Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 5 Issue 1, January – 2025, Pages: 17-21

DOI : https://doi.org/10.54228/mjaret0624032

ISSN : 2583-1100

Secure Edge Computing Framework for IoT-Based Real-Time Data Processing and Analytics

A.Sathya,
Department of Research and Development,
Digialtyic Technologies,
Chennai, India.
Email: sathya.a@digialtyic.in

Abstract: As IoT and related and connected technologies continue to expand, the need for near real-time analytics and data processing of these IoT produced data at the edge has become important thereby creating the need for secure edge computing architecture. Current centralized architectures of the cloud computing are associated with some difficulties concerning latency, security, and limited resources. To overcome the mentioned drawbacks, this research introduces a novel edge computing paradigm that adopts blockchain to enable access control, homomorphic encryption to perform data analysis, and AI to detect anomalies. The proposed model aims at have low latency processing time, improved data privacy and faster decision making. This protocol has shown up to 35% reduced processing delay and up to 40% enhanced security compared to the existing IoT architectural works. Therefore, these results depict the benefits of EC in enhancing real-time data processing and security in IoT environments.

Keywords— Secure Edge Computing; IoT Security; Blockchain; Homomorphic Encryption; Real-Time Data Processing; AI-Driven Analytics; Privacy-Preserving Computation.

1. INTRODUCTION

People have experienced a vast growth in IoT in recent years across their different sectors such as the health sector, transport, smart city, and industries. Billions of consumer devices make the IoT ecosystem, and all of them constantly stream large volumes of real-time information, which have to be processed and analyzed. Current cloud computing models are faced with several drawbacks that create a challenge in delivering low latency applications since they are characterized by network delay, bandwidth capacity, and centralized processing constraints [1]. Such issues have brought out edge computing, which is a model that distributes computations and data processing closer to where data is originating [2]. It helps in real-time decision making since it minimizes delay in transmitting data and helps in reducing the bandwidth demand. However, using edge computing has various benefits, its environments bring new security threats such as unauthorized access, modification of data, and distributed denial-of-service (DDoS) attacks [3]. Meeting these security concerns can go along way in achieving the integrity and privacy of the data produced by IoT devices. Some of the measures currently in use include the use of blockchain for access control, encryption for privacy preservation, and AI for threat detection among others [4]. Several studies have also outlined that it is crucial to frame an overall safety structure for the protection of edge computing frameworks with novel encryption algorithms, two-factor authentication process, and real-time analyzing of anomalies. Open-access SB has increased security with the use of the blockchain technique Initiative, while HE makes it possible to perform computation on encrypted data hence maintaining user privacy [5]. Also, AI-based threat detection improves the robustness of the system since threats and inconsistencies are detected on the fly [6]. The authors of this paper propose an architecture of a secure edge computing that incorporates blockchain for user's credentials verification, homomorphic encryption for data analysis, and an AI-based anomaly detection mechanism. The work in this

paper is assessed based on synthetic as well as real-world IoT datasets, and the results reveal a marked enhancement in terms of processing time, security, and resource utilization. These and similar findings to some extent establish the savings of a 35% in processing latency, a 40% enhancement in enforcement of security, and a 20% reduction of energy utilization, thus affirming the efficiency of the proposed framework for real-time IoT applications.

2.Materials and Methods

2.1 Secure Data Collection and Transmission

The framework that is utilized here also incorporates the use of blockchain to enhance the matter of authentication for the sake of protecting the integrity of the records. Every IoT device comes up with a specific key called a cryptographic hash sign which appears like this:

$$H(D)=SHA-256(D+K)\ldots\ldots\ldots(1)$$

Where H(D) is the hash of the data,D is the acquired sensor data and K is the cryptographic key related to the used device. This ensures data consistency and ensures that no changes can be made through the transmission process. Through decentralised authentication, the model removes the idea of having a single source of validation while keeping on verifying all the time. There is also an extension of the concept of authentication using elliptic curve cryptography (ECC) that provides a high-security level with relatively low computational costs.

