EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Leveraging AI and Blockchain for Privacy Preservation and Security in Fog Computing

S. B. Goyal[1,*], Anand Singh Rajawat[2], Manoj Kumar[3] and Prerna Agarwal[4]

[1]Faculty of Information Technology, City University, Petaling Jaya, 46100, Malaysia
[2]School of Computer Science & Engineering, Sandip University Nashik, India
[3]University of Wollongong, Dubai, UAE
[4]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, NCR, India

Abstract

INTRODUCTION: Cloud computing's offshoot, fog computing, moves crucial data storage, processing, and networking capabilities closer to the people who need them. There are certain advantages, such improved efficiency and lower latency, but there are also some major privacy and security concerns. For these reasons, this article presents a new paradigm for fog computing that makes use of blockchain and Artificial Intelligence (AI).
OBJECTIVES: The main goal of this research is to create and assess a thorough framework for fog computing that incorporates AI and blockchain technology. With an emphasis on protecting the privacy and integrity of data transactions and streamlining the management of massive amounts of data, this project seeks to improve the security and privacy of Industrial Internet of Things (IIoT) systems that are cloud-based.
METHODS: Social network analysis methods are utilised in this study. The efficiency and accuracy of data processing in fog computing are guaranteed by the application of artificial intelligence, most especially Support Vector Machine (SVM), due to its resilience in classification and regression tasks. The network's security and reliability are enhanced by incorporating blockchain technology, which creates a decentralised system that is tamper resistant. To make users' data more private, zero-knowledge proof techniques are used to confirm ownership of data without actually disclosing it.
RESULTS: When applied to fog computing data, the suggested approach achieves a remarkable classification accuracy of 99.8 percent. While the consensus decision-making process of the blockchain guarantees trustworthy and secure operations, the support vector machine (SVM) efficiently handles massive data analyses. Even in delicate situations, the zero-knowledge proof techniques manage to keep data private. When these technologies are integrated into the fog computing ecosystem, the chances of data breaches and illegal access are greatly reduced.
CONCLUSION: Fog computing, which combines AI with blockchain, offers a powerful answer to the privacy and security issues with cloud centric IIoT systems. Combining SVM with AI makes data processing more efficient, while blockchain's decentralised and immutable properties make it a strong security measure. Additional security for user privacy is provided via zero-knowledge proofs. Improving the privacy and security of fog computing networks has never been easier than with this novel method.

Keywords: Artificial Intelligence, Fog computing, Privacy Preservation Model, Cloud Computing

Received on 22 December 2023, accepted on 19 March 2024, published on 26 March 2024

doi: 10.4108/eetiot.5555

*Corresponding author. Email: drsbgoyal@gmail.com

1. Introduction

The fusion of Artificial Intelligence (AI) and blockchain technology in fog computing has emerged as an innovative and pioneering method to augment confidentiality and safeguarding in distributed computing environments. This introduction immerses itself in the symbiotic utilization of these technologies, accentuating the implementation of Support Vector Machines (SVM), consensus decision-making mechanisms, and zero-knowledge proofs. AI in Fog Computing: AI, particularly through the utilization of SVM, assumes a pivotal role in

fog computing by enabling astute decision-making at the periphery of the network. SVM, an algorithm for supervised machine learning, exhibits proficiency in categorizing and forecasting data patterns. In the realm of fog computing, SVM can be harnessed to scrutinize vast quantities of data generated by IoT devices, expediting real-time decision-making and the detection of anomalies. This elevates the system's capacity to promptly counter security threats, ensuring the integrity and secrecy of data. Blockchain for Augmented Security: Blockchain technology contributes significantly to the security facet of fog computing. By its very nature, blockchain is a decentralized and tamper evident ledger system. Its integration into fog computing environments guarantees that data transactions and exchanges are securely documented and immutable. This attribute proves particularly advantageous in upholding a transparent yet secure means of communication among numerous nodes within the fog network. Consensus Decision Making: Consensus decision-making, an integral component of blockchain technology, fortifies the security and dependability of the network. In fog computing, consensus algorithms empower nodes to concur on the validity of transactions or data without necessitating a central authority. This decentralized approach diminishes the vulnerability to single points of failure and bolsters the overall resilience of the network against malevolent activities.

