ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

A Trust-Based Framework for Secure Data Aggregation in IoT

[1] Saurabh Kumar, [2] Zaineb Naaz, [3] Vidushi Sharma

[1] [2] [3] Department of Computer Science and Engineering, Gautam Buddha University, Greater Noida, India
Corresponding Author Email: [1] saurabhkumar843327@gmail.com, [2] zainebnaaz119@gmail.com, [3] vidushi@gbu.ac.in

Abstract*— With the increasing use of Internet of Things (IoT) devices, ensuring the security and privacy of these devices is crucial. It is necessary to obtain accurate data from trusted IoT nodes for effective decision-making. In traditional methods, devices are more complex and consume more power, which has driven the need for a Trust-Based Design Framework. In this paper, we design a trust-based framework to assess the trustworthiness of a device and then aggregate the data at the edge node. Data aggregation is an efficient technique widely used in the IoT for collecting statistics from IoT sensor nodes. However, resources are limited, and the inherent unreliability of wireless transmission makes sensors in IoT vulnerable to various attacks. A compromised node may leak sensitive information to an unauthorized node, significantly threatening the integrity of the data aggregation process. Protecting the aggregation process from compromised-node attacks and quantifying the uncertainty in aggregation results has been a significant research challenge. There are various parameters for determining the trust value of each node, and developing a framework for a trust management system based on these parameters and trust factors is essential. The working of the proposed model is demonstrated through simulation experiments conducted in MATLAB, focusing on communication, data aggregation, detection of malicious activity, and the trustworthiness of nodes.

Index Terms*— Edge Computing, IOT, Peer-to-peer communication, Secure data aggregation, Trust management system (TMS).

I. INTRODUCTION

The Internet of Things' (IoT) rapid expansion has revolutionized data-driven applications by enabling end-to-end connectivity and real-time decision-making, from smart cities to industrial automation. However, IoT networks are vulnerable to security risks like data tampering, spoofing, and denial-of-service attacks due to their dispersed and resource-constrained nature. To facilitate data transfer between devices, IoT uses a variety of communication technologies, including wireless sensor networks, Bluetooth, Wi-Fi, and Zigbee. But as the number of IoT devices rises, so does the amount of data generated, creating enormous difficulties for data processing and transmission. Designing and developing an efficient and secure data processing mechanism becomes critical. Data aggregation is an efficient technique in data collection processing, in which data is processed and aggregated at

The edge node within the network. Data aggregation has emerged as a crucial technique for addressing IoT network challenges, serving three primary functions: (1) reducing network traffic through data condensation, (2) minimizing storage requirements, and (3) optimizing energy consumption [7]. Traditional aggregation methods simply forward raw data to centralized servers without preprocessing, making them susceptible to malicious node attacks. When compromised nodes inject false data, the entire aggregation process becomes corrupted, ultimately delivering inaccurate information to decision-making systems [8]. There are different data aggregation approaches that are based on assumptions that sensor nodes are cooperative and not attacked, but in reality, the exposure to the natural environment and a lack of protection make sensor nodes prone to different types of attacks. To counteract this, edge computing is explored as a promising technology that stores and processes data at the edge node, reducing data transmission overhead and optimizing real-time processing. As shown in Fig. 1, edge computing allows real-time data processing and aggregation. Many researchers have proposed different methods of trust calculation. Atkali et al proposed a novel malicious node detection scheme based on weighted trust calculation. Hue et al have proposed a secure model based on credibility and reputation using a probability distribution function. In this paper a weight based model was proposed which will calculate the trust score of each node using different parameters like package delivery ratio, time consumed, energy consumption and each parameter is having some weight and if any node is having a trust score less than threshold then it is a malicious node or above the threshold value then it is trustworthy. The Remainder of the paper is organized as follows: Section 2 discusses related work. Section 3 provides the Preliminaries for the research. Section 4 provides system models. Section 5 provides the simulation results, and finally, Section 6 concludes our work.

II. RELATED WORK

There are several proposals for calculating trust and finding malicious nodes in IoT Networks. The work [1]in Yanbing Liu et al had proposed a novel trust-based secure data aggregation for IoT that uses the behavior of IoT nodes and then integrates with data aggregation techniques. In this research, they can detect the abnormal behavior of IoT nodes, penalize them, and improve aggregation accuracy and reduce maliciousness for the tempering of data.

