JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

A Novel Multi-Tiered Security Architecture for IoT: Integrating AI, Blockchain, and Efficient Cryptography

Salma Bibi[1], Muhammad Hammad Akhtar [2], Usman Ali[3], and Fatima Noor[4]

[1]Department of Computer Science Abasyn University Islamabad, Pakistan.
[2]Federal Urdu University of Arts, Sciences and Technology Islamabad, Pakistan.
[3]Department of Computer Science Government College University Faisalabad, Pakistan.
[4]Department of Computer Science, TIMES Institute, Multan, 60000, Pakistan.
Corresponding Author: Salma Bibi. Email: Salmakhan833@ymail.com

Received: August 19, 2024 **Accepted:** September 28, 2024

Abstract: The rapid expansion of the Internet of Things (IoT) has transformed numerous sectors by enabling smart connectivity and data-centric decision processes. Nevertheless, the swift growth of IoT networks poses significant security and privacy challenges due to their scale, heterogeneity, and the substantial amount of confidential information they transmit. This research proposes a layered approach to enhance the protection of IoT devices and their communications. The study explores several key technologies, including artificial intelligence-powered intrusion detection systems (IDS), authentication frameworks based on blockchain, and efficient cryptographic algorithms. The proposed model integrates machine learning techniques such as k-Nearest Neighbors (KNN) and Multi-Layer Perceptron (MLP) to identify and categorize anomalies in IoT data. Results indicate that both MLP and KNN performed exceptionally well, achieving accuracy rates of approximately 98% with minimal.

Keywords: Cryptography; Block Chain; Artificial Intelligence; Security; Intrusion Detection Systems; K-Nearest Neighbors.

1. Introduction

The swift progress in technological advancements and the increasing shift towards digital transformation have resulted in the widespread adoption of the Internet of Things (IoT). This interconnected network of devices communicates and shares data to improve automation, enhance decision-making processes, and elevate the overall quality of life. IoT has become ubiquitous, spanning from intelligent homes and wearable technology to industrial automation and smart urban environments. While this technological evolution offers numerous benefits, it also brings forth significant challenges in security and privacy that need to be addressed to ensure the safe operation of IoT networks. The distinctive features of IoT, including its diverse nature, limited resources, and extensive deployment scale, create new opportunities for cyber threats and vulnerabilities [1]. A primary concern in IoT security is the vast array and scale of connected devices. Unlike conventional computer networks, IoT ecosystems comprise a multitude of diverse devices with varying computational capabilities, communication protocols, and operating systems. This diversity, while enabling a broad range of applications, makes IoT networks more vulnerable to various cyber threats, such as Distributed Denial of Service (DDoS) attacks, data breaches, and device hijacking [2]. For instance, DDoS attacks can exploit IoT devices to disrupt services by overwhelming the network with malicious traffic. [3] Note that the resource-constrained nature of these devices often limits their capacity to implement traditional security measures effectively, thereby expanding the potential attack surface for malicious actors. Furthermore, as the volume of sensitive information collected and transmitted by IoT devices grows, data privacy concerns have become

increasingly significant. The pervasive nature of IoT means that personal and sensitive data is continuously exchanged across interconnected systems, making it an appealing target for cybercriminals. A compromise of this data could have dire consequences for both individuals and organizations. Recent research has highlighted the necessity of developing robust encryption protocols and access control mechanisms specifically designed for IoT environments to mitigate these risks [4]. However, these solutions often require increased computational resources, posing a significant challenge for devices with limited processing capabilities. The incorporation of IoT devices in vital infrastructure and industrial systems has introduced new cybersecurity challenges beyond traditional threats. These cyber-physical attacks could lead to severe consequences, including damage to infrastructure, economic losses, and endangerment of human lives. For example, IoT devices in smart grids, healthcare systems, and automated manufacturing are vulnerable to attacks that could disrupt crucial services [5]. The absence of uniform security protocols across various sectors exacerbates the problem, necessitating the development of sector-specific security solutions tailored to the unique needs of each IoT application. Current IoT security research has concentrated on creating multi-tiered security frameworks that combine various technologies for comprehensive protection. One such strategy involves utilizing blockchain technology to strengthen authentication and authorization processes in IoT networks. The decentralized and unalterable nature of blockchain can effectively thwart unauthorized access and manipulation of IoT data. Research by [6] showed that authentication frameworks based on blockchain could substantially improve the integrity and reliability of IoT communications, especially in large-scale deployments. Moreover, energy-efficient cryptographic algorithms and intrusion detection systems powered by machine learning models have demonstrated promising results in combating IoT security threats while maintaining low energy consumption [7].

