Mesopotamian Journal of Computer Science

Volume 3 | Issue 1 Article 6

1-1-2023

Infusing k-means for securing IoT services in edge computing

Tam Sakirin
Computer Science Department, Faculty of science and information technology, International University, Phnom Penh, Cambodia, kirin.it@gmail.com

Iqra Asif
Riphah International University, Islamabad, Pakistan

How to Cite This Article

Sakirin, Tam and Asif, Iqra (2023) "Infusing k-means for securing IoT services in edge computing," *Mesopotamian Journal of Computer Science*: Vol. 3: Iss. 1, Article 6.
DOI: https://doi.org/10.58496/MJCSC/2023/007
Available at: https://map.researchcommons.org/mjcsc/vol3/iss1/6

Mesopotamian journal of Computer Science
Vol. **(2023)**, 2023, **pp**. 39-46
DOI: https://doi.org/10.58496/MJCSC/2023/007; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

Infusing k-means for securing IoT services in edge computing

Tam Sakirin [1,*], Iqra Asif [2]

[1] *Computer Science Department, Faculty of science and information technology, International University, Phnom Penh, Cambodia.*

[2] *Riphah International University, Islamabad, Pakistan.*

ARTICLE INFO

Article History
Received 11 Jan 2023
Accepted 16 Feb 2023
Published 08 Mar 2023

Keywords
Infusing k-means
Securing IoT services
Edge computing
Intelligent computing

ABSTRACT

Accurate, timely, and safe administration of data from IoT devices is made possible by intelligent computing. As the number of IoT devices proliferates, more and more data will be collected, adding depth and breadth to the existing range of IoT services. Technology that incorporates entire systems on a single integrated circuit has improved to the point where more and more consumer electronics can support full-fledged operating systems. It is impractical to use a single computing model for the entire planet since doing so would cause severe network congestion and security holes. In order to solve this problem, we present a framework that utilizes both blockchain technology and edge computing to provide a lightweight data aggregation and secure data investigation solution for Internet of Things (IoT) applications without compromising data security or protection. We use a lightweight data aggregation process at the hub level to keep traffic flowing smoothly and quickly. In order to protect the safety of sensitive data and ensure the precision of IoT AI models, we also offer a multi-level fuzzy hashing process. Preliminary testing demonstrates the viability of the method presented here.

1. INTRODUCTION

Edge computing (EC) is utilized in different apparatuses consistently, including cell phones, iPads, robots, and shrewd vehicles utilized in the auto and assembling ventures. Likewise, EC consolidates medical services IoT and clinical checking gadgets. Information assortment and handling in EC happens toward the finish of the network where data is delivered as opposed to in focal cloud servers, diminishing distance and dispensing with dormancy. The fundamental thought behind EC is to utilize levels of leadership of end waiters with creating computational assets to perform low-end IoT exercises in versatile and huge and different computing and compact gadgets, explicitly edge gadgets. EC is likely to give the area, adequate data transfer capacity, constant, privacy, and a moderate discussion to help developing applications for savvy urban communities. These CC-related areas of interest brought about the fast improvement of this sort of computing. As per Measurement's latest examination, the EC market in the US, which was $85.3 million out of 2018, is supposed to reach $1033 million by 2025. As per a later report, the assessed number of parts utilized in 2018 in all regions of the planet is a little more than 11 billion and is supposed to be twenty billion by 2025. Notwithstanding, when contrasted with CC, EC is more practical by using IoT instruments, which are more affordable by moving the end microcontroller and asset ability to the end stages without bringing about extra expenses. As EC creates capacity and computing abilities straightforwardly for clients, the postpone in information taking care of is altogether decreased. Moreover, any exercises that don't need the cloud server's assets can be coordinated straightforwardly to end hubs. Then again, to diminish workload stress, they will execute the exercises and information on the cloud server [1].

Notwithstanding, by killing the chance of sending client information to the focal framework and sending the confirmation parts on the endpoint, EC can accomplish the classification and strength of the private framework as well as client information security. EC has been consistently developing lately because of these qualities. Notwithstanding the way that substances have a far reaching arrangement in EC innovation circumstances like intelligent wellbeing, business IoT, and savvy associated vehicles, there are still some underlying problems that hinder EC's quick execution, one of which is security [2].