Similarly, Atakali et al[2] have proposed a novel malicious node detection scheme based on weight trust evaluation . The Aim of this research is to detect and then isolate the malicious nodes to avoid false information through compromised node

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

in the network.

Hu et al [3] have proposed a reputation-based secure model that can evaluate the credibility of an IoT node, guaranteeing the authenticity and reliability of the IoT node in the network. In this, the researcher used a probability distribution function to evaluate the behavior of the IoT node. Usually, the compromised IoT nodes behave abnormally, like delays in sending data, not participating in transferring data, which can impact the credibility of the network.

The authors [4] present an efficient privacy-preserving edge computing framework by utilizing the RSA digital signature scheme, symmetric cipher model, and data aggregation. With edge devices deployed at the edge of the network, our framework efficiently aggregates IoT data and performs secure data transmission. The performance analysis shows that the proposed framework is secure and efficient in both energy consumption and computational cost

The Authors Joshi and Sharma[5] have proposed a Hidden Markov Model(HMM) based trust mechanism to find the maliciousness and selfishness of IoT networks within the network. In this Paper, they evaluate the behavior of IoT nodes over time and they are isolating the malicious nodes after finding the vulnerability.

III. PRELIMINARIES

A. Edge computing

Edge Computing is a process in which the data is processed close to the source or at the edge of the network, which helps in reducing latency and increasing efficiency. The term "Edge" refers to computing devices such as routers, gateways, and switches, which act as a link between the cloud center and the data source. The data sources include IoT devices such as sensors, wearables, and smartphones. Edge nodes first collect data from source nodes, preprocess it, and then send it to the cloud server. One of the main functions of edge computing is data aggregation, where tasks like data summation are performed before forwarding the preprocessed information. Processing Data at the local level will reduce latency, and it will improve the efficiency of the network. It also helps in enhancing the security of the network as data is processed locally, and then it is transmitted to the cloud. As shown in Figure 1, the IoT node is sending the data to the edge node, and then, further, the edge node is sending the data to the cloud.

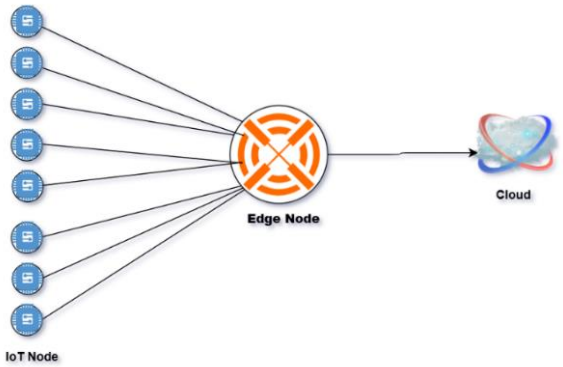

Fig. 1. Edge computing

B. Trust evaluation parameters

In this research we are making a trust management system which will evaluate the trustworthiness of each individual node in the network.

To evaluate the trust score, here are some parameters:

i. Data Accuracy(DA)

Data Accuracy measures how close the data from the IoT node matches the reference data, which is given by the edge node. It reflects the reliability of the IoT node and helps to identify the malicious node in the network

$$Data\ Accuracy\ (DAi) = 1 - \frac{|Di - Dref|}{Dref}$$

- DAi = Data Accuracy of ith node
- Di = The Actual Value Sent from the IoT node
- Dref = The reference value from edge node

ii. Transmission Behavior (TB)

It is defined as the number of packets forwarded by the node divided by the number of packet received by node. It is a metrics on which we can find if the node can send data without dropping or altering it.

$$Transmission\ Behavior\ (TBi) = \frac{Packets_{Forwarded}}{Packets_{Received}}$$

- TBi = Transmission Behavior of IoT ith node
- Packets Forwarded = Packets Sent from IoT nodes
- Packets Received = Packets Received at Edge Node

iii. Authentication Success Ratio (ASR)

It is defined as how a node successfully passes the authentication or protocol. It is calculated using the formula, the number of successful authentications divided by the total number of authentications.

$$AuthenticationSuccessRatio(ASRi) = \frac{Successful\ authetication}{Total\ Authentication}$$

iv. Energy Consumption

It is defined as the energy consumed in transmitting the data from IoT nodes to the edge node. to calculate energy, we are using a first-order radio model that will calculate the energy consumed by each node.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

Energy Consumption $E_{TX}(k,d) = E_{elec} * k * E_{amp} * k * d^n$

E_{elec}= Electronics Energy

E_{amp} = Amplification Energy

k=No of bits being transmitted

d= distance between IoT nodes and edge node

n= path loss exponent

n=2: Free Space Model

n=4: Multipath Fading Model

v. Latency

Latency is defined as the time consumed in transmission of data from IoT nodes to edge nodes, or, in the case of a conventional method, the latency is defined as the time consumed in transmission of data from an IoT node to a cloud node or base station.

