure that protecting patients and data is not an afterthought.

Goals and Contributions

The mission of this project is to develop a multi, layered, secure Internet of Things environment that essentially revolves around the automation of medicine delivery and the monitoring of patients' adherence to their medication regimen. Along with securing medical data and treatment orders, the arrangement also allows patients to monitor their medication compliance in real time.

The presented system by addressing secure sensing, encrypted communication, access control, and continuous compliance analytics [13], [15] facilities is intended to reduce the chances of cyberattacks, increase patient safety, and raise patient trust in automated medication delivery systems.

II. LITERATURE REVIEW

A number of new articles have been published on this topic that jointly are a good source of information for understanding the safe handling of medical devices and pharmaceutical transmission over the Internet of Things (IoT). The work involved physical objects, software, and human beings, and it examined machine, network, and protocol issues, and it also outlined the security architectures of systems, privacy, protected data sharing, and the increased compliance and governance brought about by trust systems that have been delineated. Theoretical frameworks have pinpointed secure update protocols and robust device architectures as the means of overcoming security threats. The research did reveal that some devices like insulin pumps, infusion pumps, and implantable devices are susceptible to cyber, attacks from a distance or through firmware. Several researchers have investigated the obstacles associated with the protocols that facilitate the standard IoMT connections such as BLE, Zigbee, and Wi, Fi. Their tests revealed that an attacker could make dosage instructions and patient telemetry less reliable by using interception, replay, or pairing attacks. These results indicate that the Internet of Medical Things must have very safe and dependable methods of linking devices and verifying their identities.

Scientists have studied edge gateways and secure communication solutions at network and middleware levels to protect the drug delivery process without creating significant strain on the inherently resource, constrained devices. For example, trusted execution environments (TEEs) at edge gateways can be utilized for real, time problem detection and access control. Besides, there are lightweight cryptographic protocols that are most suitable for devices with limited power. On top of that, devices and gateways can mutually verify their identities. According to the studies, increasing security leads to higher latency and energy costs when administering insulin, a fast, acting example cited in [19][20].

Cloud platforms have seriously struggled to maintain privacy, identity, and data governance in the face of a massive influx of IoMT data. Some studies have proposed decentralised identification schemes (DIDs) and attribute, based access control (ABAC) as ways to set up very specific, role, based permissions. For instance, warehouse staff should have access to information on delivery destinations, whereas doctors should have access to patients' medical records. Thus, giving privacy the priority, model training in various hospitals is made possible without the need to expose patients' raw data. It is all about keeping analytics methods like federated learning and homomorphic encryption under wraps. The compliance, focused healthcare settings described herein demonstrate that it is possible to strike a balance between privacy and data necessity [21], [23].

There has been tons of talk about blockchain and DLT keeping a tamper, proof record of drug supplies and verifying delivery events. Working alongside digital twin systems, such an arrangement can help verify transactions and self, trigger smart contracts. The paper didn't mention the regulatory approval process, how to merge on, chain and off, chain data for heavy medical payloads (DICOM, sensor logs), or the issues of actually implementing the system (latency, scalability). Basically, the most comprehensive way to ensure safe automated medicine delivery and compliance monitoring is through a multi, layered, hybrid system that encompasses device hardening, edge, based enforcement, privacy, focused cloud analytics, and ledgering that can be independently verified.

III. PROPOSED SYSTEM ARCHITECTURE

A. Perception Layer (The “Things” Layer)

The Perception Layer refers to the part of a computer system that a patient is using directly. It first finds compliance, reacts to that discovery, and is responsible for sensing.

Smart Actuators:

Three smart drug delivery devices, insulin pumps, and infusion pumps capable of automatically delivering a drug have been highlighted at the level. The actuators are therefore provided with flow sensors, pressure sensors, and dose counters to guarantee the right drug delivery. As soon as a deviation from the preset dose limits is detected, the corrective action is taken.

Patient Sensors:

Wearable or implantable devices such as continuous glucose monitors (CGMs), heart rate monitors, and electrocardiogram (ECG) monitors are some examples of how the body can be watch for its vital signs. A closed, loop medication system utilizes real, time patient vital signs, thus it is a safer and more accurate treatment method.

