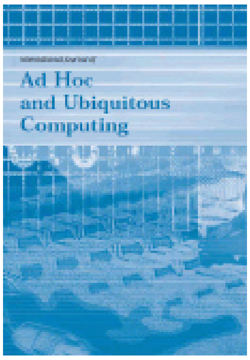


International Journal of Ad Hoc and Ubiquitous Computing

ISSN online: 1743-8233 - ISSN print: 1743-8225
https://www.inderscience.com/ijahuc

Data security enhancement in internet of things using optimised hashing algorithm

U. Arun Kumar, R. Prem Kumar, S.A. Siva Kumar, B. Maruthi Shankar, G. Mahendran

DOI: 10.1504/IJAHUC.2023.10053339

Article History:

Received:	07 August 2022
Accepted:	28 November 2022
Published online:	18 January 2024

Data security enhancement in internet of things using optimised hashing algorithm

U. Arun Kumar*

Department of EEE,
Faculty of Engineering,
Karpagam Academy of Higher Education (Deemed to be University),
Coimbatore, 641021, Tamil Nadu, India
Email: arun.udayakumarn@gmail.com
*Corresponding author

R. Prem Kumar

Department of EEE, Sri Eshwar College of Engineering,
Coimbatore, Tamilnadu, 641202 India
Email: premkumar.r@sece.ac.in

S.A. Siva Kumar

Department of ECE,
Dr. N.G.P Institute of Technology,
Coimbatore, Tamilnadu, 641048, India
Email: drsasivakumar@gmail.com

B. Maruthi Shankar

Department of Electronics and Communication Engineering,
Sri Krishna College of Engineering and Technology,
Coimbatore, Tamilnadu, 641008, India
Email: maruthishankar@gmail.com

G. Mahendran

St. Joseph University in Tanzania,
P.B. No. 11007, Plot No. 111@113,
Kibamba ‘B’, Dar Es Saalam, Tanzania
Email: gmrmahe@gmail.com

Abstract: The internet of things (IoT) has advanced quickly, providing customers with significant convenience in a variety of areas, including smart homes, smart transportation, and more. It might potentially pose security issues too. Significant security difficulties for the communications between such devices are brought on by the development of smart devices in IoT networks. As the IoT ecosystems develop, blockchain will become a platform for their security. Blockchain is a decentralised, distributed technology that may be able to address the IoT network security issues. Blockchain can address IoT restrictions on privacy and data protection. IoT is not a good fit for blockchain because of its high computing complexity, limited scalability, significant bandwidth overhead, and latency. This study develops an effective blockchain paradigm to address IoT requirements. Initially, the dataset is collected from the IoT sensors and pre-processed using the normalisation method. The pre-processed data is validated using smart contracts and stored in the blockchain network. Proof of work (PoW) consensus protocol is employed for the validation of the blocks. We propose an optimal key search fuzzy hashing algorithm (OKSFHA) for enhancing the security of the data. To optimise the security enhancement Spider monkey optimisation (SMO) is employed. The proposed algorithm is compared with traditional algorithms to prove the efficiency of the suggested system.

Keywords: internet of things; IoT; blockchain; smart contracts; proof of work; PoW; optimal key search fuzzy hashing algorithm; OKSFHA; spider monkey optimisation; SMO.

Reference to this paper should be made as follows: Kumar, U.A., Kumar, R.P., Kumar, S.A.S., Shankar, B.M. and Mahendran, G. (2024) ‘Data security enhancement in internet of things using optimised hashing algorithm’, *Int. J. Ad Hoc and Ubiquitous Computing,* Vol. 45, No. 1, pp.26–35.

Biographical notes: U. Arun Kumar received his PhD in Electrical Engineering in 2022. His area of research includes power quality improvement, BLDC motor drives, artificial intelligence, IoT, optical sensors and solar absorbers. He currently works as a Professor and Researcher at SRM Institute of Science and Technology, Ramapuram Campus, Chennai, India. He has published around 20 papers in well-reputed journals and conferences including, IEEE, Springer, Elsevier and MDPI. He has reviewed over 25 IEEE, Springer, and Elsevier articles. He served as an editorial board and advisory committee member in various IEEE international and national conferences.

R. Prem Kumar is working as an Assistant Professor in the Department of EEE at Sri Eshwar College of Engineering, Coimbatore. He has completed his Doctorate from Anna University, Chennai and his areas of interest are control systems, IoT and renewable energy systems.

S.A. Siva Kumar is working as an Associate Professor in the Department of ECE at Dr. N.G.P. Institute of Technology, Coimbatore. He has completed his Doctorate from Anna University, Chennai and his areas of interest are embedded systems and low-power VLSI design.

B. Maruthi Shankar is working as an Associate Professor in the Department of ECE at Sri Krishna College of Engineering and Technology, Coimbatore. He has completed his Doctorate from Anna University, Chennai. His areas of interest are embedded systems and low-power VLSI design.

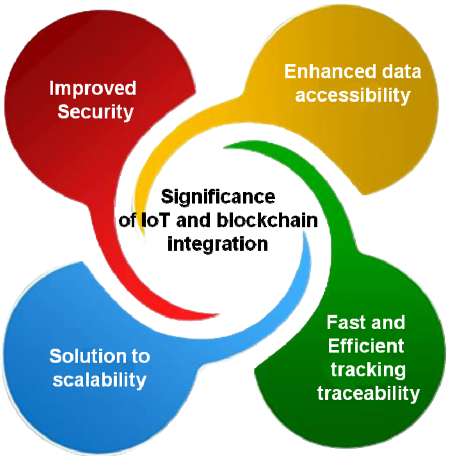
G. Mahendran received his BE degree in Electrical and Electronics Engineering from Bharathiar University in 1999, ME degree in Power Electronics and drives from Anna University, Coimbatore, India in 2011 and PhD in Radial Distribution System Optimisation from Anna University, Chennai, India in 2021. Currently, he is working as an Associate Professor and Head in the Department of Electrical and Electronics Engineering at Kathir College of Engineering, Coimbatore, India. His research interests are distribution system optimisation and renewable energy systems.