Latency(L) = $D_{proc} + D_{trans} + D_{prop} + D_{queue}$

D_{proc}=Processing Delay

D_{trans} = Transmission Delay

D_{prop} = Propagation Delay

D_{queue} = Queuing delay

C. Data Aggregation

Data aggregation is the process of collecting data from multiple sources and organizing it in a single source, then aggregating it by using any aggregation function like sum, min, max, avg, etc. It takes multiple values as input and returns a single summary

IV. SYSTEM MODEL

In this mode, we are using edge computing to find a malicious node in the network. Edge computing is a simple and organized method that can directly connect with the IoT network. It consists of 1 edge node, one cloud node, and 8 to 48 normal nodes, which are randomly placed within a 350×350 field. The system will evaluate the trust score of each individual IoT node in the network. The trust score is evaluated based on parameters like data accuracy, transmission behavior, authentication success rate, energy consumption, and time consistency. Each of the parameters has some weightage. In this paper, we are applying equal weightage to all the parameters. If the trust score is below the threshold value, it can be marked as malicious, and if the value is greater than or equal to the threshold value, it can be marked as a trustworthy node. After evaluating the trustworthiness of the IoT node, the edge node will aggregate the data from the trustworthy node and send it to the cloud node or base station, as shown in Figure 2

In this research, the edge node is considered safe and secure, as it does not have any malicious properties. When each IoT node starts sending the data to the edge node, the edge node will collect the data and calculate its trust score. If the trust score is above the assigned threshold value, the data will be aggregated. Otherwise, the data will not be aggregated. The aggregated data will be sended to the cloud node, which will be further used in analysis or other work. The trusted data will not impact further research or analysis as it is from a trusted source. Using edge computing to filter out the malicious data will also help in cost because we are eliminating the malicious data at the edge node only, so the cost of storage should be low as to traditional method

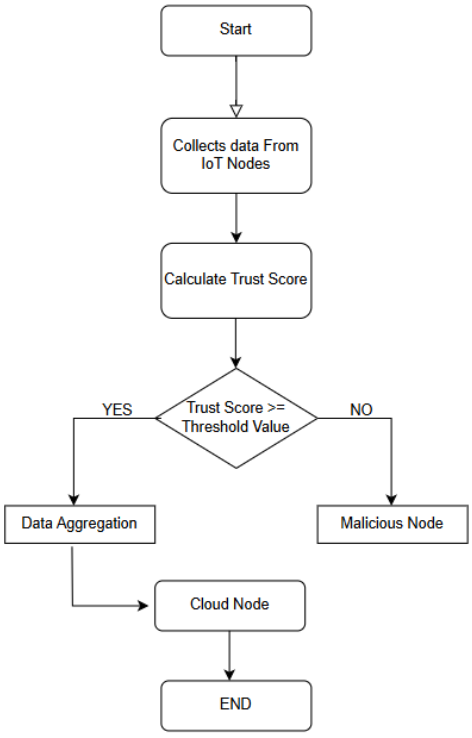

Fig 2. System model

A. System Simulation:

The simulation of the system model is performed in MATLAB with a network field size of 500 m x 500 m. The IoT nodes are distributed randomly in the network, and the Edge Node and Cloud Node are located at fixed positions. The data is considered to be homogeneous and is of Constant Bit Rate (CBR) traffic. It is considered that the packet size of the data sent by IoT nodes. Other parameters are mentioned in Table 1

Table 1: Simulation Parameters

Parameters	Values
Total Number of Nodes	10-50
Number of edge Nodes	1
Number of cloud Nodes	1
Field Size	500m x 500m

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

Parameters	Values
Electronics Energy (E) $elec$	50nJ/bit
Energy for Data Aggregation $(E)DA$	5nJ/bit/Signal
ε fs	10pJ/bit/m^2
ε amp	0.0013pJ/bit/m^4

V. SIMULATION RESULTS

A. Trusted and Malicious Nodes Analysis:

Figure 3 compares trusted vs malicious IoT nodes in the network. In this, the trust score is calculated using different parameters, and if the value is below the threshold, then it is a malicious node; if the trust score is above the threshold, then it is a trustworthy node. Using this Figure, we can identify that the network size grows, and the number of malicious nodes also increases, which helps us to filter the malicious data earlier. Using this trust-based edge computing method, we can reduce the risk of malicious data propagation to the cloud.