1.1 AI's Role in Enhancing Fog Computing Security

AI's ability to keep an eye out for possible threats and respond to them in real time could be helpful for network security. In traditional security measures, algorithms and patterns that have already been set up are often used. In the long run, it's possible that these hard-and-fast safety measures won't help much if hackers come up with new ways to attack. Even so, AI can learn and adapt to new threat patterns on the fly. This makes the ecosystem of fog computing less vulnerable to attack. IDSs [2] that are powered by AI can analyses traffic in real time in a fog computing environment, for example. These AI systems are always learning from what is going on in the network. This lets them quickly spot unusual behavior and send up red flags for anything that could be dangerous. In fog computing, AI can help with the adaptive allocation of resources, which keeps the performance of edge devices from being affected by security measures. This is necessary because there are so many de-vices involved and each one has a different way of processing information.

1.2. Blockchain for Immutable Security and Privacy

The ledger structure of blockchain is decentralized and spread out, which a perfect match for fog is computing, which is also decentralized and spread out. Blockchain does this by making a distributed ledger that keeps track of each transaction across several nodes. The information that comes out of this process is shared with the public and can't be changed. Because data can't be changed, there is a higher level of data integrity, which is important for applications that depend on correct data. And since there is no need for middlemen, agreements that have already been made can be turned into smart contracts and automatically put into place and enforced within the Fog network by using the features of Blockchain technology. With the help of these smart contracts, financial transactions in the Fog can be automated in a way that doesn't require trust and is safe. One way to do this would be to put a smart contract into a Fog node so that data from IoT devices is only processed if it meets certain criteria.

End-to-end encryption, which is made possible by the cryptographic algorithms that are built into the Blockchain, is another way to protect sensitive data. Blockchain technology makes sure that only the right people can see private information by using cryptography to prove who owns the data and who has control over who can access it.

1.3 AI and Blockchain: A Symbiotic Relationship

When artificial intelligence (AI) and blockchain technology are integrated, the end product may be superior to the sum of their individual capabilities. Artificial intelligence may get useful insights into the condition of a network's security, performance, and other parameters by analyzing the immutable record of data transactions that Blockchain maintains. On the other hand, Blockchain has the ability to log and confirm the decisions made by AI algorithms, which helps to make AI operations open, traceable, and protected from malicious interference.

This synergy has the potential to be very useful for ensuring that the privacy of an individual is preserved. After personally identifiable information has been removed

From data through the use of AI-powered anonymization algorithms [3], the data can then be recorded on the Blockchain in a condition that has not been altered and is valid. When it comes to maintaining users' privacy and maintaining their security in the burgeoning fog computing business, the combination of AI and Blockchain may prove to be a game-changer. As fog networks continue to expand and encompass an increasing number of devices, it is becoming increasingly critical to implement security solutions that are not only powerful

but also dynamic, scalable, and flexible. The utilization of artificial intelligence for the purpose of intelligent threat assessment as well as the decentralized and immutable qualities of blockchain technology stand out as essential strategies for this goal. These advancements not only improve the dependability of fog ecosystems but also pave the way for new, cutting-edge applications of edge computing that are also secure.

This section is meant to serve as an illustration of how the organization of the rest of the paper should be. In the following section (Section 2), we will talk about previous research that is relevant, and in the following section (Section 3), we will provide context by analyzing the research literature that is relevant. The proposed that is unique to our organization and the associated security proof are both covered in Section 4. The design of the system that we have recommended will be covered in Section 5, and Section 6 will be devoted to an analysis of the proposed model from both a theoretical and an experimental vantage point. In order to wrap up this inquiry, we will finish by discussing the consequences of our research for the development of data security in the future.

2. Related Work

In recent years, significant progress has been made on the increasingly prevalent inter- section of artificial intelligence and fog computing. The primary objective is to protect individuals' privacy and maintain their safety while simultaneously deriving insights from data that is physically located closer to their point of origin.

The upsurge of Fog Computing and the Internet of Things (IoT) has drawn significant attention to privacy and security concerns. Several research efforts have aimed at designing and implementing privacy-preserving schemes specifically for this domain.

