International Journal for Modern Trends in Science and Technology
Volume 10, Issue 06, pages 73-76.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue06.html
DOI: https://doi.org/10.46501/IJMTST1006013

Performance and Analysis of Smart IoT Devices using Machine Learning and Blockchain Technology

Muppidi Sai Kumari

Assistant professor, Andhra Loyola College, Vijayawada, India.

To Cite this Article
Muppidi Sai Kumari, Performance and Analysis of Smart IoT Devices using Machine Learning and Blockchain Technology, *International Journal for Modern Trends in Science and Technology*, 2024, 10(06), pages. 73-76. https://doi.org/10.46501/IJMTST1006013

Article Info
Received: 29 May 2024; Accepted: 21 June 2024; Published: 23 June 2024.

ABSTRACT

The integration of Smart Internet of Things (IoT) devices with machine learning (ML) and blockchain technology represents a significant advancement in optimizing performance, ensuring security, and enhancing the analytical capabilities of IoT systems. This paper investigates the synergistic potential of these technologies, focusing on how machine learning can improve the efficiency and functionality of Smart IoT devices, while blockchain offers a robust framework for secure data management and decentralized trust. Machine learning algorithms are employed to analyze the vast amounts of data generated by IoT devices, enabling predictive maintenance, anomaly detection, and efficient resource management. These algorithms help in identifying patterns and trends that can lead to improved decision-making and automation processes. On the other hand, blockchain technology addresses the critical issues of data integrity, security, and privacy in IoT networks. By providing a decentralized ledger, blockchain ensures tamper-proof data recording, secure transactions, and transparent data sharing among devices without relying on a central authority. This work explores various case studies and applications where the combination of IoT, ML, and blockchain has been successfully implemented. It also discusses the challenges and limitations associated with integrating these technologies, such as computational constraints of IoT devices, scalability issues of blockchain networks, and the complexity of machine learning models. Finally, the convergence of IoT, machine learning, and blockchain technology holds immense potential to revolutionize industries by enhancing the performance, security, and analytical capabilities of IoT systems. Future research directions are proposed to address the current challenges and to further explore the possibilities of this technological synergy.

Keywords: Internet of Things (IoT), Machine Learning (ML), Blockchain Technology, Data Security, Predictive Maintenance, Anomaly Detection, Decentralized Trust, Data Integrity.

1.INTRODUCTION

The Internet of Things (IoT) is a cutting-edge invention that has tremendous potential, rapid expansion, and immense influence. Networks of devices that exchange data to allow for new applications are referred to as IoT. IoT devices come in a range of sizes and forms, from smart items to low-power equipment. Processes can be automated with the help of IoT, saving both money and time. Data collected by instruments, cameras, and other Internet of Things devices is often sent to a server for

analysis and tracking. The data must always be accessible to other people and systems, but the quality of the information kept on the server must be preserved to thwart malicious attempts to alter the data [1]. The expansion of IoT networks has led to a growth in the number of IoT devices, with an estimated increase from 7.74 in 2019 to 25.44 billion in 2030. The fundamental issue with these gadgets is that security is generally not taken into consideration, as the login and password are often not modified during deployment. So, IoT devices have become the primary target of attackers, as they attempt to breach them to launch Distributed Denial-of-Service (DDoS) attacks or use them as botnets to steal data [2]. This is evident from the estimated 105 million attacks on IoT devices in the first half of 2019. Various authentication methods, architectural designs, and algorithms have been proposed that take into account the resource constraints of IoT devices [3-4].

IoT networks are frequently linked to cloud computing and data centers. As IoT devices typically generate a large amount of data, various algorithms are used to extract important information and automate processes. Machine Learning (ML) techniques are also used to create Intrusion Detection Systems (IDSs). Data from IoT devices are often transferred to servers where they are stored before being examined [5]. Typically, data should be kept in a way that protects their integrity and thwarts hostile attempts to alter them while being constantly accessible to other users and systems. Data can be stored securely using blockchain (BC) [3]. The possibility of combining ML methods and BC approaches to address cyber risks in the IoT area is a new concept that warrants further investigation. Security and privacy are interconnected, and privacy is a collection of rules that vary depending on the application [5].

