A Theoretical Study of IoT Data Security Through the Integration of Machine Learning, Artificial Intelligence and Blockchain Technology

Ms. Priyanka S. Yengantwar (Chandawar)[#1], Dr Ujwal A. Lanjewar[#2], Dr S. J. Sharma[#3]

[#1]*Assistant Professor, Department of Computer Science, Dr. S. C. Gulhane Prerna College of Commerce, Science, and Arts, Nagpur, MS. (India)*

[#2]*Professor, & Principal, Department of Computer Science, Binzani Mahila Mahavidyalaya, Nagpur, MS. (India)*

[#3]*Head of Department of Electronics & Computer Science Rashtrasant Tukadoji Maharaj Nagpur University, Research Centre, Nagpur, MS. (India)*

Abstract The **Internet of Things (IoT) is one of the most rapidly used technologies in the last decade in various applications. The smart devices are connected wireless or wired for communication, processing, computing, and monitoring different real-time operations. The devices are heterogeneous with low memory and less processing power. The implementation of IoT applications comes with challenges like security and privacy because traditional-based security protocols do not match IoT devices. In this paper, in the first section, the author describes an overview of the IoT technology. The primary security issues like confidentiality, Integrity, Availability, and layer-wise issues are identified. Then the author studied the three primary technologies for addressing the security issue in IoT that is Machine learning (ML), Artificial intelligence (AI), and Blockchain. In the end, security issues were solved by the integration of ML, AI, and Blockchain. This paper proposes a comprehensive approach to fortify IoT security by harnessing the synergy of Machine Learning (ML), Artificial Intelligence (AI), and Blockchain technology.**

Keywords- Internet of Things, Machine learning, Artificial intelligence and Blockchain

I. INTRODUCTION

The Internet of Things (IoT) is a network of smart devices that share information over the Internet. The smart devices are used to deploy in a different environment to fetch the information, and some events are triggered. As per CISCO's estimate, the active IoT devices will be 50 billion at the end of 2020. The number of IoT devices is rapidly increasing day by day. The data generated by the IoT devices is huge. In traditional IoT, architecture there are three types of layers available namely physical, network, and application layers. In the physical layer, devices are embedded with technology in which they sense the atmosphere and are also able to connect IoT devices. For example, in smart hospitals, patients can monitor an emergency through sensors and corresponding computing devices. As we know sensors and IoT devices have less computation power and are heterogeneous. Implementation of IoT leads to lots of challenges such as standardization, interoperability, data storage, processing, trust management, identity, confidentiality, integrity, availability, security, and privacy. Later on, these challenges related to surveys work on IoT security.

The main objective of this paper is to find out the security and privacy challenges that are available in IoT applications. It has also identified some unfold technology that can address security issues present in the system.

A. IoT Infrastructure

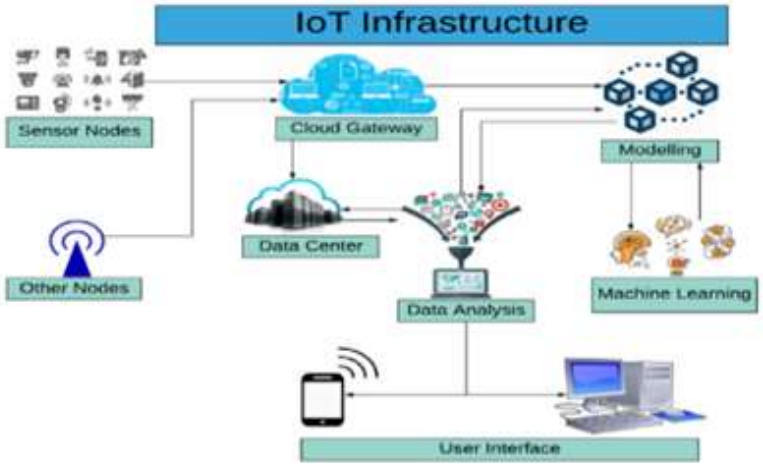

Figure 1. Internet of Things Infrastructure

IoT application contains several smart devices that collect, process, compute, and communicate with different smart devices. It has three layers physical, network, and application layer. As shown in Fig. 1 IoT infrastructure consists of sensors integrated with some emerging technologies, which are based on either IoT-cloud or IoT-fog-cloud. The architecture of IoT may be centralized, distributed, or decentralized structure. The most challenging issue in the IoT application is processing and computing in real time. We know that cloud computing provides vast storage and assures security to the data. But now most of the real-time monitoring IoT application demands processing and computing at the edge of the network. When it is done at the edge using fog nodes, it becomes more vulnerable to attackers. During analytic data. an advanced technique like Machine Learning is used to make the IoT system more intelligent and independent in making a decision. The different smart devices are connected to make an application using some standard protocols. The data interoperability [1] in IoT works using an intelligent algorithm.

Table 1 shows four layers in IoT infrastructure, their standard protocol name, and possible security attacks in respective layers.