1 Introduction

Due to the development of several applications, data has grown significantly over the past few years. These data must be protected and kept in safe zones. Its importance is increased by the technology’s advancement. Data security has emerged as a key challenge in the modern world as a result of the growth of networks (Thabit et al., 2021a). Consequently, data security from hackers often becomes crucial to maintain its safety, data protection, preservation, security, and handling processes. Data security measures are used to maintain the safety of the data collected through the study of internet security status (Xu et al., 2022). Currently, with the widespread adoption of the internet of things (IoT), technology is being constructed. The key considerations are privacy and security. Applications for data security that are IoT-centric are subject to specific security risks since they are prone to security problems (Duraisamy et al., 2021). Although it is specifically adapted to the modern world, blockchain technology (BCT) is becoming more and more appealing to the younger generation. The IoT can also benefit from the use of BCT. Cloud applications have advanced significantly as a result of IoT technology improvement in a lot of fields. For maintaining and exchanging data and network processes, the blockchain idea needs a decentralised technology platform (Singh et al., 2021). Even while researcher innovation, invisibility, improved capacity, and improved security are all advantages of blockchain, its unchanging nature is the primary factor that makes it the perfect fit. Blockchain may be utilised as a crucial innovation to do away with the need for a trustworthy third-party vendor in networks that are connected because of how it is disseminated. Other good blockchain systems that may be used for implementation are Cloud hosting Technology, IBM Blockchain, Ethereum, Ripple, R3 Corda, and multichain (Patil et al., 2021). IoT platform is used to expand the available bandwidth. Due to very constrained network, computation, and memory capacity, IoT devices like smartphone devices are more susceptible to security attacks. Additionally, the existing platforms still have a problem with processing, analysing, and identifying trends in the data in vast volume of data generated by IoT devices to create a convenient environment (Shahbazi and Byun, 2021). A different method is therefore needed to guarantee data integrity, enhance data security and availability, and uncover hidden trajectories and valuable information to deliver acceptable products (Jamil et al., 2021). Machine-to-machine (M2M) data transmission access networks and inexpensive sensors are the two main components of the IoT. However, the data obtained by IoT sensors contain a lot of sensitive data and has to be protected.

For IoT applications, security and privacy are the two most important concerns, and both still present significant difficulties. Block chain's origin narrative explains a shared ledger that facilitates safe and irreversible transactions without the need for centralised authority and that can only be changed with the consent of all stakeholders. Multiple businesses, including the IoT, might be disrupted by such a scientific advancement. Information decentralisation makes it harder to interfere with information and creates a safe setting for IoT. Although centralised IoT ecosystems like clouds, hybrid, and network virtualisation have made safety breakthroughs, the security implications are still inadequate to overcome the difficulties (Omar and Goyal, 2022).

Figure 1 Significance of IoT and blockchain integration (see online version for colours)


Improved Security
Enhanced data accessibility
Significance of IoT and blockchain integration
Solution to scalability
Fast and Efficient tracking traceability

Remote monitoring in the healthcare industry is now feasible thanks to IoT-enabled devices, releasing the potential to keep patients safe and healthy and enabling doctors to provide excellent treatment. As doctor-patient interactions have gotten simpler and more effective, it has also raised patient participation and satisfaction. Additionally, remote patient monitoring shortens hospital stays and avoids readmissions by keeping an eye on patients' health. IoT has a huge influence on lowering healthcare expenses and enhancing patient outcomes. Without a question, IoT is revolutionising the healthcare sector by changing how devices and people interact while providing healthcare solutions. Applications of IoT in healthcare are advantageous to patients, families, doctors, hospitals, and insurance providers.

We propose an optimal key search fuzzy hashing algorithm (OKSFHA) for data security enhancement in IoT using integrated BCT. Figure 1 represents the significance of IoT and blockchain integration.

The remaining portion of this paper is briefly described as follows. Related works are provided in Section 2. In Section 3, the suggested technique is outlined and the performance of the system is analysed. Results and discussions are expanded in Section 4. The conclusion is in Section 5.

1.1 Problem statement

Scalability is a significant flaw in BCT, which is not invincible. Blockchains' freedom and transparency are drawbacks, and proof of work (PoW) is an unnecessary burden. Blockchain may be incredibly complicated. To overcome these limitations, we proposed an OKSFHA for data security enhancement in the IoT using integrated BCT.

2 Related works

Parthiban and Kumar (2022) proposed a concept that combines the hybrid gradient decent cuckoo search (HGDCS) algorithm for efficient regional cooperation with Blockchain systems to provide high standards of ethics and intrinsic security for sensitive information. This algorithm, however, also struggles to modify and produce the best relevant results, and its capacity to resolve complicated issues is constrained. Therefore, it struggles to perform effectively with separate and cross issues.

Adere (2022) analysed how BCT is being used to enhance security controls and how it is being integrated with IoT. The paper also shows the advantages of implementing blockchain in two subsets of the different systems, namely urban planning and medicine distribution networks, in addition to assessing the appearance of developments in emerging models. There is not enough efficiency to facilitate real-time transaction processing. Transactional and micro-transaction fees can affect the profitability of a business. Distributed ledger technology (DLT) renders obsolete conventional data processing systems. The environmental consequences of energy waste continue to be a major hurdle.