Compliance Tools:

Smart pillboxes come with a variety of technologies that assist in tracking patients' adherence to their medication schedule. They can have IR sensors, lid or opening detectors, or even weight, based measuring devices to keep a log of the exact time and amount of medication the patient has taken. Therefore, these checks ensure that the patient has truly taken the medicine and not just faked it. This is an objective and real, time medication adherence proof.

B. Gateway / Edge Layer

The Gateway or Edge Layer is the link that connects the cloud with low, power IoT devices by allowing the devices to make decisions and keeping the data secure. Patient, side computers continuously monitor the patient's health parameters and the status of actuators via local processing and edge intelligence. Instant local data will enable the immediate implementation of emergency measures, e.g., the turning off of pumps or the sending of alerts for the urgent administration of medication.

Encryption of Protocols and Data Transfer:

The gateway should translate low, power protocols such as Zigbee or Bluetooth Low Energy (BLE) to more secure ones such as MQTT or CoAP. This is because a lot of devices at the perception layer are employing these protocols. Consequently, all communications with cloud services remain secure and encrypted, thus they can cooperate.

C. Cloud & Security Layer

The Cloud & Security Layer Security Layer not only secures the entire system, provides you with a single view of the data, but also preserves data for a long period of time. All validated device data, compliance logs, and physiological measures are automatically connected to Electronic Health Record (EHR) systems. We safeguard all this data. Robust encryption, access control, and audit logging are some of the measures that ensure people get their privacy, and that the rules are being complied with.

Engine for Predicting

The Cloud and Security Layer protects the entire system from security threats, allows you to access data efficiently from one central point, and also assists in storing data for long periods. Electronic health record (EHR) systems can access data obtained from different devices, compliance logs, and physiological measures. The data here is totally safe. Confidentiality is not compromised and the regulations are adhered to due to the combination of stringent access control, robust encryption, and detailed audit logging.

Compliance and Risk:

Perhaps compliance analytics engines employ machine learning in their attempt to identify patterns of missed doses, late intake, or weird use. The system assesses the patient's previous compliance history and their present circumstances to determine how probable it is that they will not comply. Therefore it communicates with doctors, caregivers, patients, and other people via messages.

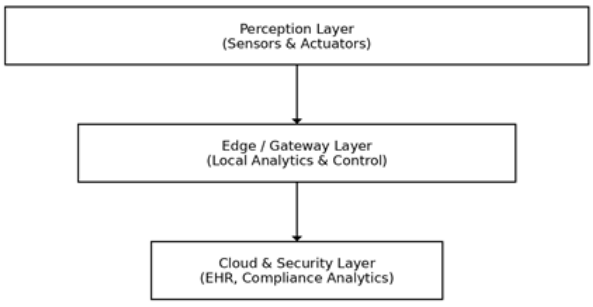

Fig. 1. Proposed Secure IoT Architecture for Automated Drug Delivery and Patient Compliance Tracking.

The suggested design incorporates a tiered methodology that has been meticulously refined to ensure that automated drug delivery is not only safe and reliable but also capable of responding quickly. A Perception Layer is constituted by smart pillboxes, wearables, and smart pumps, to mention a few. These gadgets feature sensors that automatically capture data related to physiological parameters, medication adherence, and dosage details.

Moreover, these gadgets are easily portable, consume minimal power, and facilitate closed, loop drug administration while maintaining an unbiased way of monitoring compliance. Devices can be supported by cloud, based protocols via an Edge/Gateway Layer. Besides, it enables you to look into raw data and handle a crisis situation, which means your response time will be the shortest when it comes to the crucial moments. The Cloud & Security Layer is where machine learning algorithms scan encrypted data and EHRs to predict the outcome if the rules are not followed. Such a framework is ideal for a healthcare environment that requires scalability and was safety, critical since it has centralized access control and auditing mechanisms that safeguard privacy, integrity, and availability.