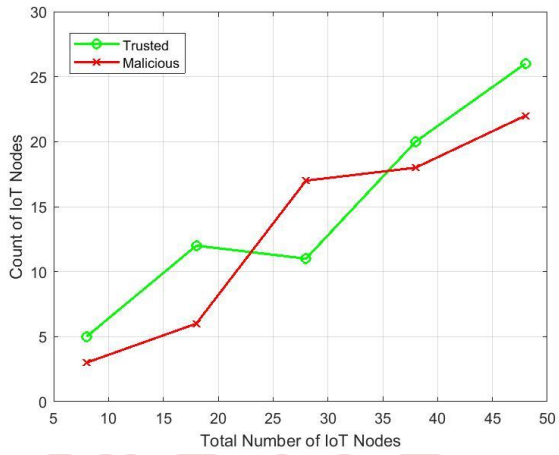

Fig. 3. Trusted Vs Malicious IoT nodes

B. Data Aggregation Comparison: edge computing vs traditional method

Figure 4 shows the data aggregated from the number of IoT nodes. In trust-based edge computing, only data from trusted IoT is aggregated at the edge node, and in the traditional approach, the data from both trusted and malicious IoT nodes is aggregated. This shows the data reduction and bandwidth efficiency in edge computing, which helps in scalable and secure IoT deployment

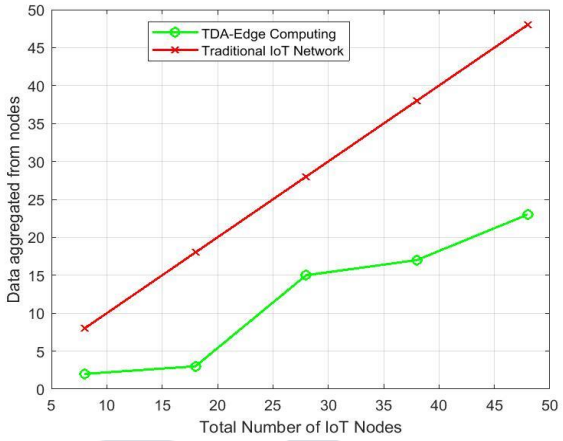

Fig. 4. Data Aggregation Comparison

C. Energy Consumption

Figure 5 shows the energy consumption in trust-based edge computing vs energy consumption in traditional IoT networks. The energy consumption in edge computing is less than that of traditional IoT networks. It is beneficial for battery-powered devices.

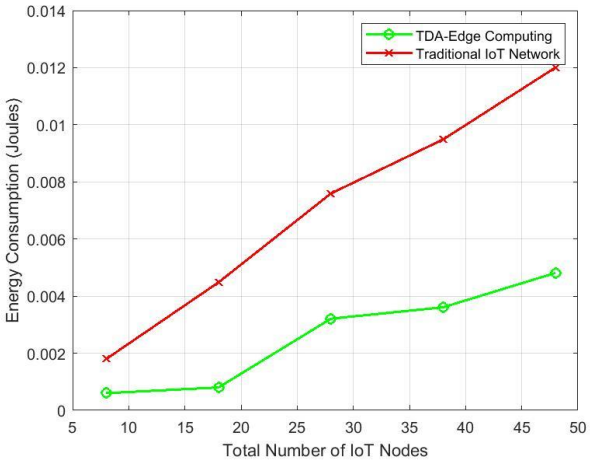

Fig. 5. Energy Consumption in Edge Computing Vs Traditional IoT Network

D. Latency

Figure 6 shows the latency in data transmission of trust-based edge computing vs traditional IoT networks. Edge-based systems have lower latency as compared to traditional IoT networks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 12, Issue 06, June 2025