Attkan and Ranga (2022) examined current methods from the perspective of IoT security and discuss classic essential security techniques. Incorporating IoT with blockchain and AI-based authentication in cybersecurity, this technique also provides researchers with a thorough, high-quality investigation at an authenticated and predetermined time. The largest problem is technical complexity. Even simple system development changes require the hiring of software employees, coders, and data analysts by organisations. Many intricate details seem to be complicated to understand.

Gao et al. (2022) suggested BlockchainBot, a botnet concept that incorporated blockchain, also known as DLT, and used the IoT as maintainers. The BlockchainBot was able to completely launch bots. It was adaptable for a variety of botnet implementations and would have nothing to do with the need for neighbour lists (NL).

Kelli et al. (2021) provided a framework with a multi-layer tool for an extremely effective security mechanism adapted to the individual of eHealth, and a blockchain access control feature related to smart contracts to give dispersed access control for authorised parties to patient records and health information.

Aoun et al. (2021) aimed to broaden perspectives on BCT as a liberating instrument for the fourth industrial revolution. Additionally, the author focused on the principles of Industry 4.0, as well as its difficulties, restrictions, and obstacles. Lastly, Strong representation is looking into the ways that BCT may provide major updates and benefits to the implementation of Industry 4.0.

Qashlan et al. (2021) established a safe foundation for IoT devices in smart home systems and offer a hard concept that blends attribute-based access control with smart contracts and cloud technologies. By outsourcing time-consuming tasks simultaneously and aggregating data stored in the cloud securely and comfortably utilising a data hiding mechanism, the edge node increases the system's application performance.

Wang (2020) stated that IoT-powered miniature healthcare sensors can be used for diagnostic procedures and self-health monitoring. Additionally, it aids in rapid testing and therapy advice by doctors working in distant areas without having direct touch with the patients. The inconsistency of safety rules and authentication and authorisation has made it difficult to satisfy the security standards.

Singh et al. (2020) outlined all the privacy concerns and challenges that affect the use of BCT in smart city implementation. Additionally, it provides a thorough analysis of some crucial elements that will enable the fusion of blockchain with AI, resulting in a realisation of a smart society. Explain how to improve blockchain security while highlighting the fundamental ideas that may be applied to the creation of different blockchain-based, AI-based automated driving.

Barati and Rana (2019) implemented the general data protection regulation (GDPR), which gave consumers choice over their data collection and information about the equipment used to gather it. BCT enables IoT devices to have an audit trail that complies with GDPR. For transparent and automated data protection, it converts a collection of these principles into a consensus mechanism.

Faika et al. (2019) investigated the use of BCT to protect wireless battery management systems (WBMSs) that support the IoT against hostile cyberattacks.

Pundir et al. (2019) focused on the concept of the value of supplementary innovations, such as IoT and blockchain, for the full digitalisation of the distribution chain. The feasibility study of a provider that rents out pallets are used to illustrate that information technology is used to boost the effectiveness of its maintenance factor and financial services.

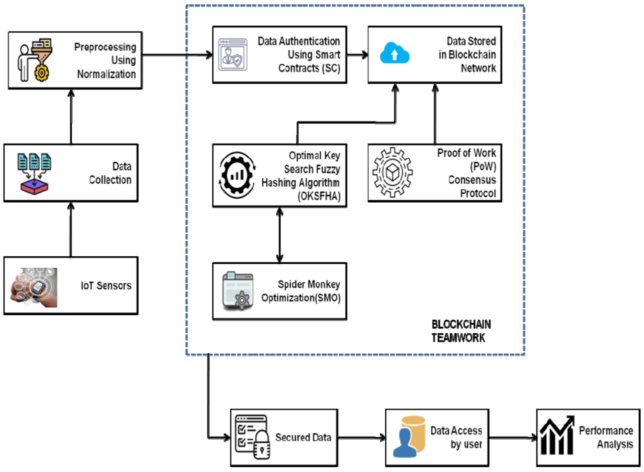
Khan et al. (2021) demonstrated whether the integration of IoT with BCT improves people's confidence, organisation, and finally the effectiveness of humanitarian logistics (HL). Most of the disaster prevention and mitigation stakeholders might benefit from it because they are desperately seeking ways to aid those in need. Transactive memory systems (TMS) theory viewpoints serve as its foundation.

To overcome the limitations in the existing works such as lack of processing time, poor performance, and inefficient energy consumption, We proposed the OKSFHA for enhancing the security of the databased on the IoT using integrated BCT. Enhancing data security maintains correct information. Access to potential growth or expansion plans must be restricted to preserve a technological edge. It lowers the potential expenses for upcoming advancement and maintenance in terms of code alterations.

3 Proposed methodology

IoT technology has significantly increased as a result of the explosion of expanding inventories in telecommunication and networking technologies. The network may be used to link multiple technologies, which has several benefits including file transfer, accessibility, and network monitoring. Blockchain is becoming more and more well-known because of its advantages, including its decentralised organisation, privacy, and also immutability. The key advantage of implementing a blockchain platform is that it is more secure in terms of innovation. Hence, in this paper, we proposed an OKSFHA for enhancing data security in IoT using integrated BCT. Figure 2 illustrates the suggested methodology's flow.