*Corresponding author. Email: kirin.it@gmail.com

1.1 Edge Computing Taxonomy for the Internet of Things

An IoT-based scientific classification of edge computing that takes into account concrete factors including distant network advances, computing hubs, computing standards, administration-level goals, major enabling impacts, information types, applications, and features.

A. Network Technologies

IoT devices collect data and transmit it to an edge server that is conveniently located nearby. These devices communicate with edge computing nodes using wireless and cellular networking (e.g., 3G, 4G, and 5G) or traditional networking advancements like Ethernet. These network improvements vary with respect to data transfer rate, transmission range, and supported devices. Clients whose applications are deployed to the edge server take advantage of the flexibility and scalability of remote networks. But, wireless network developments aren't as dependable as their wired counterparts [3].

B. Computing Nodes

IoT devices are inadequate for computationally intensive activities due to their low processing power. Yet, edge servers can help low-powered IoT devices perform better by providing access to their resources. The edge computing paradigm employs various computational devices to provide various forms of support to IoT customers. IoT-based edge computing relies on these process gadgets as its foundation. Computing hubs can be anything from servers to base stations (BS) to switches to even vehicles, all of which can provide resources and services to devices in the Internet of Things (IoT). In the context of the computing universe, their application is unprecedented [4].

C. Computing Paradigms

Different computing ideal models are utilized in IoT to offer different types of assistance in light of utilization necessities. Distributed computing, edge computing (i.e., MEC, haze, and cloudlet), portable specially appointed cloud (Macintosh), and cross breed stages are instances of these ideal models. Distributed computing is a unified computing foundation intended to give ceaseless admittance to strong cloud servers. At the point when information is gotten from far off IoT gadgets, these servers can handle it quickly and send the outcomes back. Notwithstanding, continuous postponement delicate applications can't endure long network delays. Constant transmission of a lot of crude information over temperamental remote links may likewise be wasteful. Edge computing, then again, is a decentralized computing stage that carries distributed computing capacities to IoT gadgets at the network edge. MEC, which carries distributed computing capacities to the edge of a cell network, is a significant sort of edge computing stage. BS gives computational and stockpiling services in MEC. Unlike MEC, haze computing utilizes nearby haze hubs (i.e., neighborhood network gadgets like a switch or change) to offer computational types of assistance inside a particular geographic district. Following the outcome of IoT, haze computing is viewed as a head innovation. Cloudlet is one more kind of edge computing in which time-delicate and calculation concentrated IoT gadget tasks are performed on a server conveyed in the neighborhood. Unlike cloud and edge computing stages, which depend on framework arrangement, Macintosh utilizes the common assets of adjacent cell phones to handle calculation serious tasks. In mixture computing, cloud and edge computing are utilized couple. Such foundation is ordinarily utilized when we want the huge computing assets of distributed computing yet can't endure the cloud's inertness. To conquer the dormancy issues related with distributed computing, edge computing variations can be utilized in such applications [5].

D. Service Level Objectives

The different help level targets for edge computing with regards to IoT are as follows:

1. Idleness Minimization: High dormancy has turned into a significant issue for IoT-based shrewd applications. An elective stage, for example, edge computing, that can ensure convenient conveyance of services is expected to satisfy the nature of administration (QoS) necessities of postponement delicate IoT applications (e.g., shrewd transportation and internet gaming)[6].
2. Network the executives: various peculiarities, for example, deficient virtualization support, lack of consistent availability, and wasteful clog control, corrupt the general network execution. Consequently, productive utilization of network assets in edge computing is crucial for IoT.
3. Cost Enhancement: The utilization of a satisfactory stage for empowering edge computing requires broad framework sending that includes significant forthright venture and functional costs. The greater parts of these costs are connected with network hub situation, which requires conscious preparation and streamlining to limit the general expense. Sending of an ideal number of hubs at fitting positions can essentially diminish capital, and ideal game plan of edge hubs can limit functional expenses.

4. Energy The board: Energy the executives is additionally a significant goal of IoT-based edge computing. Supporters need to have severe command over power the board. Energy-effective IoT gadgets and applications are advantageous in edge computing. As indicated by a review, one trillion IoT hubs need detecting stages that help different applications utilizing power reaping to guarantee versatility, lessen costs, and keep away from successive battery substitution.
5. Asset The board: Ideal administration of computational assets is significant in acquiring administration level goals. Suitable asset the executives incorporates coordination of assets, assessment of accessible assets, and appropriate portion of workload [7].
6. Information the executives: The huge number of IoT gadgets at present is supposed to produce a lot of information that should be overseen on time. Productive and powerful information the board systems are positive in edge computing. Transmission and accumulation of IoT-produced information are significant worries in information the board [8].