2. LITERATURE SURVEY

In [6], a widespread IDS was proposed that used fog computing to detect DDoS attacks against edge nodes in BC-based IoT networks. The system's efficacy was assessed using an actual IoT-based dataset that included current assaults in BC-based IoT networks. Random Forest (RF) and XGBoost trained on dispersed fog nodes were used to measure performance. XGBoost beat RF in binary attacks, whereas RF exceeded XGBoost in terms of multi-attack detection. Furthermore, compared to XGBoost, RF needed less time for instruction or testing on dispersed fog nodes. In [7], pattern recognition, AI, and BC were examined to address IoT security challenges, highlighting the security concerns that can be handled using them and the research obstacles that must be addressed. In [8], a random subspace learning KNN was used to protect against forged commands aiming at manipulating an industrial control process, and a BC based Integrity Checking System (BICS) was used to prevent misrouting attacks that alter the OpenFlow rules of SDN-enabled industrial IoT systems. In [9], an IDS based on neural network clustering was proposed to help administrators identify and reduce the risk of attacks in the early stages, reducing power consumption. The RP protocol has a clear objective and enables real-time applications to conserve energy while ensuring security. Increasing the number of online applications that require protection against different risks, the demand for security will only increase. An ML system was proposed to address the nonlinear identity problem, detect faults, and reconstruct the system. To detect and classify malicious attacks on network integrity and node power consumption in a wireless sensor network, a self-organizing map could be trained to monitor the network using a learning technique and identify any nodes that behave abnormally. In [10], the possible uses and limitations of distributed ledger technology were explored in domains that interact with social impacts, including social justice and concerns. A major challenge is that ML algorithms require large amounts of data to train effectively. This can be a problem in the context of IoT, as devices may have limited processing and storage capabilities. Furthermore, ML algorithms may be vulnerable to attacks that can be used to fool the algorithm into making incorrect predictions [11].

3. RESULT ANALYSIS

In this section, the system's implementation is described. Health data about the patient is kept fully confidential. Security in mobile healthcare communication channels is important due to the severe repercussions of data tampering or leakage brought on by hacked infrastructure. This E-healthcare service is highly dependent on resource allocation and security.

A virtual private network extends a private network within an organization on a public network like the Internet. It provides policy benefits such as functionality, security, and management by allowing the computer to send and receive data as if immediately linked to a private network over a shared or public network. A private network is created by establishing a digital point-to-point connection using dedicated connections, virtual protocols, or traffic encryption. A WAN link between the two sites is similar to a virtual private Internet connection. Users can access resources from other trusted networks and their organization's intranet by using virtual private networks. Internet users can use this method to protect their location and identity by connecting to proxy servers. Authentication requirements must be met before establishing a virtual private connection. Administrator is able to view the statistical data on users who have registered as well as health centre statistics While producing a report, the system administrator usually introduces an employee, a new hospital, an insurance office, and a local hospital. In addition, the administrator has access to the patient information system, profile history, and patient data. Documents, medical tests and other information that is necessary are gathered and entered into computer software. At that facility, health information is accessible to doctors, patients and trust professionally. The health maintenance division is responsible of providing health cards and maintaining patients who are currently enrolled in health insurance. The registration data is saved in a central database that is stored in the cloud and the system analyzes the data and provides a health card. On the website, users need to enter their details. To finish the authentication process, they should create a password. After installation, users can view or access their data by logging in. Once the password was entered, a One Time Password (OTP) must be sent to their email address. The customer can use the OTP to log in to the respective module.

Average response time of retrieving the medical files through Integrated Dynamic Cloud based E-Health Management (IDCEHM) and traditional or physical E-health management system. As observed from results, it is clear that, in emergency health situations this Integrated Dynamic Cloud Computing based E-health management systems are retrieving the health records of patient with high speed than traditional management systems. Therefore there is high chance of saving the patient's life. As a result, described framework has many issues related to remote patient monitoring, routine examinations, provision of appropriate personal planning and access to patient information to defined individuals such as doctors, nurses and relatives, therefore the problem solved.

Table 1: Performance of E-Health Management Systems

	IDCEHM	Traditional E-Health Management	Proposed System
10	0.3	2.5	2
20	0.45	2.4	2
40	1.2	3.1	3
80	1.6	3.6	5
160	1.7	4	3
320	1.9	3.8	3.3
10	0.3	2.5	2

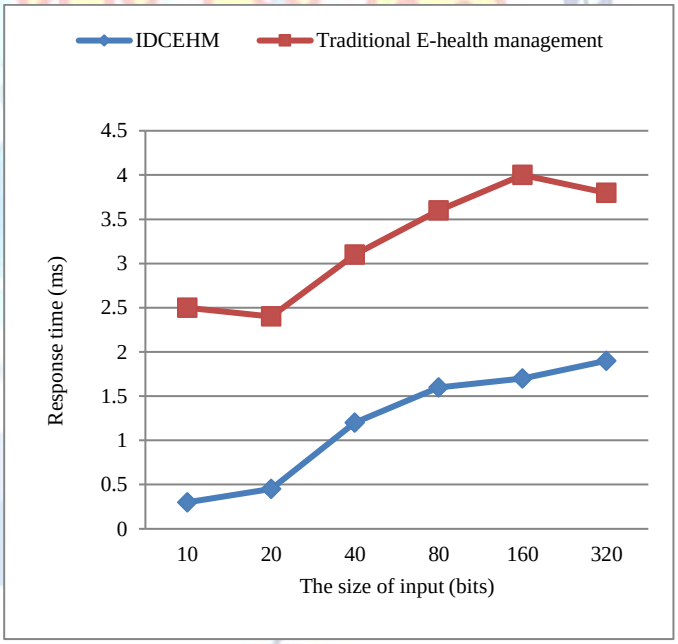

Figure 2: Response Time Performance of Two Models

Security and Privacy parameters are more important in patient's health records maintenance. The comparative analysis of Integrated Dynamic Cloud based E-Health Management (IDCEHM) and *traditional or physical* E-health management system is represented in below Fig. 3.