Figure 2 Flow of proposed methodology (see online version for colours)


Preprocessing Using Normalization
Data Authentication Using Smart Contracts (SC)
Data Stored in Blockchain Network
Data Collection
Optimal Key Search Fuzzy Hashing Algorithm (OKSFHA)
Proof of Work (PoW) Consensus Protocol
IoT Sensors
Spider Monkey Optimization(SMO)
BLOCKCHAIN TEAMWORK
Secured Data
Data Access by user
Performance Analysis

3.1 Data collection

IoT Sensors is a commercial data collection created with economics in consideration. The data collection incorporates precision agricultural data, including temperature and precipitation values from 41 locations over 15 minutes. The attribute list inside the dataset includes aspects like location-based, the dates, the moment, and the sun's angle, how much rain fell, the weather, moisture, air velocity, air movement, and oxygen content. The data collection comprises a total of 873 344 recordings (Lohiya and Thakkar, 2020; Alqahtani et al., 2022) that were gathered from sampling points throughout the globe (Lohiya and Thakkar (2020).

3.2 *Data processing*

Normalisation is designed to assure that certain data strongly associated with the data security are included, that always one data item is present in each data field, and to eliminate duplicate and unnecessary data. The attribute values are scaled throughout this method to keep them in a certain range. Although there are many different normalising methods, min-max normalisation is the one used in this case. Then the normalisation is written as

$$n = \left(\left(\frac{(a - a_{min})}{a_{max} - a_{min}} \right) * (1 - 0) + 0 \right) \tag{1}$$

where n represents normalisation, a_{max} and a_{min} represents maximum and minimum values of normalised data and the range is from 0 to 1. The measured and calculated values of the attribute are used to depict its mean and median values. While previously described as the inequality of a dataset's range, minimal skewness denotes normally distributed data. Hence mean, median and skewness are depicted in equation (2), (3), and (4).

$$M = \frac{\sum_{i-1}^{n} y_1}{n} \tag{2}$$

$$M_d = \begin{cases} y\dfrac{n}{2}, & if \;\; n \; is \; even \\ \dfrac{\left(y\left[\dfrac{(n-1)}{2}\right] + y\left[\dfrac{(n-1)}{2}\right] \right)}{2}, & | if \;\; n \; is \; odd \end{cases} \tag{3}$$

$$S_k = \frac{n\sum_{i=1}^{n} (y_i - \overline{y})^3}{(n-1)(n-2)\sigma^3} \tag{4}$$

where '*n*' depicts the number of values in the dataset, y depicts the values of the dataset. Furthermore, $\overline{y}$ represents the mean value and σ depicts the standard deviation. The technique of security normalisation involves locating and compiling all relevant data related to security. For many abnormalities detection processes, attributes in normalisation are crucial.

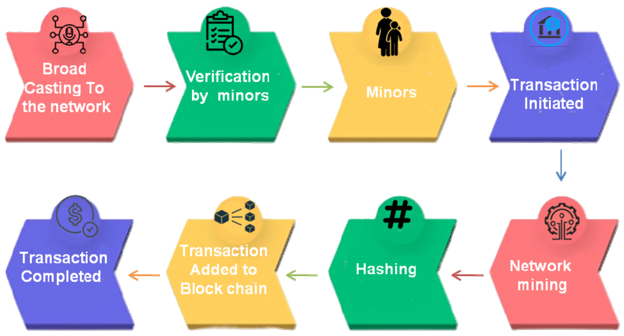
3.3 *Data authentication using smart contracts*

On the blockchain, smart contracts are software programs running on their own. The primary intended applications necessitate that systems accept data from sources other than the blockchain. Therefore, reliable data sources that can accommodate a variety of information requirements will be essential to smart contract ecosystems. SC is symbolised by a contract account that contains code, a money balance, and permanent storage inside the pattern of a key store. Messages are accepted as input data to any of the specified functions by a contract. A message from some other contract or a transaction from an account that is not a contract triggers the execution of the contract code. Thus, a transaction always catalyses contract execution. An automated creature on the blockchain may be considered a smart contract. Hence data stored in the blockchain networks are accessed only by the smart contracts during authentication.

3.4 *Consensus protocol using proof-of-work*

One of the most widely used consensus protocols is proof-of-work (PoW). To locate a node that complies with the consensus protocol, PoW has to perform a substantial amount of computing power. The PoW's privacy works on the assumption that there is no cash benefit to using a significant portion of the computational resources and power production to the blockchain. Collecting data power is needed for the PoW calculation, but it can only do certain computations, often hash functions. Since there are more resource-effective protocols available, PoW is a resource-guzzling protocol that consumes a significant amount of processing power. Due to its high computation requirements, it also provides strong data security. Considering the computational complexity level of the protocol, a hostile user would need to control more than 50% of the processing power, which is very possible. The protocol is quite sensitive to some attacks. Figure 3 illustrates the working protocol of PoW.

Figure 3 Working of PoW (see online version for colours)



3.5 *Optimal key search fuzzy hashing algorithm*

Hashing algorithms are well-known techniques for converting arbitrary big inputs into bit strings of a predetermined length that act as distinct input patterns. Through linking similar information as associated binary codes, hashing effectively retrieves the information from scattered clouds when optimisation and fuzzy logic are applied to acquire the necessary details. For enhancing the data security in the IoT by utilising integrated BCT we proposed an OKSFHA. To increase the security of the data and the recovery effectiveness in dispersed cloud environments, data retrieval is systematically improved. Fuzzy development information, which is articulated as fuzzification, is something that gives the OKSFHA implementation its logical basis. In a simultaneous process, this combination improves retrieval accuracy by learning data security and prediction accuracy through fuzzy systems. The fuzzy hashing algorithm can locate comparable files and generate a similarity measure that is reported as a proportion of its similarity. Utilising the proposed algorithm establishes the connection between the data source and the request, which saves memory, and the training procedure needs to be effective. The OKSFHA is described using mathematical formulation.