Ferrag et al. [1] presented a detailed evaluation of privacy-preserving strategies for the field of fog-based Internet of Things applications. The authors outlined a variety of threat models and developed a classification system for the privacy concerns that are associated with this field. In addition, they shed light on prospective solutions as well as the underlying problems that are associated with the process of implementing such solutions. Their work is a critical basis for understanding the security landscape of fog-based Internet of Things (IoT) deployments, and it serves this purpose admirably.

Gowda et al. [2] provided a novel technique to integrate blockchain technology for access control within a Fog Computing environment. This study followed a similar subject but put more of an emphasis on the potential of blockchain technology. The fact that they provide a decentralized and unchangeable access control system, which in and of itself provides an increased level of safety, is the primary advantage of their concept. In addition, their methodology guarantees that the anonymity of users is maintained during transactions, which positions it as a viable contender for actual deployments of fog computing in the real world.

Chen et al. [3] took on the task of preserving data privacy during both the collection and computation stages in fog-assisted Internet of Things setups. This was a challenge from a computational point of view. Their idea successfully offloads computing work in an efficient manner while simultaneously protecting user data from the risk of possible intrusions. The methodology that they presented makes use of cryptographic methods to ensure that data is kept secure both during transmission from IoT devices to Fog nodes and, later, during the computing processes themselves.

Even though each of these publications has a unique viewpoint, taken together they highlight the growing significance of safeguarding Fog Computing environments, particularly when they are linked with Internet of Things (IoT) networks. Their solutions, which range from cryptographic methods to the utilization of blockchain technology, provide scholars and practitioners operating in this field with significant insights and resources.

Table 1. Comparative Analysis methods, advantages, disadvantages, and research gaps

S.n.Citation	Method	Advantage	Disadvantage	Research gap
1 C. Lai, et al. [4]	Smart parking with dual Privacy	Secure smart parking options. Offers two privacy layers	Potential scalability or dynamic environment issues	Integration of various privacy-preserving methods
Zhonghu C., et al. [5]	Iot attribute-based access contracts leveraging blockchain and edge computing	Iot security and privacy improvements computing real time processing	Complexity handling attribute-based controls. Possible delay.	Reduce complex system latency via optimization
Thien The, et al. [6]	Review of metaverse Huynh-blockchain applications	blockchain knowledge in the coming metaverse.	not offer new solutions.	metaverse blockchain integration.
A. S. Ra-	Decentralized	Increases metaverse	Platform interoperabi	Integration methods

jawat et al., [7]	metaverse security leveraging blockchain	security through decentralisation.	lity issues.	for centralised metaverse platforms
S. Pundir etal., [8]	Intrusion detection protocols in IoT-integrated WSNs survey	Detailed knowledge of intrusion detection protocols	It may not solve problems because it is a survey	Creation of new protocol or optimization methods.
T.D. Luong et al.,[9]	Federated learning and blockchain for collaborative AI model development	Allows secure decentralized AI model training across devices.	Device synchornisation or coordination issues.	More efficient FedChain synchronization or data harmonization

Table 2. Existing Encryption Method for Security

Author /Year	Technique	Method
[10]	Holomorphic Encryption is a type of encryption that uses holomorphic morphology.	Multi-level security is used to protect the data. Additionally, personal information is safeguarded.
[11]	Encryption standard known as Advanced Encryption Standard (AES)	Decrypt. Using three datasets to test for fog security
[12]	Identity-Based Encryption (IBE) is a type of encryption that is based on a person's identity. (IBE)	Identity-Based Encryption (IBE) is a type of encryption that is based on a person's identity.
[13]	Accumulation of Data and Holomorphic Encryption	Identity protection is essential when uploading data to public cloud services. Preserve fog nodes' bandwidth.

3. Proposed Methodology

The combination of blockchain technology with AI (Artificial Intelligence) methods such as SVM (Support Vector Machines) and Random Forest opens up new possibilities for protecting the personal information of users and preventing malicious activity in fog computing. SVM stands for support vector machines [14], and Random Forest is an example of an AI method. IoT (Internet of Things) capabilities and ap-plications can benefit from fog computing since it moves processing closer to the network's edge than traditional cloud computing does. On the other hand, this opens the door to concerns of confidentiality and safety.