1.2 Challenges in Cloud computing

Numerous applications all over the planet use distributed computing to store monstrous measures of information, process it, and dissect it for factual examination or to acquire significant bits of knowledge from the information to produce esteem from it. IoT is growing more refined gadgets for a large number of uses, bringing about huge measures of information that should be put away, shared, and moved starting with one area then onto the next. Cloud services are utilized to finish the jobs recorded above while additionally giving clients more prominent adaptability and productivity. These cloud-based services are incredibly gainful to business needs. Contingent upon their necessities, they will utilize cloud services like public cloud, confidential cloud, and business cloud [9].

Distributed computing is generally utilized in various applications that create a lot of information and can endure delays. In spite of the way that cloud services are utilized in various spaces, not many applications demand continuous information examination and significant bits of knowledge immediately. We can't involve the cloud for these sorts of utilizations for the accompanying reasons.

- These days, numerous applications require next to no start to finish delay and an extremely quick reaction.
- Networks are regularly temperamental, and solid associations are just accessible in a couple of areas; in any case, distributed computing requires areas of strength for a to communicate and get information to and from the cloud.
- Information is put away, handled, and recovered from the cloud, bringing about expanded network dormancy.
- Information created by sensors is sent to the cloud through the web by means of various networking parts. Information hacking is more probable, so information protection and security are compromised.

2. LITERATURE REVIEW

In this segment, we examine past examinations on edge computing that endeavored to address a portion of the recently referenced edge computing difficulties. Since distributed computing performs more awful than edge computing because of its unified nature in handling, stockpiling, and security, which is brought about by the mists' separation from IoT clients and the chance of information robbery en route to the mists, distributed computing performs more awful than edge computing.

IoT edge gadgets take care of issues related with cloud engineering centralization; by carrying distributed computing abilities to neighborhood gadgets, IoT edge computing can handle information quicker in certifiable situations where reaction time is a fundamental prerequisite for the majority of these applications.

Iot and Edge Computing Architecture

This segment centers around edge computing structures as well as edge computing-based IoT gadgets and innovations. While the capacities and services of these gadgets fluctuate, there are a few key highlights that recognize these frameworks [10].

Complex occasion handling, man-made reasoning models, disconnected help, information the board, and their different applications are undeniably included. A key component of the up and coming age of IoT edge gadgets ought to be the capacity to quickly change gadget designs through remote devices, as well as expanded security in packet and update transmission, among different capacities [11].

The second level of this engineering is the edge server stage, which can be a passageway for network assets like capacity and calculation; it is found near a requesting IoT client, bringing about diminished dormancy and further developed load handling. The third level is the framework based cloud, where most of information handling and calculation happens, and

all produced information by IoT gadgets and sensors is put away and can be gotten to practically or online by some other gadget of any level.

3. METHODOLOGY

3.1 Data Fusion and Security Data Analysis for IoT

Sensor hubs in IoT applications communicate information to cloud server farms through network entryways and edge servers. Sensor-gathered unstructured information and spatiotemporal stream information can affect server farm handling rate and dynamic way of behaving, possibly causing transmission capacity bottlenecks, idleness, and throughput debasement for time-basic and dormancy delicate applications. Unreasonable excess information causes packet misfortune, longer deferrals, and network blockage. All the while, a solitary incorporated data set arrangement is regularly lacking for complex IoT frameworks, so we are thinking about coordinating the circulated construction of block bind and IoT to give secure huge information investigation services. This segment talks about our proposed information combination technique and information security methodology for dispensing with repetitive information and giving secure and viable information examination services for IoT applications [12].