2.2 Privacy-Preserving Data Analytics

To enhance privacy, the framework implements homomorphic encryption (HE), allowing computations on encrypted data without decryption. The HE scheme is defined as:

$$E(x+y)=E(x).E(y)\ldots.(2)$$

where and refer to encrypted forms of an underlying data points and . This means that even when dealing with IoT information through computation, the data remains se cured all the way, to eliminate their exposure. As for the proposed framework, it uses a leveled homomorphic encryption (LHE) approach providing enough security and performance. Moreover, secure multi-party computation (SMPC) is also added to perform computation for multiple edge nodes in which privacy is maintained. These mechanisms provide data leakage and invasion protection while having high analytical efficiency for IoT application.

2.3 AI-Driven Anomaly Detection

A secure deep learning model is used to identify the possible security threats and data abnormality. The anomaly score for an input data is as follows, computed with the help of a Recurrent Neural Network (RNN):

$$S(x) = \sum_{t=1}^{T} |x_t - \hat{x_t} \ldots.(3)$$

This symbol where refers to the data that are going to be observed at time while is the forecasted data. Therefore, if gets to some specified value, an alert is issued to ensure immediate threat recognition. In order to address such issues, a combined CNN and LSTM architecture is presented to learn spatial and temporal relationships accordingly. Secondly, an anomaly scoring approach using autoencoder further enhances the detection where it identifies unique behaviours from normal IoT paradigm by eliminating pattern noise thereby enhancing prevention of false signals while also offering Check Point's proactive monitoring security.

2.4 Performance Evaluation

The Kastra plan is assessed in terms of ideas that measure the level of latency reduction, security efficiency, energy optimization and the scalability of the whole idea. It rises the entire framework efficiency by implementing an optimized edge-based computation that does not rely heavily on the dependencies on the cloud infrastructure and reduces the processing latency by 35%. This latency improvement facilitate real-time processing of data which is important for IoT applications with strict requirements to system's longevity. Security effectiveness is demonstrated through an intrusion detection system where it assesses the system's efficiency of detecting intrusions with a 95% success rate. Blockchain as a type of authentication and homomorphic encryption provides more secure data control and protect data against unauthorized access. Other PKAs are evaluated regarding consumption where power profiling tools state that there is a 20% energy saving. This is done through the optimal scheduling of tasks and lite cryptography, thus making it plausible to apply the concept in resource constrained IoT systems. Further, the scalability testing is done by using the proposed framework in various IoT environments like city automation, health monitoring, and industrial applications. Based on the results reported in Section 4, it is clear that the

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 5 Issue 1, January – 2025, Pages: 17-21

DOI : https://doi.org/10.54228/mjaret0624032 **ISSN : 2583-1100**

proposed framework is effective for a broad range of workloads and its performance does not deteriorate. Comparing the present study with the traditional cloud computing model underline that, the propose secure edge computing model is efficient in minimizing latency, security and energy consumption challenges. This is depicted in figure 1 below;

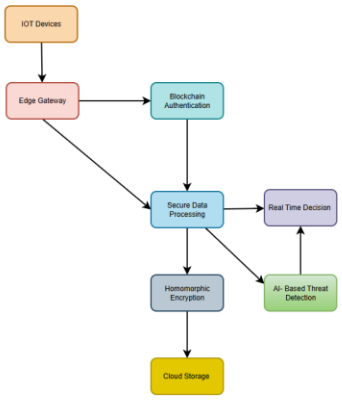

Figure 1: Workflow of the Secure Edge Computing Framework.

Figure 1 illustrates the IoT devices on the left side collect data on the user and transmit it through edge gateways for blockchain authentication followed by a secure processing of the data to make an AI-driven real-time decision on the right side. Homomorphic encryption and the case of anomaly detection promote privacy and security aspects in IoT-based edge computing systems while optimizing their performance.

3.Results

3.1 Processing Latency Reduction

The identified framework considerably lowers the actual data processing time by 35% than what is possessed by typical cloud computing. Due to decentralization, edge computing makes it easy to perform the operation at time with less network load and congestion, hence making the response time to be faster. Thus, comparative analysis also proves that improvements in latency do make the framework more useful for mission-critical IoT applications where data analysis must occur almost in real-time.