Let us consider that the query consists of ϑ initial details and that the requisite hash codes are created and linked for the query within the limit of m-bit binary codes.

$$\varphi: \vartheta \rightarrow \{+1,-1\}^{m} \tag{5}$$

Let ϑ_1, ϑ_2 and ϑ_3 are the pairs of the query ϑ and the corresponding hash codes are $\lambda_1\ \lambda_2\ \lambda_3 \in \{+1, -1, +1\}^m$, and the loss function is given by

$$\begin{aligned} L_F(\lambda_1, \lambda_2, \lambda_3, c) &= \frac{1}{2}(1-c)\ h_d \\ &+ \frac{1}{2}c_{max}\left(m - h_d(\lambda_1, \lambda_2, \lambda_3), 0\right) \end{aligned} \tag{6}$$

where h_d is the hamming distance and c is the class which is 0 for the same class and 1 for a different class. If the hamming distance is close to the margin, as determined by the target function, the loss function will be greater. Those combinations that are different are permitted by such an inverse proportional requirement, preventing collision in the loss function. Hence, for the training datasets, the net loss function will be shown as in equation (7)

$$LF = \sum_{m-1}^{N} L(\lambda_{m1}, \lambda_{m2}, \lambda_{m3}, c_m) \tag{7}$$

This article provides an improved blockchain-based IoT for data security that uses the optimal key search fuzzy hashing technique to protect the data. By applying an optimum key search fuzzy hashing methodology, it is possible to find and potentially maintain documents. Data is safeguarded and security is improved by utilising OKSFHA to compare files to every node in the blockchain network. The suggested approach is used in securing data to detect file tampering during assessing the consistency and resemblance of data value. The data value is divided into smaller parts, with a hash function being calculated for each part. The last step is the summation of all parts of the hash function to get the fuzzy hash value to increase security. The proposed OKSFHA is used for enhancing data security in IoT using BCT.

3.6 Spider monkey optimisation

A worldwide efficient method called Spider Monkey optimisation (SMO) has been motivated by the fission-fusion economic group of spider monkeys during habitat activity. Typically, a group of up to 60 spider monkeys coincides. In a region, a commander divides out the duty of foraging for food. In cases of food scarcity, a female often serves as the group's global leader and divides the population into changeable smaller units. The number of people in the group depends on where they can get their meals. The size is closely related to the quantity of food on hand. The process for enhancing data security is analysed by the SMO. The data is first acquired for secure authentication, and then it is separated into smaller groups by the techniques. The task of creating smaller groups is given to the leader. Data security is handled by small groups.

3.6.1 Initialisation of data

SMO constantly distributes the data of m members (sm_d). Where d = 1, 2, 3 m and sm_d represent the d^{th} member of data. SMO initiated each sm_d as given in equation (8)

$$sm_{ds} = sm_{lows} + RN(0,1)\times\left(sm_{highs} - sm_{lows}\right) \tag{8}$$

where sm_{ds} is the s^{th} dimension of the d^{th} sm

sm_{lows} and sm_{highs} are maximum and minimum limits.

3.6.2 Local leader group

In LLG, the sm shifts its present location by capturing the experiences of the localised members of the group and the local representative in the earlier. The local leader group is represented in equation (9)

$$\begin{aligned} sm_{newds} &= sm_{ds} + RN(0,1)\times(lg_{ls} - sm_{ds}) \\ &+ RN(-1,1)\times sm_{rs} - sm_{ds} \end{aligned} \tag{9}$$

where lg_{ls} depicts the l^{th} local group location of the leader

sm_{rs} Shows that randomly selected s^{th} location in leader group hence, $r \neq d$

3.6.3 Global leader group

GLG is used to find the location of all members. It is processed after LLG. GLG equation is given by

$$\begin{aligned} sm_{newds} &= sm_{ds} + RN(0,1)\times(gg_{ls} - sm_{ds}) \\ &+ RN(-1,1)\times(sm_{rs} - sm_{ds}) \end{aligned} \tag{10}$$

where gg_{ls} Shows the location of the global leader.

Then the fitness of probability for data security in terms of SMO is represented in equation (11)

$$P_{ds} = \frac{F_d}{\sum_{d=1}^{N} F_d} \tag{11}$$

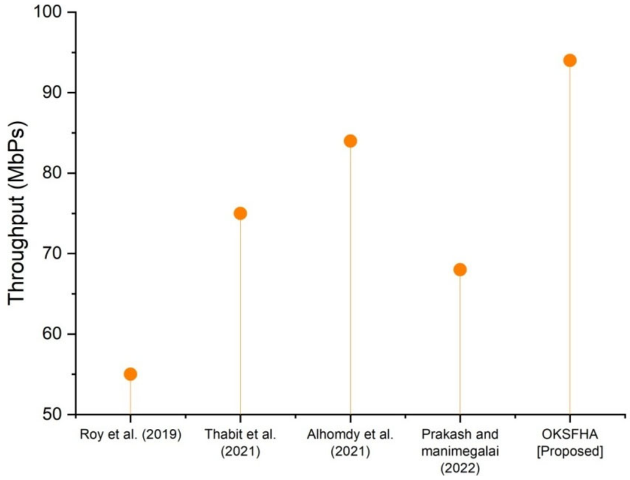
where, F_d is the probability of fitness for data security.

By using the SMO the data is more secured. The user cannot access the optimised data until it has been secured and sent to a computing unit for safe and secure processing and transfer. After securing the data, the user has permission to access it for further process. Data access allows for moving data across the system using a request process until the desired data is found. Until the necessary data is located, each section of data must be retrieved one at a time. Then the performance of the proposed system is carried out.