3.2 IoT Framework Integrating Edge Computing and Block chain

Assuming that information gathered by the IoT application layer is communicated straightforwardly or through the edge to the cloud layer, it might cause blockage and huge deferral at the cloud administration layer. Accordingly, we incorporate information combination at the hubs for advancement. Confidential information, like power utilization information in brilliant networks, clinical and wellbeing information, and other confidential information that ought not be leaked, are much of the time engaged with IoT. All the while, the IoT network requires continuous observing, anticipating, and different services, for example, traffic determining, alarms, etc, and the information should regularly be handled locally. Given the previous, in our model, edge hubs will perform neighborhood model preparation on the information to safeguard the information's protection. Subsequent to communicating the nearby model boundaries to the cloud server, the cloud server will prepare the worldwide model and return it to the edge hub. The edge hub will utilize the cloud server's information examination results or model boundaries to handle the information so as to meet the IoT network's practicality. Simultaneously, the proposed design utilizes block chain to check the consistency and legitimacy of neighborhood information and cloud information transmission to forestall harming attacks. Figure 1 portrays the general design of this paper [13].

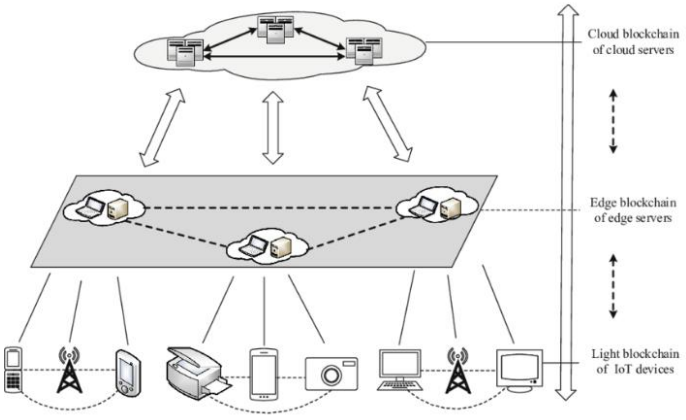

Fig.1. Overall framework

4. EXPERIMENTAL RESULTS

In view of trial measurements, we assess the proficiency of our proposed lightweight information combination and the adequacy of the progressive fuzzy hashing security methodology in this segment.

Information Combination Calculation Test. For information combination, we perform information combination at the hub level. We utilize the information gathered by the Intel Berkeley Exploration Lab to test the information combination calculations' exhibition and combination rate [14].

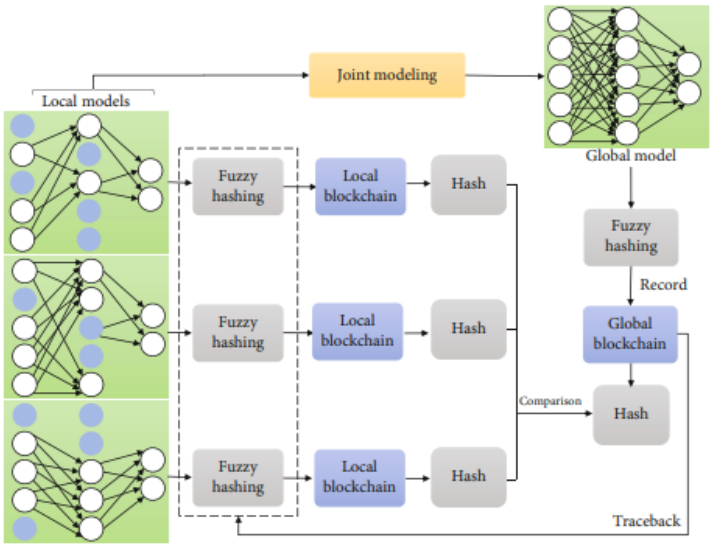

Fig 2. Dispersed abnormality discovery and restriction calculation joined with block chain. (1) The hub thinks about the hash worth of the nearby chain to the hash worth of the worldwide chain to see whether there is an irregularity. (2) After the irregularity happens, the hub finds the inconsistency by looking at the nearby model's fuzzy hashing worth to the worldwide chain's fuzzy hashing esteem.

We originally surveyed the lightweight combination calculation's capacity to catch information highlights. Involving temperature sensor information from a particular day for instance, we set the combination period to 60 minutes. Figure 2 portrays the information packets sent by our proposed lightweight information combination calculation at different combination records. As outlined in the figure 2, our proposed calculation essentially lessens the quantity of packets. Simultaneously, we found that our calculation can decrease the quantity of packets while keeping up with the information's attributes and quality. The consequences of our analyses show that our strategy diminishes information overt repetitiveness, packet crash likelihood, and network blockage [15].