3.1 Role of Machine Learning

Anomaly Detection:
By training their models on typical network traffic and device behavior, SVM and Random Forest can be helpful for recognizing anomalies, which may be indicative of cyber-attacks or system breakdowns. This can be done by analyzing the data.
Predictive Maintenance:
Administrators may be able to take preventative action with the assistance of ma- chine learning models in the event that vital components of the fog network fail.
Optimized Resource Allocation:
The AI is able to figure out the most effective way to allocate its resources in order to keep everything secure and working smoothly despite the fog.

3.2 Blockchain in Fog Computing:

Cloud computing can be extended to the edge of the network via fog computing, which moves processing closer to the location where the data was generated. While it does enable faster processing and lower latency, it also presents new issues in terms of privacy and security. These challenges are novel because of the nature of the technology. When paired with AI machine learning algorithms [15] such as SVM and Random Forest, blockchain, with its features of being decentralized and immutable, presents a possible answer to these difficulties.
Immutable Records:
In a fog computing environment, blockchain technology can maintain an immutable record of all transactions, so guaranteeing traceability.
Decentralized Security:
Blockchain operates on decentralized principles, meaning there isn't a single point of failure. This enhances the robustness of the security framework in fog computing.
Smart Contracts:
These are computer-based agreements that can carry out their own terms [16]. These can regulate data exchange in fog settings, making sure it is done in a private and safe manner.

3.3 Integration Strategy

Data Collection: Before being sent out, data is first captured and preprocessed locally by the devices [17] that make up a fog network.
Secure Transmission with Blockchain: Before information is sent from a user's de-vice, it is encrypted to prevent manipulation and distributed in a safe manner through a blockchain network.
ML-based Analysis: After the data has arrived at its destination and been analysed with an SVM or Random Forest model, additional activities such as anomaly detection, optimization of resource allocation, and other similar tasks may be carried out on the data.
Consensus Decision Making: Consensus mechanisms in the blockchain have the ability to ensure that the findings of machine learning analyses are verified by many nodes before crucial decisions are made based on those analyses.
We propose a computing paradigm that is based on fog coupled with a Three Layer Storage (TLS) framework for the purpose of protecting user privacy [18]. It is possible that the TLS framework will be able to give the user some degree of control and properly protect their privacy. It was mentioned earlier that fending off an assault from within is not an easy endeavor, and this is true. While conventional tactics are useful for fending against exterior dangers, they are completely ineffective when the problem lies within CSP itself [18]. Encoding is utilised in our solution as opposed to the more conventional ways in or- der to partition the user's data into three groups of varied sizes. Because of the need to maintain confidentiality, each of them will be lacking some important information. When cloud computing is combined with the concept of fog computing [19], the three layers of data storage that are used (the fog server, the cloud server, and the user's local workstation) are organized in descending order of the amount of data stored at each level [20]. If an adversary implements this tactic, even if he is successful in accessing all of the data that is stored on a particular server, he will not be able to recreate the user's original data. Without having access to both the user's local workstation and the fog server, the CSP will be unable to obtain any information that is of any use.
Proposed algorithm,
Proposed algorithm 1
Step 1: Data Initialization:
Step 2: Plain Data: A given string representing raw data, initialized with "input the plan data". Step 3: Reading the Data:
Step 4: Utilize the WL function to display the raw data: WL ("Raw data: {0}", plain Data). Step 5: Hashing the Data:
Step 6: Generate the hash of the plain data using the SHA-256 algorithm: Hashed Data = Calculate Sha256 Hash (plain Data).
Step 7: Display the hashed result: WL ("Hash {0}", hashed Data).
Step 8: Directly compute and display the hash using: WL (Compute Sha256Hash ("input the plan data")).
Step 9: Reading the Line: Step 10: Use the RL () function to read a line of input. Step 11: Hash Calculation:
Step 12: Compute Sha256 Hash: A function to hash the raw data.
Step 13: Initialize the SHA-256 hashing process: Using (SHA256 sha256 Hash = SHA256.Create ()).
Step 14: Convert the raw data into bytes and compute its hash: Bytes = sha256 Hash. Compute Hash (Encoding.UTF8.GetBytes(raw Data)). Step 15: Loop Implementation:
Step 16: A loop iterates through each byte in the hashed byte array. Step 17: Csharp
Step 18: for (int i = 0; i < bytes. Length; i++) Step 19: Inside the loop, convert each byte to a 2-character hexadecimal string using: bytes[i].To String ("x2").
Step 20: Return Process:
Step 21: Return the concatenated string representation of the hash.