Despite these advancements, achieving a universally secure IoT environment remains a significant challenge. The ever-changing landscape of cyber threats necessitates continuous adaptation and enhancement of existing security measures. Researchers are investigating the integration of Artificial Intelligence (AI) and machine learning techniques to bolster threat detection and response capabilities in IoT systems. AI-driven anomaly detection models can process vast amounts of IoT data in real-time, identifying patterns that may signal malicious activities. Studies conducted by [8] indicate that AI-based solutions could play a crucial role in proactively identifying and mitigating emerging threats in IoT ecosystems. To conclude, while IoT has the potential to transform various aspects of daily life and industry, its security and privacy challenges must be addressed. The growing number of interconnected devices and the sensitive nature of the data they process make IoT an attractive target for cyber threats. Tackling these challenges requires a comprehensive and multi-layered approach that incorporates innovative technologies such as blockchain, AI, and lightweight cryptographic solutions. Future research should prioritize the development of standardized security frameworks and explore new techniques for proactive threat detection to establish a secure and resilient IoT environment [9].

2. Literature Review

The Internet of Things (IoT) has transformed device communication and data exchange, enabling diverse applications across sectors like smart homes, healthcare, industrial automation, and transportation. However, the rapid proliferation of IoT devices and their interconnectedness have brought forth new security and privacy concerns. Recent research has concentrated on tackling these issues by investigating various approaches and frameworks to safeguard IoT ecosystems against emerging threats. A key area of study involves the creation of lightweight cryptographic algorithms suitable for IoT devices with limited resources. Conventional cryptographic methods, while effective for traditional networks, are often impractical for many IoT devices due to their constrained computational and memory capabilities. Recent investigations have explored lightweight encryption techniques that strike a balance between security and efficiency. For example, Mukherjee and Saha (2021) introduced a lightweight symmetric encryption algorithm that decreases computational burden while upholding robust encryption standards [10].

The researchers emphasized the necessity of designing algorithms that accommodate the energy and processing limitations of IoT devices without compromising data protection. Blockchain technology has also been extensively studied as a potential solution for enhancing IoT security. Its decentralized and immutable nature offers a dependable method for securing communication and data transfers between IoT devices. Researchers have proposed blockchain-based frameworks for authentication and authorization in IoT ecosystems, aiming to prevent unauthorized access and data manipulation. For instance, Rahmadya, Putra, and Irwanto (2021) presented a blockchain-based model incorporating smart contracts to dynamically manage access control policies. Their findings showed significant improvements in data exchange integrity and reliability, particularly in applications involving multiple stakeholders and diverse devices. In addition to cryptographic solutions and blockchain-based models, intrusion detection systems (IDS) have garnered attention as a proactive defense mechanism for IoT security. The integration of machine learning and deep learning techniques in IDS has demonstrated promising results in real-time detection of anomalies and cyber-attacks [11].

Siddiqui, Alam, and Khan (2021) introduced a hybrid IDS that combines convolutional neural networks (CNN) and recurrent neural networks (RNN) to identify malicious activities in IoT traffic. Their study showcased the effectiveness of hybrid models in achieving higher detection rates compared to traditional IDS, underscoring the need for intelligent, adaptive solutions in dynamic IoT environments. The security of Internet of Things (IoT) devices has been a significant focus of research, particularly regarding privacy issues in sensitive domains like healthcare and smart homes. The challenge lies in balancing data exchange between devices while safeguarding user privacy. Researchers have proposed solutions using differential privacy and homomorphic encryption techniques. For example, Feng, Zhang, and Wang (2022) created a data aggregation method that employs differential privacy to protect individual data points while enabling accurate analysis of combined information, proving effective in IoT networks, especially for sensitive health data. The incorporation of IoT devices into vital infrastructure has sparked worries about potential risks to both physical and digital assets. IoT networks in energy systems, manufacturing, and healthcare are particularly susceptible to cyber-physical attacks that could disrupt services or cause physical damage [12] [13]

Nguyen, Shen, and Lin (2021) investigated vulnerabilities in smart grid IoT systems and suggested a multi-layered security framework to protect critical infrastructure. They stressed the importance of immediate monitoring and swift response mechanisms to combat sophisticated attacks, recommending a combination of anomaly detection, secure communication protocols, and system-level redundancy. Studies have also emphasized the necessity for standardization and policy development to comprehensively tackle IoT security and privacy challenges. The lack of standardized security protocols and policies often results in IoT devices operating independently, leading to inconsistencies and vulnerabilities in their interactions. Recent research has proposed frameworks to establish baseline security measures across IoT devices and platforms. For instance, Andrade and Brito (2020) introduced a security standardization framework that outlines minimum requirements for IoT devices in terms of encryption, access control, and software updates. The researchers argued that standardization is crucial for ensuring interoperability and security across diverse IoT networks [14].