Table 1

Protocols and attacks on the IoT layer

Layer	**Protocol Name**	**Possible security attack**
Application	MQTT, CoAP, REST, AMQP	Repudiation Attack, DDoS Attack, HTTP Flood Attack, SQL Injection Attack, Cross-Site Scripting, Parameter Tampering, Slowloris Attack
Transport	TCP, UDP, DCCP, SCTP, RSVP, QUIC	SYN Flood, Smruf Attack, Injection Attack, Opt-ack Attack
Network	CLNS, DDP, EIGRP, ICMP, IGMP, IPsec, IPv4, IPv6, OSPF, RIM	IP Address Spoofing, DoS Attack, Black Hole Attack, Worm Hole Attack, Consumption Attack
Physical	DSL, ISDN, IDA, USB, Bluetooth, CAN, Ethernet	Access Control Attack, Physical Damage or Destruction, Disconnection of Physical Links

B. Machine Learning and Artificial Intelligence: Machine Learning and Artificial Intelligence offer their expertise to the identification of anomalous behaviors, predictive threat analytics, and real-time monitoring. These technologies enable the creation of dynamic behavioral patterns, facilitating the prompt detection of deviations from the norm. AI-driven authentication methods, including biometric recognition and natural language processing, bolster access control mechanisms, thereby enhancing overall IoT device security.

C. Blockchain technology: Blockchain technology, known for its immutable and decentralized nature, forms a robust foundation for the proposed security paradigm. By immutably storing IoT data and

transactional records, Blockchain ensures data integrity and offers an auditable trail of events. Additionally, the introduction of autonomous identities and smart contracts empowers devices to establish their authenticity and autonomously execute predefined security protocols.

II. LITERATURE REVIEW

Reference Paper	Year	Research Work
Jing et al. [2]	**2014**	This paper stated the security issues of the three layers of IoT and its corresponding solutions.
Ngu et al. [3]	**2016**	The author described the IoT middleware-based architecture adaptability and security issues in the IoT system.
Mosenia et al. [4]	**2016**	The author explained the reference model and security threads present on the edge of the network and it also addresses the possible solutions.
Lin et al. [5]	**2017**	This paper describes the IoT and Cyber-Physical System (CPS) integration with the survey of the security and privacy issues.
Yang et al. [6]	**2017**	In this survey, the four-layer computing integration based on IOT application is explained in this survey paper.
Alaba et al. [7]	**2017**	In this paper, the authors investigate the state of the art of security and privacy issues on IoT applications and systems. It also reviewed the authentication protocol in the IT system and challenging security issues in the four-layer architecture based on the IoT application.
Grammatikis et al. [8]	**2018**	In this paper, the author provides a detailed study of the IOT security layer-wise. The suitable countermeasures and the potential threats model are discussed in detail.
Das et al. [9]	**2018**	In this paper, the author investigates the security and threat model in IT applications. This paper also describes some of the issues in IT system like authentication, trust, management, and access control, and some solution approach was also addressed.
Di Martino et al .[10]	**2018**	In this paper, the different standard architectures of IoT systems and the current solution approach in terms of security and interoperability are explained.
Hassija et al. [11]	**2019**	In this paper, the author reviewed the security and three in IoT application, whereas different solution approach using machine learning, fog computing, edge computing, and Blockchain was proposed.
Proposed Paper	**2023**	In this paper, the author initially identified the necessary infrastructure protocol of the IoT system. Then the security issues are identified in the IoT model. Some emerging techniques that can be used to solve the security issues in IoT have been identified. After a rigorous survey, the author found that machine learning, Blockchain, and artificial intelligence are the current solution approaches to solving the security issues in IoT.

III. SECURITY ISSUE ADDRESS USING MACHINE LEARNING (ML) AND ARTIFICIAL INTELLIGENCE (AI)

Machine learning is a technique to perform intelligent computation. The model always needs to be designed and tested using various learning methods. For example, predicting a fire in a kitchen or any industrial area and alarm to prevent the fire. This could be possible if machine learning technologies are used in IoT applications. Also, it needs to address the security issue present in the IoT system to make the system tamper-proof. Whereas AI could help IoT huge volumes, unstructured data, and heterogeneous data to compute in real-time, which makes the system realistic. IoT security with Machine Learning (ML) and Artificial Intelligence (AI). Here's how each technology can contribute:

A. *Anomaly Detection:* ML and AI algorithms can analyze patterns of normal behavior for IoT devices and networks. Any deviations from these patterns can be flagged as potential security breaches, enabling quick responses to mitigate risks.

B. *Behavioral Analysis:* By continuously learning and adapting to device behavior, ML algorithms can identify evolving threats and adapt security protocols accordingly.

C. *Predictive Analytics:* ML can predict potential security threats based on historical data, helping organizations take proactive measures to prevent breaches.

D. *Real-time Monitoring:* AI-driven systems can monitor IoT networks in real-time, detecting and responding to security incidents as they occur.

E. *Advanced Authentication:* AI can power advanced authentication mechanisms like biometric recognition, voice recognition, or facial recognition for access control.

a. *Natural Language Processing (NLP):* NLP can be used to analyze and understand the context of communication between IoT devices, identifying suspicious or unauthorized interactions.