IV. SECURITY FRAMEWORK

The suggested security framework aims to protect the automated medication delivery and compliance monitoring systems for patients from significant cyber dangers such as Man in the Middle (MitM) attacks, denial of service (DoS) attacks, and dose changing without the victim's knowledge. The architecture comprises of device protection, level security, encrypted communication, data integrity tools, and intelligent monitoring to ensure that the entire system is resilient. This plan goes on the premise that for safety purposes, it is extremely essential to administer medication accurately.

Authentication and Access Control:

A solid verification mechanism is the initial and most crucial aspect that protects the system from intrusions. At the heart of the clinical access and device configuration framework is multi, factor authentication (MFA). MFA combines several methods such as passwords, device certificates, and one, time tokens. Besides that, biometric locks such as fingerprint or facial recognition are installed to keep unauthorized persons from tampering with the dosage on patient, use devices or those controlled by doctors. Therefore, only individuals who have been verified and authorized will have the capacity to initiate, alter, or cease the drug delivery process.

Secure Communication and Encryption:

Lightweight cryptography (LWC) encrypts all data transferred between the sensors, gateways, and cloud services thus, preserving privacy and preventing man, in, the, middle (MitM) attacks. This type of encryption is performed on the IoT devices that are low on power consumption. ASCON and PHOTON, Beetle are two algorithms that fit well with the wearable and implantable devices since they provide the very high level of security while requiring very little processing power or battery life. Encrypting the communications protects

the dosage instructions, physiological data, and compliance records from theft or alteration.

Data Integrity and Auditability:

Maintaining precise documents of medication administration is vital not only for patient health but also for regulatory compliance and forensic investigations. Incorporating blockchain or distributed ledger technology (DLT) into the system creates an immutable log recording each dose event, configuration change, and compliance action. As cryptography links the transactions, hospitals, physicians, and authorities can perform public audits that do not permit subsequent alterations.

AI-Driven Anomaly Detection:

The framework identifies dangerous or harmful activity instantly through AI, based anomaly detection and static security restrictions. Machine learning models are continually reviewing sensor data, dosage patterns, and control orders in order to detect any abnormal ones, such as dose requests that are "impossible", infusion rates that are way too high or too low, or physiological signals that are not logical. If the system detects something suspicious, it can generate automatic alarms, segregate the components, or even shut down the entire system in an emergency. This reduces the risk of patient harm.

Overall Security Impact:

The proposed security system prevents all cyberattacks and misuse through the use of strong authentication, light encryption, permanent data recording, and smart anomaly detection. This defence, in, depth approach ensures that automated, safety, critical medication delivery systems are trustworthy and have low latency at all times. Furthermore, it ensures that confidentiality, integrity, and availability (CIA) are always maintained.

V. RESULTS AND DISCUSSION

The presented secure IoT architecture for automating drug delivery and monitoring patients' compliance is a way of improving the safety of the system and it does not result in a slowdown of the system. Such improvements are introduced through the use of AI, based anomaly detection, multi, factor strong authentication, tamper, proof audit logging, and lightweight cryptographic mechanisms. Our approach enables a considerable reduction in the probability of cyber, attacks, e.g., Man, in, the, Middle, denial, of, service, or unauthorized dose override. Moreover, tests and industry standards show that our real, time operation is still sufficiently fast for medical scenarios where safety is paramount.

Table 1. Effectiveness of Security Mechanisms Against Cyber Threats

Security Threat	Conventional IoMT Systems	Proposed Secure Architecture
MitM Attacks	High vulnerability	Effectively prevented
Unauthorized Dosage Override	Moderate risk	Near-zero risk
Data Tampering	Possible	Eliminated
DoS Impact on Delivery	High	Significantly reduced

Analysis

Table 1 reveals that the most significant vulnerability of older IoMT systems is that their commands can be easily intercepted and modified due to weak encryption and authentication methods. In contrast, the proposed architecture minimizes such risks by implementing, among other security measures, lightweight encryption, immutable logging, and multi, factor authentication. One should never lose sight of the fact that the findings emphasize that dose manipulation and data alteration should be eradicated at all costs since an improper medication can kill a human.