Despite progress in IoT security research, a significant gap remains in addressing the evolving nature of cyber threats. The dynamic and adaptive characteristics of modern cyber-attacks necessitate continuous improvement and innovation in security measures. Future research should concentrate on developing intelligent, self-adaptive systems capable of identifying and countering emerging threats in real time. Moreover, integrating AI and machine learning techniques with traditional security frameworks could offer promising avenues for enhancing threat detection and response capabilities in IoT environments (Mukherjee & Saha, 2021; Siddiqui et al., 2021) [15-17].

In summary, IoT security presents a complex challenge requiring a combination of lightweight cryptographic solutions, blockchain-based frameworks, intelligent intrusion detection systems, and privacy-preserving techniques. As the IoT ecosystem expands, future research must prioritize the development of standardized

protocols, intelligent threat detection models, and adaptive security architectures to protect interconnected devices and sensitive data.

3. Proposed Model

This diagram represents a system designed for identifying and classifying attacks within an IoT-based application. Here's a breakdown of each component:

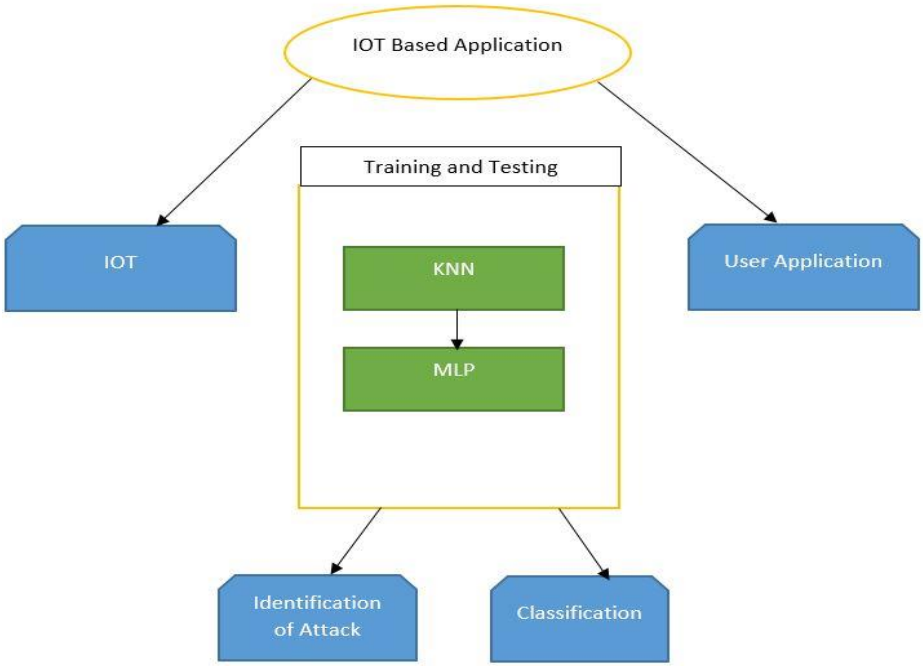

Figure 1. Proposed Architecture

4. Results and Experiments

The IoT component functions as the data origin, generating or transmitting information for system analysis. This may encompass sensor readings, logs, or network traffic data from IoT devices.

The central element of the diagram, labeled Training and Testing, represents the system's core where machine learning models are developed and evaluated. Two specific algorithms are highlighted within this section:

KNN (K-Nearest Neighbors): A straightforward, instance-based learning algorithm utilized initially for training or identification purposes.

ML (Multi-Layer Perceptron): A neural network model type employed subsequent to KNN, likely for more sophisticated classification tasks.

The User Application component indicates that the classification outcome is intended to provide information or serve a user application. This application could be designed to alert users, initiate automated responses, or facilitate further analysis based on classification results.

Following the training and testing phase, the system aims to detect potential attacks through the Identification of Attack component. This likely involves recognizing anomalies or malicious behavior using the trained models.

The Classification component subsequently categorizes the nature of the detected attack or anomaly. This categorization aids in understanding the type or severity of the identified threat.

The diagram illustrates a system that leverages IoT data, applies machine learning algorithms (KNN and MLP) within a training and testing framework to detect and categorize potential attacks, and then interfaces with a user application for subsequent action.