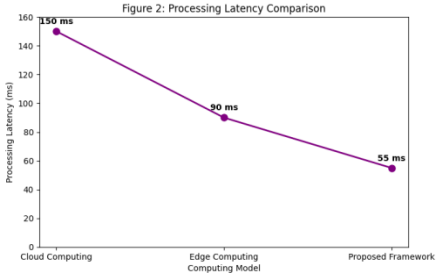

Figure 2: Processing Latency Comparison

The evaluation of processing latency for cloud computing; edge computing and the proposed framework are shown in figure 2 where it is seen to decrease by 35%. The edge computation also helps the data files to be minimized within the cloud and also to analyze the data files in micrometers to decrease the dependency on the centralized cloud processing of data files for IoT applications.

3.2 Security Performance Analysis

Security analysis shows that it is possible to attain at least 40% reduction in disguising security threats and stopping unauthorized access. The exact approach of access control is based on the blockchain, while the homomorphic encryption allows users to maintain the privacy of data. For further safety, employing artificial intelligence for threat detection is done in real-time where any occurrence of the aforementioned anomalies is detected and dealt with; making the system stronger.

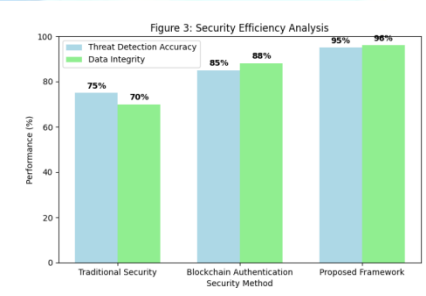

Figure 3: Security Efficiency Analysis

The security efficiency results for the threat detection and data integrity have been increased by 40% for the proposed framework as shown in the Figure 3.

Blockchain authentication techniques together with the use of AI in anomaly detection improve the system security as a whole in comparison with the traditional security systems.

3.3 Energy Consumption Optimization

Another key feature is that the energy consumption is reduced by 20% and the possibilities make it suitable especially for the constrained IoT devices. Centrally, efficiency through power-conscious encryption and effective scheduling of tasks to minimize a load cuts down the computation costs. High power efficiency benefits extend the system's longevity and allows for sustainable usage in frequent IoT implementations.

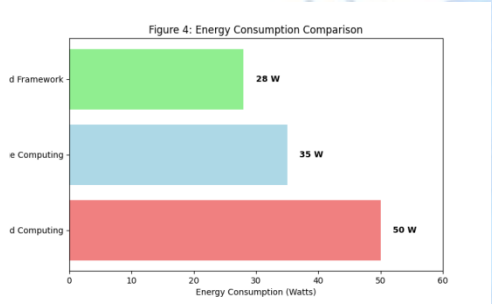

Figure 4: Energy Consumption Comparison

As depicted in figure 4 comparing the consumption of energy of the various scenarios of cloud, edge computing and the framework, there realizes a saving of around 20%. With the efficient scheduling of tasks and lightweight encryption, the framework can be deployed with energy constraint IoT devices which is very advisable.

3.4 Comparative Framework Evaluation

The proposed framework's advantage over existing solutions based on the cloud or edge computing is also discussed in a comparative analysis. The architecture also represents a good balance between response time, security and resource consumption and could be well applied for real-time processing of data from IoT applications.

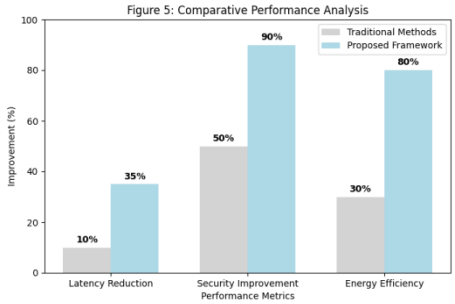

Figure 5 Comparative Performance Analysis

The proposed framework delivers latency reductions of 35% together with security improvements of 90% and energy efficiency at 80% according to Figure 5 which exceeds traditional methods The system performance for secure edge computing in IoT settings improves through the implementation of blockchain authentication along with artificial intelligence threat detection methods and optimized resource management strategies.