TABLE I. WIRELESS COMMUNICATIONS AND MOBILE COMPUTING

	Time		
Temperature	Without data fusion	Data fusion with α	Data fusion with α
18.92	00:12	00:16	00:22
18.96	00:45	00:12	00:16
19.00	1:00	00:48	1:00
19.18	2:18	00:45	00:45
19.10	00:48	1:00	2:18
19.28	1:45	2:18	00:48

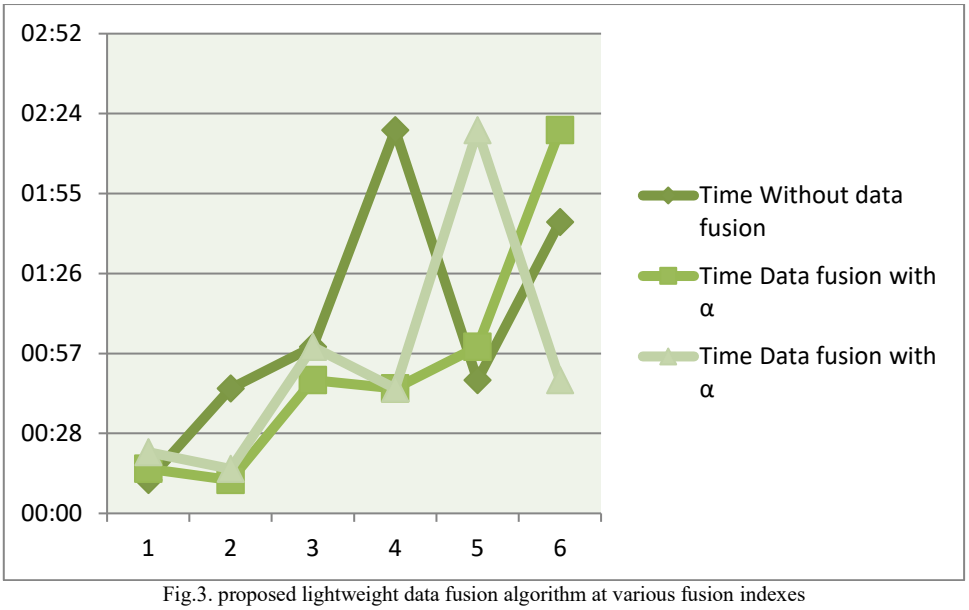

Fig.3. proposed lightweight data fusion algorithm at various fusion indexes

Our suggested progressive hash algorithm is thoroughly evaluated in this experiment, revealing its performance features. Firstly, we utilize a traditional, AI-free, and progressive fuzzy hashing-free method to evaluate the effectiveness of the hierarchical hash function on the blockchain architecture (edge nodes directly send all data to the cloud server for processing). In this section, we evaluate two models, both of which make use of data from the same sensor, to see which one performs better when it comes to a fuzzy hash. The paper and the method are compared to the proposed hierarchical approach. At the same time, we use the hub node as the verification node to increase the system's openness and efficiency. When the central node (cloud service) approves an operation, it is added to the global chain; in the meantime, every node on the periphery keeps its own chain and routinely transmits encrypted data to the cloud service. There are five nodes in the periphery and one server in the middle, in this experiment. If you look at Figure 3, you can see how the time to complete a task depends on the amount of processing blocks that node uses [16].

TABLE II. THE RELATIONSHIP BETWEEN A NODE'S NUMBER OF PROCESSING BLOCKS AND THE REQUIRED TIME

	Number of blocks		
Processing Time	Basic Method	Fizzy hashing	Hierarchical fuzzy hashing
0.04	5	16	33
0.05	10	20	18
0.08	18	25	28
0.10	45	30	35
0.15	17	10	40