IV. SECURITY ISSUE ADDRESS USING BLOCKCHAIN TECHNOLOGY

Blockchain technology is a decentralized and distributed network where each block is connected to others in some way. The message is broadcast in the Blockchain network. A block consists of lots of trusted transactions and their associated attributes. Following are the contributions of AI in IoT Security.

A. *Immutable Data Storage:* Blockchain's decentralized and tamper-proof nature ensures that data collected from IoT devices remains secure and unalterable, maintaining data integrity.

B. *Secure Transactions:* Blockchain facilitates secure and verifiable transactions between IoT devices, reducing the risk of unauthorized access or data manipulation.

C. *Decentralized Identity Management:* Blockchain can enable self-sovereign identities for IoT devices, enhancing authentication and access control while reducing the risk of identity theft.

D. *Audit Trails:* All transactions and changes are recorded on the blockchain, creating an audit trail that helps trace the origin of security breaches and unauthorized activities.

E. *Smart Contracts:* Smart contracts can automate security protocols and responses. For instance, if an anomaly is detected, a smart contract can trigger predefined actions to isolate or shut down compromised devices.

F. *Consensus Mechanisms:* Blockchain's consensus algorithms ensure that changes to the system are agreed upon by a majority of participants, preventing unauthorized modifications.

V. INTEGRATION OF TECHNOLOGIES MACHINE LEARNING WITH ARTIFICIAL INTELLIGENCE

ML and AI can enhance the accuracy of anomaly detection, behavioral analysis, and predictive analytics in the context of IoT security. Blockchain can provide a secure and transparent data storage layer for ML and AI models, ensuring the integrity of algorithms and results. Combined, these

technologies can create a holistic security framework where IoT data is collected securely, analyzed for threats, and stored in a tamper-proof manner.

VI. CHALLENGES AND CONSIDERATIONS

A. *Resource Constraints:* IoT devices often have limited computational resources. ML and AI algorithms must be optimized to run efficiently on these devices.

B. *Scalability:* As IoT networks grow, ensuring that ML, AI, and blockchain solutions can scale to handle the increased load is essential.

C. *Data Privacy:* While ML and AI require substantial data for training, data privacy concerns must be addressed. Blockchain's privacy features (e.g., zero-knowledge proofs) can help in this aspect.

D. *Regulatory Compliance:* Depending on the industry and location, there may be regulations governing the use of AI, ML, and blockchain in IoT security. Compliance is crucial to avoid legal issues.

Incorporating ML, AI, and blockchain into IoT security strategies can create a robust and adaptive defense against evolving threats. However, implementation requires careful planning, collaboration between experts in various domains, and ongoing monitoring to ensure the system's effectiveness and resilience.

CONCLUSION

The Internet of Things (IoT) in recent times attracted lots of attention to the research community as well as the industry sector. The IoT devices are manufactured in large numbers which already cross the total world population. These smart devices are connected to different applications for capturing information from the environment. The IoT devices are resource-constrained, so devices are vulnerable to attackers. Security and privacy issues are important for IoT applications.

In this paper, the authors first study in-depth the IoT infrastructure also various security challenges that exist in it. Secondly, the authors have found that some research has already been done on various technologies like Machine learning, Artificial intelligence, and Blockchain technology, which are capable of addressing the existing security issues. So, in detail, a study has been made on three technologies machine learning, artificial intelligence, and Blockchain technology, and their integration with IoT. Security is an important issue that needs to be addressed. In this paper, the authors outline emerging technologies like ML, AI, and Blockchain integrated with IoT to make the system more secure.

REFERENCES

[1] Nawaratne, Rashmika, et al. "Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments." Future Generation Computer Systems, vol. 86, 2018, pp. 421-432.

[2] Jing, Qi, et al. "Security of the Internet of Things: Perspectives and challenges." Wireless Networks, vol. 20, 2014, pp. 2481-2501.

[3] Ngu, H. Anne, et al. "IoT middleware: A survey on issues and enabling technologies." IEEE Internet of Things Journal vol 4, no.1 2016, pp.1-20.

[4] Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of the security of internet-of-things." IEEE Transactions on Emerging Topics in Computing vol 5, no.4, 2016, pp. 586-602.

[5] Lin, Jie, et al. "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal, vol.4, no.5,2017, pp. 1125-1142.

[6] Yang, Yuchen, et al. "A survey on security and privacy issues in Internet-of-Things." IEEE Internet of Things Journal vol.4., no.5, 2017, pp. 1250-1258.

[7] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks, vol.54, no.15, 2010, pp. 2787-2805.

[8] Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." Internet of Things, vol 5, 2019, pp. 41-70.

[9] Das, Ashok Kumar, Sherali Zeadally, and Debiao He. "Taxonomy and analysis of security protocols for Internet of

Things." Future Generation Computer Systems, vol.89, 2018, pp. 110-125.

[10] Di Martino, Beniamino, et al. "Internet of things reference architectures, security and interoperability: A survey." Internet of Things Vol.1 ***(2018):*** *pp. 99-112.*

[11] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 ***(2019)****: pp.82721-82743.*