3.4 Privacy Preservation

Data Tokenization: Instead of storing sensitive information, tokens (representative data) can be stored and transacted in the fog environment, ensuring data privacy [21].
Zero-Knowledge Proofs: This cryptographic method allows one party to prove to another that something is true, without revealing any specific information about it. Combined with blockchain [22], it ensures that data can be verified without com-promising privacy.
Proposed algorithm
Advance security Architecture for IoT using machine learning.
The coordinator should be a well-known fog node consequently, an authorized node creates a unique key along with associated parameters.
On the cryptographic algorithms RSA and ECC Fog nodes must be able to communicate with other things while retaining a high level of accuracy and confidentiality in their communications. Before sending an encrypted message from one device to another, it is necessary to decrypt the message. In order to prevent fog nodes and un- signed IoT devices from reading the messages transmitted by each IoT device, they need be signed. Security keys will no longer be required when dealing with a massively networked IoT environment because the scheme will decouple the sender and recipient. The primary focus of this research is on maintaining confidentiality. If a specific method.

Algorithm 2:
1. Initialize: - Blockchain Network - SVM Parameters - Random Forest Parameters
2. FOR each Fog Node i: - Collect and Preprocess Data from i - Encrypt Data using a secure method - Add encrypted data as a transaction to Blockchain

3. FOR model training: - Retrieve and Decrypt data from Blockchain - Split data into training and testing sets Train SVM and Random Forest on training data: Optimize for best performance
4. Evaluate both models on the testing set and report metrics
5. Deploy models to relevant Fog Nodes
6. MONITOR models and Fog Node activities: IF anomaly or potential breach detected: - Alert administrator - Record incident on Blockchain END IF
7. ALWAYS ensure data privacy and use encrypted channels for communication.

Algorithm 3:
Phase 1: The key generation process utilizes fog and public curve parameters to produce public keys (pub k) and secret keys (S k).
Phase 2: The generated keys are securely stored in a vault under the jurisdiction of the authority.
Phase 3: Data is accumulated regarding the public curve parameters (PK) from other fog nodes and IoT devices.
Phase 4: IoT devices are provided with the Cid1 private key by the fog coordinator. Phase 5: Secondary fog nodes, known as slave fog nodes, retrieve the client's "Cid" (from an IoT device) through the primary Cid2 node.
Phase 6: IoT client devices encrypt their messages using the private key prik Cid1 prior to transmission.
Phase 7: After decrypting the received encrypted communication, the fog node uses Pri k Cid2 to re-encrypt it. This results in a Cid message that is in a transitional phase, having been both encrypted and decrypted. Cid used its private key, prik, Cid1, to decode the message.
is right, it must be feasible to decode the message using the correct key to verify it is correct. If you prefer, you can start with the letter m as the message and encrypt it to cre- ate a cipher text. The encryption algorithm is reused (Enc.m). (pri k Cid1, pri k-Cid2) is a pair of keys that have been created. After decrypting the message, Re Enc(Enc.m)) is identical to m. When this is the case, we may be confident in the security of our de- sign solution. Based on assault probability, the proposed system is impregnable. It is beneficial when a breach is unlikely to be detected. Its time-bound and polynomial nature minimises adversarial breach. The proposal compares RSA with ECC, which have pros and cons. Based on findings and case variables, the best applicant is chosen. Encrypting data with the robust RSA technique requires the composite number n=p*q, a pair of gigantic prime numbers. It's difficult to find the prime factorization of a large integer, also known as the composite figure. The main public key cryptography competitor to RSA, Elliptic Curve Cryptosystems (ECC), uses a different algorithm. A publicly published elliptic curve can prevent index calculus attacks. The algorithm's difficulty depends on the elliptic curve's size. Due of their proximity, discrete logarithms struggle to compute curve base points. Point multiplication cannot find the multiplicand when both the original and product points are given. This determines algorithm protection. ECC proxy protection against chosen-plaintext attacks is provided by the proposed system. Smaller cypher text and signatures are generated. More efficient than RSA in key generation. The researchers found that ECC provides the same security as a 1024-bit RSA key with a 164-bit key. ECC is computationally faster than RSA and can replace it for signing and decryption. A two-stage, incredibly safe procedure, ECC signatures are hard to make, but RSA signatures are easy. ECC's binary elliptical curve is fast, simple, and fault-tolerant for critical information exchange [19]. However, the two most effective SSL methods can be attacked. 2020 proxy re-encryption is best for distributed systems with Internet of Things and smart grid applications. This method can solve Internet of Things storage and management issues. The experiment shows that data encryption and decryption take longer as security improves, even for data of different sizes. Most times, encrypting and decrypting the same data takes at least twice as long as the first time. 4 ECC decryption is faster than RSA, according to the data. Cloud computing serves billions of apps and devices at the network edge. This ubiquitous technology can support several fog deployments when paired with cloud computing. Fog nodes can provide generic and customised services with changing resource availability [24]. The organisation maintains confidentiality throughout the conversation process. The proposed double encryption [25] meets requirements. Two legal partners conversing [26] are protected by the first level of encryption. In a fog-based Internet of Things network [27], intermediary nodes don't need to know the data they're sending. This is done with encryption [28]. Encrypting data without the node knowing the secret is possible.