4 Results and discussion

The proposed method is used for data security enhancement using optimisation techniques. Normalisation is applied for preprocessing technique. OKSFHA is proposed for data security and SMO is applied for the secured data effectively. Hence, the performance analysis is carried out in this section. Throughput, end-to-end delay, energy consumption, latency, accuracy, precision, and recall are the metrics analysed by the proposed system and compare with the existing approaches. The existing techniques are Roy et al. (2019) introduce DNA encryption for data security, Thabit et al. (2021) proposed a genetic algorithm, Alhomdy et al. (2021) suggested a lightweight cryptographic algorithm for enhancing data security and Prakash and Manimegalai (2022) examined RTL algorithm for data security enhancement. These existing techniques are compared with our proposed OKSFHA to get effective data security enhancement.

Figure 4 Comparison analysis of throughput (see online version for colours)



Throughput is the quantity of data that is successfully transmitted from the sender to the recipient. Additionally, throughput has increased as a result of decreased inefficiency driven forward by PoW. Figure 4 displays a throughput comparison using other techniques. The suggested model has a higher throughput than the alternatives.

The phrase end-to-end delay describes a method from beginning to end delay. It measures how long a packet needs to travel from its sender to the recipient. The proposed algorithm has less end-to-end delay compared to the existing techniques. The end-to-end delay is calculated by the following equation

$$E2E_{delay} = (processing\ time) + (transmission\ time) + (queuing\ time) \qquad (12)$$

End-to-end delay is defined as the summation of overall time such as processing time, transmission time, and queuing time.

Figure 5 Comparison analysis of end-to-end delay (see online version for colours)

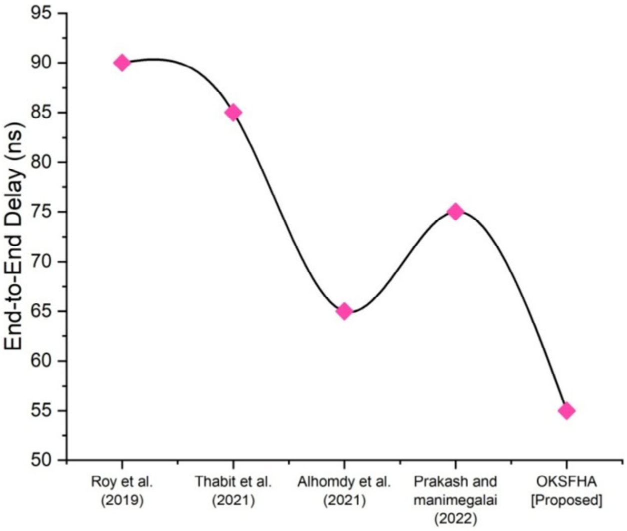


Figure 6 Comparison of energy consumption (see online version for colours)

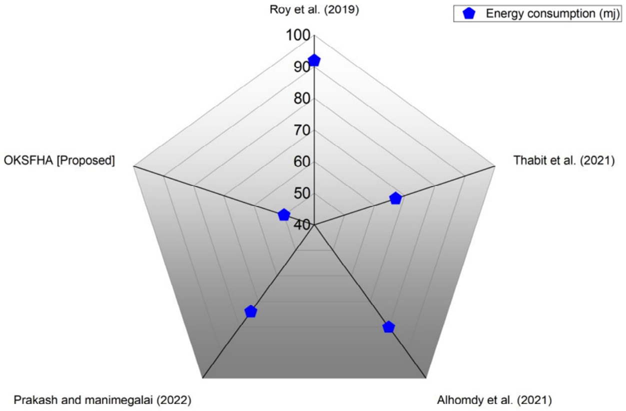


Figure 7 Comparison of latency (see online version for colours)

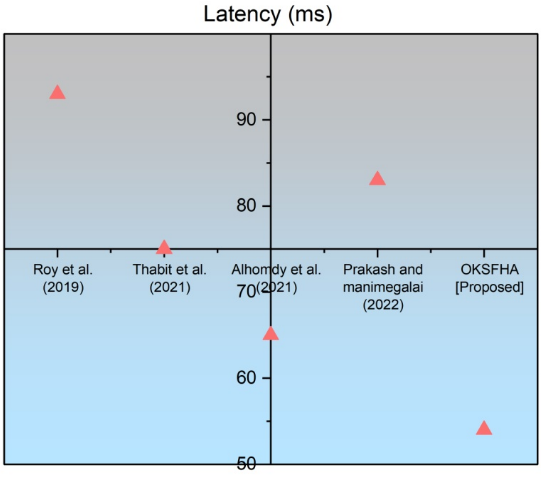


Figure 6 shows a comparison of energy. It speaks of the quantity of energy used to improve the data security procedure. The proposed work is quicker to process and operates more effectively. As a result, the energy usage is low when compared to other methods currently in use.

The proposed method's delay is illustrated in Figure 7. An execution or process's latency is its length of time. When compared to other algorithms that are already in use, the suggested algorithm's execution time is quite short. Thus, it appears that the suggested work is quite better than other systems.