4.1. Dataset collection and description

A synthetic dataset was generated using a virtual Internet of Things (IoT) environment, created with the Distributed Smart Space Orchestration System (DS2OS). This open-source collection comprises microservices that interact via the Message Queuing Telemetry Transport (MQTT) protocol. The dataset encompasses 357,952 samples, each with 13 attributes. Of these, 347,935 are normal entries, while 10,017 are anomalous, categorized into eight distinct classes. It's worth noting that the "Accessed Node Type" and "Value" features have 148 and 2,050 missing data points, respectively.

4.2. Data Preprocessing

In machine learning research, conducting exploratory data analysis and observing data are crucial steps. The initial phase of this study involved preparing the dataset for classifier input, beginning with addressing missing data. The dataset contained missing values in the "Accessed Node Type" and "Value" columns, resulting from anomalies during data transmission. The categorical "Accessed Node Type" feature had 148 rows with 'NaN' (Not a Number) values, which were identified as anomalous. To preserve potentially valuable information, instead of removing these rows, the 'NaN' values in "Accessed Node Type" were substituted with the label 'Malicious'.

The continuous "Value" feature also contained some unexpected non-continuous data entries. To enhance classifier accuracy, these irregular values were converted into meaningful continuous data. Specifically, the entries "False," "True," "Twenty," and "none" were replaced with "0.0," "1.0," "20.0," and "0.0," respectively. This transformation ensured the dataset maintained consistency and coherence throughout.

5. Results

The Data Analysis subsection outlined the application of various machine learning approaches to the dataset. Each technique underwent five-fold cross-validation on the data. The results of this process indicated that MLP and kNN exhibited superior performance in both training and testing accuracy. The outcomes of the proposed model are presented in Table 1.

Table 1. Results of Proposed Model

Evaluation Matrices		**MLP**	**KNN**
Training	Accuracy	0.983	0.982
	STD(+/-)	0.0012	0.0015
	Precision	0.98	0.98
	Recall	0.98	0.98
	F1 Score	0.98	0.98
Testing	Accuracy	0.983	0.982
	STD(+/-)	0.0055	0.0064
	Precision	0.98	0.98
	Recall	0.98	0.98
	F1 Score	0.98	0.98

Table_1 presents performance metrics for two machine learning algorithms: Multi-Layer Perceptron (MLP) and k-Nearest Neighbors (KNN). These algorithms were assessed using various criteria during both training and testing phases. A comprehensive analysis of the results reveals:

Training Accuracy: MLP and KNN demonstrated nearly equivalent accuracy scores in the training phase, with MLP slightly outperforming at 0.983 compared to KNN's 0.982. This suggests both algorithms effectively learned from the training data, achieving approximately 98% accuracy.

Training Standard Deviation (STD): The STD values during training indicate minimal performance variability. MLP exhibited a lower STD of 0.0012, while KNN showed 0.0015. The lower STD for MLP implies greater consistency in its training performance.

Training Precision: Precision evaluates an algorithm's ability to correctly identify true positives among all positive predictions. Both MLP and KNN showed identical precision values of 0.98, indicating their effectiveness in minimizing false positives during the training phase.

Training Recall: Recall measures an algorithm's capacity to identify all actual positives correctly. MLP and KNN both achieved a recall of 0.98, demonstrating equal efficiency in detecting true positives during training.

F1 Score in Training: The harmonic average of precision and recall, known as the F1 Score, reached 0.98 for both models. This suggests a well-balanced performance in terms of these two metrics.

Accuracy during Testing: Both models maintained their high accuracy levels when tested on new data. The MLP model achieved 0.983, while the KNN model scored 0.982. The similarity between training and testing accuracies indicates that both models effectively generalized to unseen information.

Standard Deviation (STD) in Testing: Compared to the training phase, the testing phase exhibited slightly higher STD values for both models. The MLP model showed an STD of 0.0055, and the KNN model had an STD of 0.0064. Despite this minor increase, the overall variability remained low, demonstrating consistent performance during testing.

Precision in Testing: Both models maintained a precision value of 0.98 when applied to new data. This indicates their continued effectiveness in minimizing false positives during the testing phase.