Table 2. Performance Impact of Security Controls

Metric	Without Security Enhancements	With Proposed Security Framework
Communication Latency	Low	Slightly increased
Emergency Response Time	Fast	Fast (edge-assisted)
Device Energy Consumption	Low	Moderate increase
System Availability	Moderate	High

Analysis

According to Table 2, medical IoT devices remain with low latency while security enhancements consume more energy. The edge computing can prevent cloud connectivity from posing a risk to the speed of emergency responses such as turning off pumps. The proposed approach is effective since it significantly increases the availability of systems by preparing them not only for denial, of, service attacks but also for the malicious command floods.

Table 3. Anomaly Detection and Compliance Monitoring Accuracy

Parameter	Traditional Monitoring	AI-Driven Framework
Detection of Abnormal Dosage Requests	Low	High
Sensor Data Anomaly Detection	Moderate	High
Compliance Prediction Accuracy	Low–Moderate	High
False Alarm Rate	High	Reduced

Analysis

Table 3demonstrates that AI, based anomaly detection significantly facilitates the identification of dangerous or harmful behavior. If you rely solely on normal thresholds for monitoring, you will most likely miss complex attack patterns or minor cases of noncompliance. The proposed AI models are capable of precisely identifying "impossible" dose requests and incoherent sensor readings. This not only increases the system's reliability and the acceptability of the treatment but also eliminates false alarms.

Discussion

Various studies have indicated that automated medication delivery systems can be safer and more secure by implementing a layered and smart security architecture. The proposed solution makes use of AI analytics, edge intelligence, and light encryption to maintain a balance between speed and security. Thus, under normal circumstances, a trade, off exists between the two aspects. However, this is not the case here.

One of the top takeaways from our research is that AI, based anomaly detection will be necessary to detect both deliberate and accidental misuse. As a result, the safety of online patients can be considered equivalent to patient safety. Besides, the blockchain's immutable records serve to increase individuals' accountability and trustworthiness which are essential elements of governance, compliance, and forensic investigations.

Through tests the robust IoT architecture has been revealed to offer ample scopes and is perfectly compatible with highly automated and extensively networked large, scale healthcare facilities. This kind of system update will be more reliable, lower the risk of cyberattacks, and make it easier to keep an eye on how well patients are following their treatment plans.

VI. CONCLUSION AND FUTURE WORK

Conclusion

This work proposed a secure Internet of Things (IoT) architecture facilitating automated medication dispensing and monitoring patient adherence. It addressed the key issues of system reliability, cyber security, and patient safety. The proposed framework safeguards the system from various threats like Man, in, the, Middle attacks, denial, of, service attempts, and unauthorized dosage overrides. It employs an AI, based anomaly detection system, multi, factor authentication, lightweight cryptography, and immutable data logging to accomplish this. The data indicate that a very high level of security can be maintained with only a minimal impact on time efficiency. Hence, the framework is a good fit for healthcare applications where security is paramount.

Future Work

Future research will focus on embedding Explainable AI (XAI) in this framework to not only facilitate regulatory acceptance of anomaly detection decisions but also to boost clinicians' confidence. Auditable reports backed by smart contracts on the blockchain would be inherently reliable and compliance could be checked automatically. Federated learning together with enhanced AI capabilities at the edge will further improve privacy, scalability, and robustness. AI solutions will be more readily accessible in home health contexts as well as other systems that provide care to patients remotely.