Figure 8 Comparison of accuracy (see online version for colours)

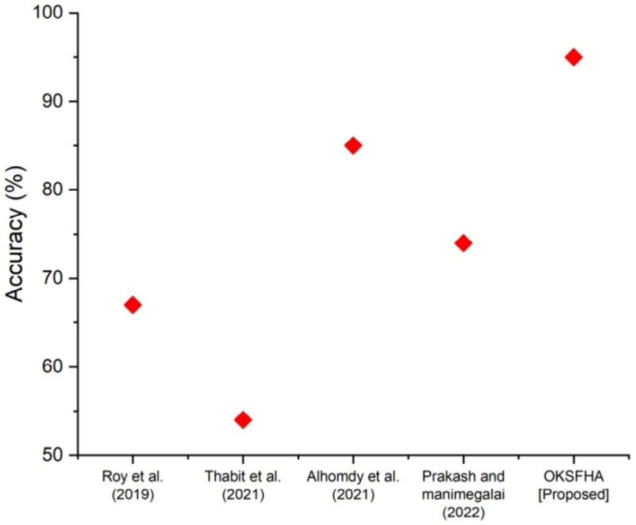
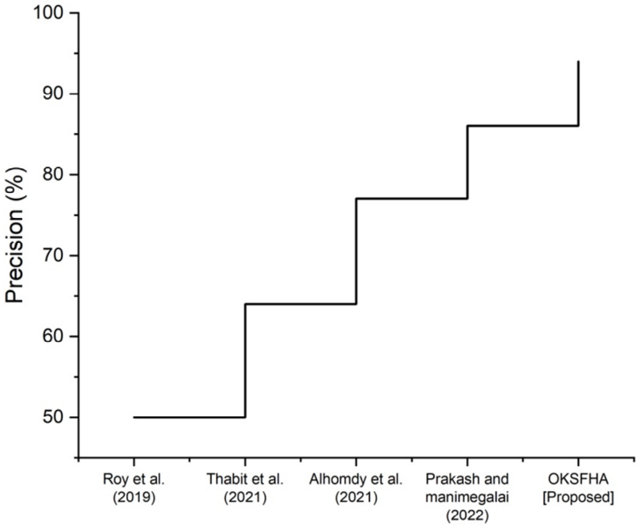


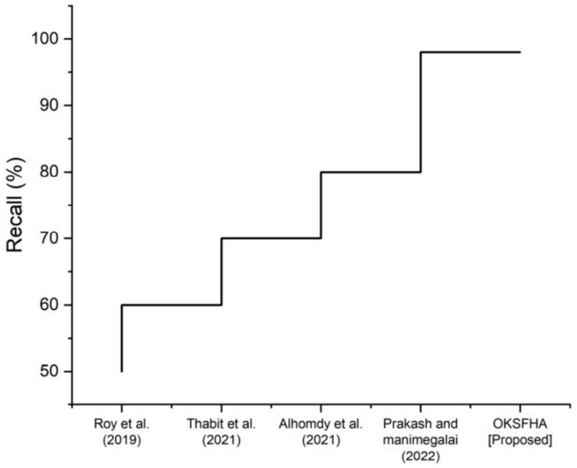
Figure 9 Comparison of precision



The comparison analysis of accuracy is shown in Figure 8. For the level of effective system performance, accuracy is tested. The suggested method has significantly high accuracy. Accuracy is a crucial factor to take into account when assessing a suggested method's efficacy. The accuracy range of the recommended model, which is higher than earlier techniques aimed at improving data security, has been determined to be superior, at 95%. The suggested approach is therefore more effective than the current algorithm.

In Figure 9, a comparison of accuracy is shown. Precision is the degree to which two or more observations are within a certain distance of one another. Comparing the suggested approach to current methods, precision is improved.

Figure 10 Comparison of recall



The recall comparison of the suggested and existing approaches is shown in Figure 10. Recall assesses a system's capacity to identify data samples. The most significant algorithm is that presented, as evidenced by the highest recall.

5 Discussion

The OKSFHA is proposed in this article for enhancing the data security in IoT using a blockchain mechanism. Data are attacked by third parties hence BCT is used to secure data from other parties. IoT makes it possible for internet-connected devices to submit data to local blockchain systems to produce impenetrable data for secured transactions. Due to weaknesses in the DNA passcode, inadequate advancement of DNA computation, and technical challenges, Roy et al. (2019) flopped. As a result, Thabit et al. (2021) struggled to secure data because of the significant expense of processing the Genetic Algorithm. Due to lightweight cryptography's decreased security; Alhomdy et al. (2021) failed. The failure of Prakash and Manimegalai (2022) is because of its significant power dissipation. To overcome these disadvantages, we have suggested OKSFHA for IoT using blockchain to increase security and improve energy efficiency by utilising the power of blockchain. We combined the two effective technologies, blockchain and the IoT, and made use of their possible advantages for effective decision-making, data protection, and improved power management. An optimisation method for IoT with blockchain integration was introduced. This technique significantly decreases transmission delay, increases transmission speeds, and preserves a lot of energy. Additional testing has revealed that the suggested model performs better for enhancing data security than both the standard blockchain technique and the existing routing protocols.

6 Conclusions

The research presents an optimal key search fuzzy hashing technique for dispersed IoT environments in data security. The suggested model is created to attain high data security effectiveness and precision while taking into account the problems in traditional data security systems. Hashing algorithm combined with IoT and blockchain integration enhances data security management. The proposed model's security efficiency of 98% is thought to be a notable increase in data security solutions. The suggested work is efficient in handling a broad variety of characteristics. Future directions for the research include employing other approaches to minimise the sum of restrictions in the OKSFHA.

Acknowledgements

All authors contributed to the study conception and design. Arun Kumar U and Prem Kumar R have done the analysis of the article. Siva Kumar S A and Maruthi Shankar have experienced the results with proper optimisation. Mahendran G has validated the complete work. Arun Kumar U prepared the first draft of the manuscript. All authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

Adere, E.M. (2022) 'Blockchain in healthcare and IoT: a systematic literature review', *Array*, p.100139.

Alhomdy S., Thabit, F., Al-Ahdal, A.H. and Jagtap, S. (2021) 'A new lightweight cryptographic algorithm for enhancing data security in cloud computing', *Global Transitions Proceedings*, Vol. 2, No. 1, pp.91–99.