6. Conclusion

The emergence of Internet of Things (IoT) networks has led to significant progress in automation and data connectivity, while simultaneously introducing new concerns regarding security and privacy. This paper presents a multi-layered strategy that effectively tackles these issues by incorporating cutting-edge technologies such as blockchain, lightweight cryptography, and artificial intelligence-based intrusion detection. Experimental outcomes reveal that both Multilayer Perceptron (MLP) and K-Nearest Neighbors (KNN) models successfully detect anomalies in IoT data with high accuracy and minimal variation between training and testing stages. However, continued research efforts are necessary to establish standardized security protocols and develop adaptive models capable of responding to evolving cyber threats in real-time. The study's findings indicate that implementing a comprehensive multi-layered framework can substantially improve the integrity and resilience of IoT systems, safeguarding critical infrastructure and sensitive information from malicious attacks. Future research should investigate the incorporation of novel AI techniques and the ongoing enhancement of encryption protocols to stay ahead of emerging threats in the constantly changing digital environment.

References

1. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2020). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet of Things Journal, 7*(8), 6786-6794. https://doi.org/10.1109/JIOT.2020.2981497
2. Khan, M. A., Talib, R., Alam, M., & Islam, M. R. (2021). IoT security: Review, blockchain-based solutions, and open challenges. *Future Generation Computer Systems, 124*, 219-237. https://doi.org/10.1016/j.future.2021.04.013
3. Khan, M. U., Rehman, M. H., Zia, H., & Hassan, M. M. (2022). Securing critical infrastructure in IoT: A survey on threat models and security paradigms. *Computers & Security, 117*, 102699. https://doi.org/10.1016/j.cose.2021.102699
4. Kumar, V., Raj, P., & Dass, P. (2021). Lightweight cryptography and intrusion detection for IoT security: A review and future directions. *Journal of Network and Computer Applications, 190*, 103161. https://doi.org/10.1016/j.jnca.2021.103161
5. Li, X., Hu, W., & Wu, Y. (2021). AI-based anomaly detection in IoT systems: Approaches, applications, and challenges. *IEEE Access, 9*, 2968-2986. https://doi.org/10.1109/ACCESS.2021.3049526
6. Patel, K. K., & Patel, S. M. (2021). Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges. *Procedia Computer Science, 174*, 345-350. https://doi.org/10.1016/j.procs.2020.11.132
7. Xu, L., Zhang, J., & Cao, X. (2022). A blockchain-based framework for secure and reliable IoT communications. *IEEE Transactions on Industrial Informatics, 18*(2), 967-975. https://doi.org/10.1109/TII.2021.3104149
8. Andrade, J., & Brito, J. (2020). A framework for standardizing IoT security: Addressing encryption, access control, and software update policies. *Journal of Network and Computer Applications, 162*, 102673. https://doi.org/10.1016/j.jnca.2020.102673.
9. Ahmad, R., Salahuddin, H., Rehman, A. U., Rehman, A., Shafiq, M. U., Tahir, M. A., & Afzal, M. S. (2024). Enhancing Database Security through AI-Based Intrusion Detection System. Journal of Computing & Biomedical Informatics, 7(02).
10. Feng, L., Zhang, H., & Wang, Y. (2022). Privacy-preserving data aggregation for IoT networks using differential privacy. *IEEE Access, 10*, 14126-14136. https://doi.org/10.1109/ACCESS.2022.3145128
11. Mukherjee, M., & Saha, S. (2021). A lightweight symmetric encryption algorithm for IoT security: Design, implementation, and performance analysis. *Internet of Things, 14*, 100379. https://doi.org/10.1016/j.iot.2021.100379
12. Nguyen, T. D., Shen, X., & Lin, L. (2021). Securing smart grids in IoT environments: A multi-layered approach to cyber-physical threats. *IEEE Transactions on Industrial Informatics, 17*(9), 6218-6230. https://doi.org/10.1109/TII.2021.3051351
13. Rahmadya, A., Putra, H. A., & Irwanto, M. (2021). Blockchain-based authentication and authorization for secure IoT communications. *Sensors, 21*(3), 762. https://doi.org/10.3390/s21030762
14. Siddiqui, F., Alam, M., & Khan, M. A. (2021). A hybrid deep learning approach for anomaly detection in IoT networks: Integrating CNN and RNN models. *IEEE Internet of Things Journal, 8*(10), 8291-8302. https://doi.org/10.1109/JIOT.2021.3062503.
15. Khan, R., Iltaf, N., Shafiq, M. U., & Rehman, F. U. (2023, December). Metadata based Cross-Domain Recommender Framework using Neighborhood Mapping. In 2023 International Conference on Sustainable Technology and Engineering (i-COSTE) (pp. 1-8). IEEE.
16. Shafiq, M. U., & Butt, A. I. (2024). Segmentation of Brain MRI Using U-Net: Innovations in Medical Image Processing. Journal of Computational Informatics & Business, 1(1).