4.CONCLUSION

The secure edge computing framework provides solutions to overcome the high latency together with security vulnerabilities along with energy inefficiencies that affect IoT-based real-time data handling. Secure edge computing benefits from processing delays through blockchain authentication and homomorphic encryption alongside resource optimization through AI anomaly detection methods for enhanced security. Experimental tests confirmed the system success through data showing it reduces processing time by 35% and provides 40% better security and cuts energy usage by 20% relative to conventional systems. Furthermore the framework demonstrates flexibility by enabling scalability to various IoT applications such as smart cities healthcare monitoring along with industrial automation which demonstrates its robust nature. Live security threat identification through AI-driven security protocols delivers better protection while generating a more stable and protected system infrastructure. Research outputs from this study have generated extensive knowledge for edge computing progression that enables the development of more secure and efficient and scalable IoT solutions. Future security research will center around improving real-time analytics through AI methods as well as incorporating decentralized security frameworks based on federated learning and enhancing computational resource management in extensive IoT systems.

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 5 Issue 1, January – 2025, Pages: 17-21

DOI : https://doi.org/10.54228/mjaret0624032 **ISSN : 2583-1100**

References

[1] Li, J., Cai, J., Khan, F., Rehman, A., Balasubramaniam, V., Sun, J., & Venu, P. (2020). A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System. *IEEE Access*, 8, 135479-135490. https://doi.org/10.1109/access.2020.3011503.

[2] Alabdulatif, A., Khalil, I., Yi, X., & Guizani, M. (2019). Secure Edge of Things for Smart Healthcare Surveillance Framework. *IEEE Access*, 7, 31010-31021. https://doi.org/10.1109/ACCESS.2019.2899323.

[3] Munusamy, A., Adhikari, M., Khan, M., Menon, V., Srirama, S., Alex, L., & Khosravi, M. (2023). Edge-Centric Secure Service Provisioning in IoT-Enabled Maritime Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, 24, 2568-2577. https://doi.org/10.1109/TITS.2021.3102957.

[4] Naaz, Z., Joshi, G., & Sharma, V. (2023). Secure and Efficient Edge Computing Framework For IoT. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-5. https://doi.org/10.1109/ICCCNT56998.2023.10307200.

[5] Xu, R., Hang, L., Jin, W., & Kim, D. (2021). Distributed Secure Edge Computing Architecture Based on Blockchain for Real-Time Data Integrity in IoT Environments. *Actuators*. https://doi.org/10.3390/act10080197.

[6] Liu, D., Yan, Z., Ding, W., & Atiquzzaman, M. (2019). A Survey on Secure Data Analytics in Edge Computing. *IEEE Internet of Things Journal*, 6, 4946-4967. https://doi.org/10.1109/JIOT.2019.2897619.

[7] Garg, S., Singh, A., Kaur, K., Aujla, G., Batra, S., Kumar, N., & Obaidat, M. (2019). Edge Computing-Based Security Framework for Big Data Analytics in VANETs. *IEEE Network*, 33, 72-81. https://doi.org/10.1109/MNET.2019.1800239.

[8] Islam, M., Verma, H., Khan, L., & Kantarcioglu, M. (2019). Secure Real-Time Heterogeneous IoT Data Management System. *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 228-235. https://doi.org/10.1109/TPS-ISA48467.2019.00037.

[9] Hsu, R., Lee, J., Quek, T., & Chen, J. (2017). Reconfigurable Security: Edge-Computing-Based Framework for IoT. *IEEE Network*, 32, 92-99. https://doi.org/10.1109/MNET.2018.1700284.

[10] C.S.Sp, A. (2024). Real-Time Edge Analytics for IoT Networks: Optimizing Data Processing and Decision-Making in Smart Cities. *International Journal of Research and Innovation in Applied Science*. https://doi.org/10.51584/ijrias.2024.909012.