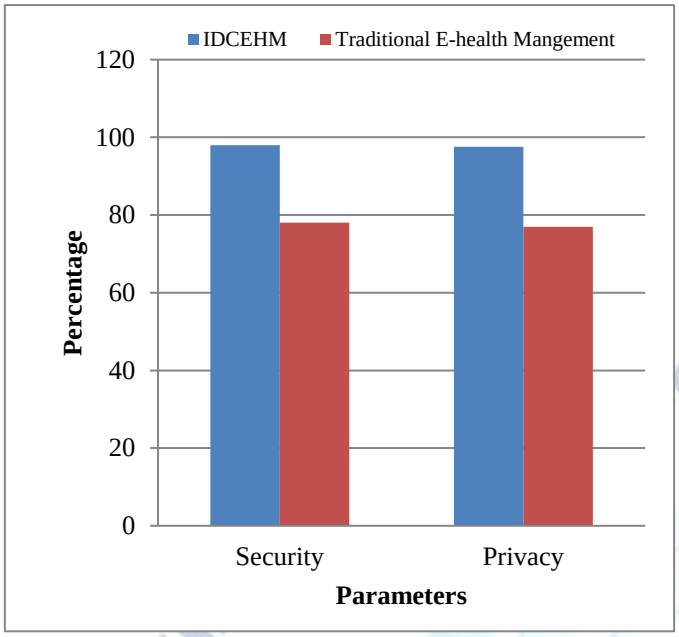

Figure 3: Comparative Analysis

From result analysis and Figures it is clear that, the performance of Integrated Dynamic Cloud based E-Health Management (IDCEHM) is better than the traditional E-health management system. In emergency health situations this IDCEHM systems are retrieving the health records of patient with high speed than traditional management systems. Therefore security and privacy of IDCEHM model are high which indicates the efficiency of this model.

3. CONCLUSION

Integrating machine learning and blockchain technology for the performance and analysis of smart IoT devices offers a comprehensive solution to address the current challenges of data overload, security, and performance optimization. This approach not only improves the operational efficiency of IoT devices but also ensures data security and integrity, paving the way for more reliable and effective IoT ecosystems.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] M. Anwer, S. M. Khan, M. U. Farooq, and Waseemullah, "Attack Detection in IoT using Machine Learning," Engineering, Technology & Applied Science Research, vol. 11, no. 3, pp. 7273–7278, Jun. 2021, https://doi.org/10.48084/etasr.4202.

[2] T. Alqurashi, "Arabic Sentiment Analysis for Twitter Data: A Systematic Literature Review," Engineering, Technology & Applied Science Research, vol. 13, no. 2, pp. 10292–10300, Apr. 2023, https://doi.org/10.48084/etasr.5662.

[3] P. Singh, Z. Elmi, V. Krishna Meriga, J. Pasha, and M. A. Dulebenets, "Internet of Things for sustainable railway transportation: Past, present, and future," Cleaner Logistics and Supply Chain, vol. 4, Jul. 2022, Art. no. 100065, https://doi.org/10.1016/j.clscn.2022.100065.

[4] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Applied Sciences, vol. 9, no. 20, Jan. 2019, Art. no. 4396, https://doi.org/10.3390/app9204396.

[5] N. Behar and M. Shrivastava, "A Novel Model for Breast Cancer Detection and Classification," Engineering, Technology & Applied Science Research, vol. 12, no. 6, pp. 9496–9502, Dec. 2022, https://doi.org/10.48084/etasr.5115.

[6] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," Internet of Things, vol. 11, Sep. 2020, Art. No. 100227, https://doi.org/10.1016/j.iot.2020.100227.

[7] A. Derhab et al., "Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security," Sensors, vol. 19, no. 14, Jan. 2019, Art. no. 3119, https://doi.org/10.3390/s19143119.

[8] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A Self Organizing Map Intrusion Detection System for RPL Protocol Attacks," International Journal of Interdisciplinary Telecommunications and Networking (IJITN), vol. 11, no. 1, pp. 30–43, Jan. 2019, https://doi.org/10.4018/ IJITN.2019010103.

[9] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," ACM Computing Surveys, vol. 53, no. 6, Sep. 2020, Art. no. 122, https://doi.org/10.1145/3417987.

[10] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," IEEE Communications Surveys & Tutorials, vol.22, no. 3, pp. 1686–1721, 2020, https://doi.org/10.1109/COMST.2020.2986444.

[11] "Welcome to Python.org," Python.org, May 29, 2023. https://www. python.org/.