Alqahtani, A.S., Mubarakali, A., Parthasarathy, P. et al. (2022) 'Solar PV fed brushless drive with optical encoder for agriculture applications using IoT and FPGA', *Opt. Quant Electron.,* Vol. 54, p.715, https://doi.org/10.1007/s11082-022-04065-0.

Aoun, A., Ilinca, A., Ghandour, M. and Ibrahim, H. (2021) 'A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology', *Computers and Industrial Engineering*, Vol. 162, p.107746.

Attkan, A. and Ranga, V. (2022) 'Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security', *Complex and Intelligent Systems*, pp.1–33.

Barati, M. and Rana, O. (2019) 'Enhancing user privacy in IoT: Integration of GDPR and blockchain', in *International Conference on Blockchain and Trustworthy Systems*, Springer, Singapore, December, pp.322–335.

Duraisamy, A., Subramaniam, M. and Robin, C.R.R. (2021) 'An optimized deep learning-based security enhancement and attack detection on IoT using IDS and KH-AES for smart cities', *Stud. Inf. Control*, Vol. 30, No. 2, pp.121–131.

Faika, T., Kim, T., Ochoa, J., Khan, M., Park, S.W. and Leung, C.S. (2019) 'A blockchain-based Internet of Things (IoT) network for security-enhanced wireless battery management systems', in *2019 IEEE Industry Applications Society Annual Meeting,* IEEE, September, pp.1–6.

Gao, H., Li, L., Chang, X., Wan, J., Li, J., Du, J. and Zhang, X. (2022) 'BlockchainBot: a novel botnet infrastructure enhanced by blockchain technology and IoT', *Electronics*, Vol. 11, No. 7, p.1065.

Jamil, F., Kahng, H.K., Kim, S. and Kim, D.H. (2021) 'Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms', *Sensors*, Vol. 21, No. 5, p.1640.

Kelli, V., Sarigiannidis, P., Argyriou, V., Lagkas, T. and Vitsas, V. (2021) 'A cyber resilience framework for NG-IoT healthcare using machine learning and blockchain', in *ICC 2021-IEEE International Conference on Communications*, IEEE, June, pp.1–6.

Khan, M., Imtiaz, S., Parvaiz, G.S., Hussain, A. and Bae, J. (2021) 'Integration of internet-of-things with blockchain technology to enhance humanitarian logistics performance', *IEEE Access*, Vol. 9, pp.25422–25436.

Lohiya, R. and Thakkar, A. (2020) 'Application domains, evaluation datasets, and research challenges of IoT: a systematic review', *IEEE Internet of Things Journal*, Vol. 8, No. 11, pp.8774–8798.

Omar, Y.A. and Goyal, S.B. (2022) 'Blockchain for Enhancing Security of IoT Devices', in *Internet of Things*, Springer, Singapore, pp.235–270.

Parthiban, R. and Kumar, K.S. (2022) 'Effective resource scheduling using hybrid gradient descent cuckoo search algorithm and security enhancement in cloud via blockchain for healthcare 4.0', *Materials Today: Proceedings*, Vol. 56, pp.1802–1808.

Patil, P., Sangeetha, M. and Bhaskar, V. (2021) 'Blockchain for IoT access control, security and privacy: a review', *Wireless Personal Communications*, Vol. 117, No. 3, pp.1815–1834.

Prakash, V. and Manimegalai, C.T. (2022) 'Data security using RTL algorithm with chaos synchronization for VLC system', *Journal of Optics*, pp.1–9.

Pundir, A.K., Jagannath, J.D., Chakraborty, M. and Ganpathy, L. (2019) 'Technology integration for improved performance: a case study in digitization of supply chain with integration of internet of things and blockchain technology', in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, January, pp.170–176.

Qashlan, A., Nanda, P., He, X. and Mohanty, M. (2021) 'Privacy-preserving mechanism in smart home using blockchain', *IEEE Access*, Vol. 9, pp.103651–103669.

Roy, M., Chakraborty, S., Mali, K., Swarnakar, R., Ghosh, K., Banerjee, A. and Chatterjee, S. (2019) 'Data security techniques based on DNA encryption', in *International Ethical Hacking Conference*, Springer, Singapore, August, pp.239–249.

Shahbazi, Z. and Byun, Y.C. (2021) 'Integration of Blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing', *Sensors*, Vol. 21, No. 4, p.1467.

Singh, S., Hosen, A.S. and Yoon, B. (2021) 'Blockchain security attacks, challenges, and solutions for the future distributed IoT network', *IEEE Access*, Vol. 9, pp.13938–13959.

Singh, S., Sharma, P.K., Yoon, B., Shojafar, M., Cho, G.H. and Ra, I.H. (2020) 'Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city', *Sustainable Cities and Society*, Vol. 63, p.102364.

Thabit, F., Alhomdy, S. and Jagtap, S. (2021a) 'A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions', *International Journal of Intelligent Networks*, Vol. 2, pp.18–33.

Thabit, F., Alhomdy, S., Al-Ahdal, A.H. and Jagtap, S. (2021b) 'A new lightweight cryptographic algorithm for enhancing data security in cloud computing', *Global Transitions Proceedings*, Vol. 2, No. 1, pp.91–99.

Wang, H. (2020) 'IoT based clinical sensor data management and transfer using blockchain technology', *Journal of ISMAC*, Vol. 2, No. 3, pp.154–159.

Xu, X., Li, S. and Zeng, J. (2022) 'Research on the data security enhancement method based on encryption paradigm', in *The proceedings of the 16th Annual Conference of China Electrotechnical Society*, Springer, Singapore, pp.1152–1158.