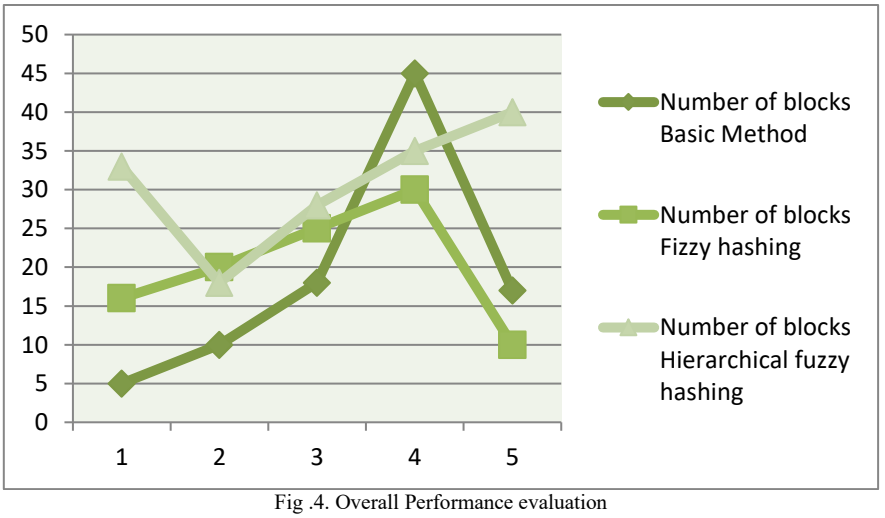

Fig .4. Overall Performance evaluation

Start to finish idleness was additionally estimated. We mimic the putting away and special case questions processes (as displayed in Figure 4). When contrasted with different techniques, our proposed various leveled fuzzy hashing calculation takes less opportunity to handle packets by and large. As represented in Figure 5, the various leveled fuzzy hashing proposed by us further develops the handling force of the block chain framework altogether [17].

TABLE III. PROCESSING POWER OF THE BLOCK CHAIN SYSTEM

Time Period	Store data time period			Search abnormal time period		
20	Basic method	Fuzzy hashing	Hierarchical fuzzy hashing	Basic method	Fuzzy hashing	Hierarchical fuzzy hashing
30	36	17	32	16	10	33
40	18	22	48	34	15	42
80	25	35	19	19	26	17

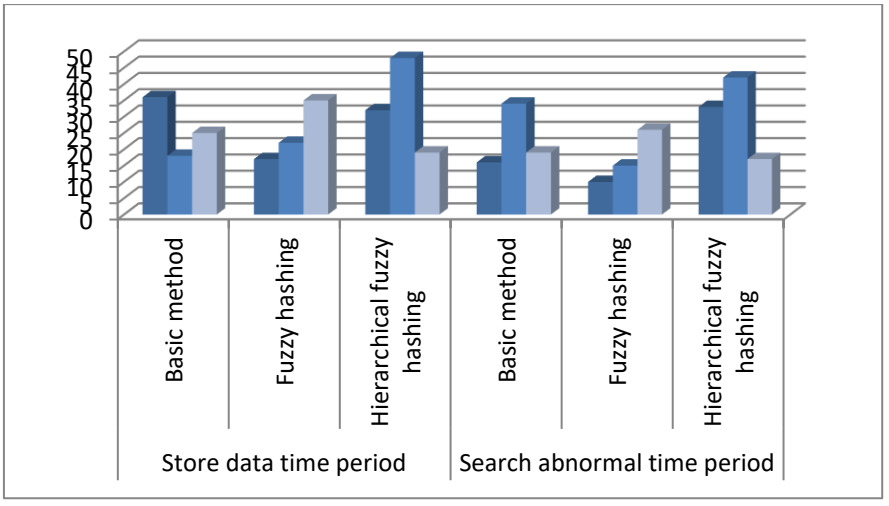

Fig.5. End to end delay testing

Above in information packets: At last, for the general examination, we run a similar trial on the above of information move packets. The's examination will probably look at the effect of our proposed information combination calculation and progressive hash capability on IoT information transmission above. In the instances of 5, 10, and 15 hubs, we determined the correlation of packet sizes communicated by edge hubs to cloud servers. The packet size handled by our technique is altogether more modest than the packet size before handling. The examinations above show that utilizing information combination, AI, and progressive fuzzy hashing can further develop IoT information investigation services by diminishing time and information volume while further developing information privacy and adaptation to non-critical failure [18-20].

5. CONCLUSION

We propose a technique to combine edge computing and blockchain to provide secure big data analysis and data fusion for IoT given the current scenario of rapid expansion in IoT data's scale and volume. Our method involves a node-level lightweight data fusion approach and a hierarchical fuzzy hashing algorithm to decrease IoT data transmission and guarantee data security. At the node level, we employ a lightweight data fusion approach to decrease data transfer. The edge node computes the local model to ease the burden on the cloud server, and the cloud node integrates the local model to enhance the model's representativeness. We employ blockchain and hierarchical fuzzy hashing to ensure consistency and validity while also maintaining data privacy for local and global models. Our experimental findings demonstrate that our technique significantly reduces IoT device data transmission while also enhancing system security. In the future, we aim to solve edge node load imbalance issues to maximize edge device utilization.