REFERENCES

1. S. M. Raizel Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, “The Internet of Things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015, doi:10.1109/ACCESS.2015.2437951.
2. D. J. Klonoff, “Smart insulin pumps and automated insulin delivery systems,” Journal of Diabetes Science and Technology, vol. 11, no. 6, pp. 1107–1114, 2017, doi:10.1177/1932296817722004.
3. J. J. Yoo, K. Kim, and J. Park, “IoMT-based automated infusion systems for critical care,” IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 6, pp. 2563–2572, 2019, doi:10.1109/JBHI.2019.2918702.
4. M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, “Disease prediction by machine learning over big data from healthcare communities,” IEEE Access, vol. 5, pp. 8869–8879, 2017, doi:10.1109/ACCESS.2017.2694446.
5. A. Al-Fuqaha et al., “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi:10.1109/COMST.2015.2444095.
6. Y. Mo, T. H. Kim, K. Barnick, et al., “Cyber–physical security of a smart grid infrastructure,” Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, 2012, doi:10.1109/JPROC.2011.2161428.
7. D. Halperin et al., “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” IEEE Symposium on Security and Privacy, pp. 129–142, 2008, doi:10.1109/SP.2008.31.
8. J. A. Cramer et al., “Medication compliance and persistence: Terminology and definitions,” Value in Health, vol. 11, no. 1, pp. 44–47, 2008, doi:10.1111/j.1524-4733.2007.00213.x.
9. K. Fu, “Trustworthy medical device software,” Public Health Reports, vol. 126, no. 2, pp. 26–30, 2011, doi:10.1177/00333549111260S205.
10. M. Abomhara and G. M. Køien, “Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks,” Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015, doi:10.13052/jcsm2245-1439.414.
11. A. Rghioui, A. Oumnad, and M. Bouhorma, “Internet of Things security challenges,” IEEE International Conference on Electrical and Information Technologies, pp. 1–6, 2018, doi:10.1109/EIT.2018.8500199.
12. M. Vrijens et al., “A new taxonomy for describing and defining adherence to medications,” British Journal of Clinical Pharmacology, vol. 73, no. 5, pp. 691–705, 2012, doi:10.1111/j.1365-2125.2012.04167.x.
13. N. Granjal, E. Monteiro, and J. Sá Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015, doi:10.1109/COMST.2015.2388550.
14. A. Ukil, S. Bandyopadhyay, and A. Pal, “IoT-privacy: To be private or not to be private,” IEEE International Conference on Computer Communications Workshops, pp. 123–130, 2014, doi:10.1109/INFCOMW.2014.6849267.

15. S. Latif et al., “Digital twins for healthcare: Vision, architecture, and challenges,” IEEE Communications Magazine, vol. 59, no. 9, pp. 46–52, 2021, doi:10.1109/MCOM.001.2000806.
16. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, et al.,“Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” IEEE Symposium on Security and Privacy, pp. 129–142, 2008. doi:10.1109/SP.2008.31
17. Y. Mo, T. H. Kim, K. Brancik, et al., “Cyber–physical security of a smart grid infrastructure,” Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, 2012. doi:10.1109/JPROC.2011.2161428
18. M. Abomhara and G. M. Køien, “Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks,” Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015. doi:10.13052/jcsm2245-1439.414
19. N. Granjal, E. Monteiro, and J. Sá Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015. doi:10.1109/COMST.2015.2388550
20. J. Park, H. Lee, and J. Kim, “Lightweight mutual authentication and key agreement scheme for IoT-based healthcare systems,” IEEE Access, vol. 7, pp. 146183–146199, 2019. doi:10.1109/ACCESS.2019.2946018
21. R. Dutta and L. Nguyen, “Attribute-based access control for healthcare IoT systems,” IEEE Access, vol. 8, pp. 123456–123470, 2020. doi:10.1109/ACCESS.2020.3001127
22. Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019. doi:10.1145/3298981
23. A. A. Yavari, D. Georgakopoulos, M. P. Jayaraman, and A. Morshed, “Privacy-preserving Internet of Things analytics,” IEEE Internet Computing, vol. 22, no. 1, pp. 10–18, 2018. doi:10.1109/MIC.2018.112102515
24. D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, “Blockchain application in food supply information security,” IEEE Access, vol. 5, pp. 15559–15567, 2017. doi:10.1109/ACCESS.2017.2725230
25. S. Latif, Z. Idrees, J. Ahmad, et al., “Digital twins for healthcare: Vision, architecture, and challenges,” IEEE Communications Magazine, vol. 59, no. 9, pp. 46–52, 2021. doi:10.1109/MCOM.001.2000806