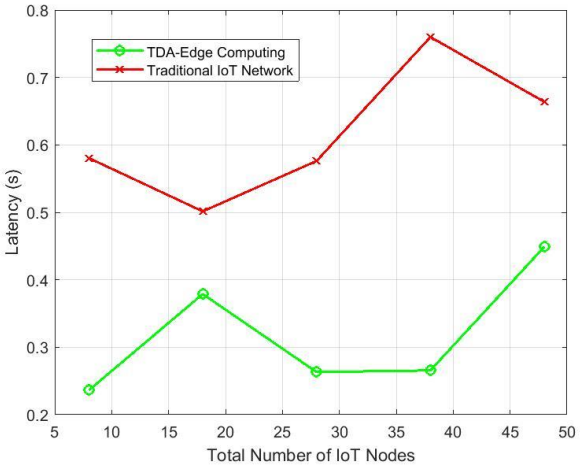

Fig. 6. Latency Comparison in edge computing vs Traditional IoT Network

VI. CONCLUSION

In this paper, we proposed a trust-based data aggregation framework utilizing edge computing to improve the security and reliability of IoT networks. By calculating the trust score of each node using parameters such as data accuracy, transmission behavior, authentication success ratio, energy consumption, and latency, we effectively detected and isolated malicious nodes from the data aggregation process. Our MATLAB-based simulation results demonstrated that the edge-based trust system provides improved energy efficiency, reduced latency, and better scalability when compared to traditional peer-to-peer (P2P) communication. This approach ensures that only trustworthy data is sent to the cloud, reducing the chances of compromised or tampered data affecting decision-making processes. The framework is particularly suitable for real-time, energy-constrained IoT applications, providing a secure and efficient alternative to existing models.

REFERENCES

[1] A. Vassil, Y. Liu, J. Liu, and X. Lu, "A Behavior-Based Trust Management Scheme for Secure Data Aggregation in IoT," IEEE Access, vol. 7, pp. 140966–140978, 2019.

[2] Idris M Atakli, Hongbing Hu, Yu Chen, Wei Shinn Ku, and Zhou Suo. “Malicious node detection in wireless sensor networks using weighted trust evaluation.” In Proceedings of the 2008 Spring Simulation Multiconference, pages 836-843. Society for Computer Simulation International, 2008.

[3] H. Hu, X. He, and Y. Chen, "A Reputation-Based Model for Secure Data Aggregation in IoT," Sensors, vol. 19, no. 9, p. 2010, 2019.

[4] Z. Naaz, V. Sharma, and S. Kumar, "Efficient Privacy-Preserving Edge Computing Framework for IoT Using Cryptographic Techniques," International Journal of Computer Applications, vol. 182, no. 17, pp. 1–6, 2021.

[5] Joshi G, Sharma V,” Hidden Markov Trust for Attenuation of Selfish and Malicious Nodes in the IoT Network” Research Square, September 21st, 2021. DOI 10.21203/ rs.3.rs-776578/v1

[6] Yanbing Liu, Xuehong Gong, Congcong Xing,” A novel trust-based secure data aggregation for Internet of Things” 2014 9th International Conference on Computer Science & Education (ICCSE), August 2014, Page 435-439, DOI:10.1109/ICCSE.2014.6926499

[7] A. Rashid and S. Hasan, "Survey on Edge Computing Models and Architectures," Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.

[8] D. Zhang, Z. Zhou, and T. X. Brown, "Data Aggregation in IoT Networks: Algorithms, Taxonomy, and Open Issues," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2412–2435, 2019.

[9] H. Al-Baz and M. El-Alfy, "A Hybrid Deep Learning Model for Malicious Node Detection in IoT Networks," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4505–4513, 2021.

[10] Z. Naaz and V. Sharma, "Performance Analysis of Edge Node in IoT Network," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp.546- 551, doi:10.1109/IC2PCT60090.2024.10486497.

[11] G. Joshi and V. Sharma, “A robust and trusted framework for IoT networks,” J. Ambient Intell. Humaniz. Comput., no. 0123456789, 2022, doi: 10.1007/s12652 022 04403 w.

[12] Z. Naaz, G. Joshi, and V. Sharma, “Secure and Efficient Edge Computing Framework for IoT,” pp. 6 10,2023, doi: https://doi.org/10.1109/ICCCNT56998.2023.10307200