Funding

No financial grants or awards related to the research are disclosed in the paper.

Conflicts Of Interest

The author asserts that there are no conflicts of interest that could have affected the study design, methodology, or results.

Acknowledgment
The author acknowledges the research department at the institution for their assistance and technical expertise in conducting this study.

REFERENCES

[1] Z. Liu, W. Yan, W. Ding, and M. Atiquzzaman, "A Survey on Secure Data Analytics in Edge Computing," IEEE Internet of Things Journal, 2019.
[2] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.
[3] H. M. Saleh, A. K. Oleiwi, and A. A. H. Abed , Trans., “Detecting attacks in banks by cyber security: an applied study”, Babylonian Journal of Machine Learning, vol. 2023, pp. 65–72, Nov. 2023, doi: 10.58496/BJML/2023/011.
[4] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.
[5] C. Patel and N. Doshi, "Security Challenges in IoT Cyber World," in Security in Smart Cities: Models, Applications, and Challenges, Springer, 2019, pp. 171–191.
[6] X. He, J. Liu, R. Jin, and H. Dai, "Privacy-Aware Offloading in MobileEdge Computing," p. 6.
[7] S. Singh, "Optimize cloud computations using edge computing," in 2017 International Conference on Big Data, IoT and Data Science (BID), pp. 49-53, IEEE, 2017.
[8] A. S. . Abdulbaqi, A. M. . Salman, and S. B. . Tambe, “Privacy-Preserving Data Mining Techniques in Big Data: Balancing Security and Usability”, SHIFRA, vol. 2023, pp. 1–9, Jan. 2023, doi: 10.70470/SHIFRA/2023/001.
[9] J. H. Namdar and J. F. Yonan , Trans., “Revolutionizing IoT Security in the 5G Era with the Rise of AI-Powered Cybersecurity Solutions”, BJIoT, vol. 2023, pp. 85–91, Nov. 2023, doi: 10.58496/BJIoT/2023/011.
[10] H. El-Sayed et al., "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a distributed computing Environment," IEEE Access, vol. 6, pp. 1706-1717, December 2017.
[11] X. Hong et al., "Evidential fusion of sensor data for activity recognition in smart homes," Pervasive and Mobile Computing, vol. 5, no. 3, pp. 236–252, 2009.
[12] C. Song et al., "Edge intelligence based condition monitoring of beam pumping units under heavy noise in the industrial Internet of Things for Industry 4.0," IEEE Internet of Things Journal, p. 1, 2022.
[13] X. Chen, C. Song, and T. Wang, "Spatiotemporal analysis of line loss rate: a case study in China," Energy Reports, vol. 7, pp. 7048–7059, 2021.
[14] Y. Pan et al., "Performance degradation assessment of a wind turbine gearbox based on multi-sensor data fusion," Mechanism and Machine Theory, vol. 137, pp. 509–526, 2019.
[15] H. Lin et al., "Toward secure data fusion in industrial IoT using transfer learning," IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 7114–7122, 2021.
[16] Maryam Abdulsalam Ali and ALI ALQARAGHULI , Trans., “A Survey on the Significance of Artificial intelligence (AI) in Network cybersecurity”, BJN, vol. 2023, pp. 21–29, Apr. 2023, doi: 10.58496/BJN/2023/004.
[17] W. Shang et al., "Research on industrial control anomaly detection based on FCM and SVM," in 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering, pp. 218–222, New York, NY, USA, Aug. 2018.
[18] M. Burhanuddin, “Secure and Scalable Quantum Cryptographic Algorithms for Next-Generation Computer Networks”, KHWARIZMIA, vol. 2023, pp. 95–102, Jul. 2023, doi: 10.70470/KHWARIZMIA/2023/009.
[19] S. Shivam, B. Bhushan, and M. Ahad, "Blockchain based solutions to secure IoT: background, integration trends and a way forward," Journal of Network and Computer Applications, vol. 181, p. 103050, 2021.
[20] M. Asante et al., "Distributed ledger technologies in supply chain security management: a comprehensive survey," IEEE Transactions on Engineering Management, 2021.