4. Results Analysis

Utilizing FogSim [29] you may generate a hazy environment. The Ganache crypto currencies can be utilized in the construction of the Truffle blockchain, which is employed for the creation of smart contracts. Tensor Flow and PyTorch, two industry leaders, are excellent choices when it comes to the construction of models for the identification of anomalies. These models will need to be packaged up first, and then Dockers will be able to be used to incorporate them into the fog nodes. Simulations of data storage and retrieval must be carried out using blockchain transactions. Smart contracts, which are built on distributed ledger technologies such as Hyper ledger and Ethereum, secure the data's privacy as well as its security. Make use of Kafka to coordinate the movement of data between your blockchain, fog nodes, and the AI technologies in your organization. Integrate methods for protecting users' privacy, such as holomorphic encryption and zero-knowledge proofs. Grafana and the ELK Stack are a powerful combination for the purpose of surveillance since they are able to provide data visualizations that are both precise and up to

date and to notify users in real time of any potential vulnerabilities. Separate the components of the system so that you can investigate their operations, precautions against security breaches, and ways of storing personally identifiable in- formation. Make adjustments in accordance with the feedback and the outcomes. We intend to combine these technologies and strategies in a realistic simulation in order to examine the potential synergy between AI and blockchain in the context of fog computing, specifically with regard to the protection of data privacy and security.

Table 3. Results Analysis

Method	Platform	Dataset	Evaluation Metric	Result
Proposed Algorithm	Cloud based IIoT system	NSL-KDD dataset	Classification accuracy	99.8 %
AILBSM[30]	Cloud based IIoT system	NSL-KDD dataset	Detection performance	99.7 %
AILBSM[31]	Blockchain based IoT system	IoT 23 dataset	Privacy prevention score	0.95
BCT-IoT [32]	Blockchain federated learning system	MNIST dataset	Data leakage	0.01
Blockchain federated learning framework [33][34]	Blockchain federated learning framework	MNIST dataset	Model accuracy	98.6 %

The following table provides a comparison of various methods to the security and privacy of fog computing that make use of AI and Blockchain. The following is a condensed version of the procedures:

• AILBSM: Artificial Intelligence-based Lightweight Blockchain Security Mode

• BCT-IoT: Blockchain Technology for Ensuring Security and Privacy Aspects in
Internet of Things

• BFLF: Blockchain Federated Learning Framework for Privacy-Preservation Platforms can be found in the column labelled "platform," and some examples of
These platforms are federated learning, cloud computing, and blockchain technology. In the experiments, many data sets were utilized, such as NSL-KDD, IoT-, and MNIST.

5. Conclusion

Fog Computing is an interesting new way of doing things. It uses AI and machine learning techniques like SVM and Random Forest, along with Blockchain technology, to give users anonymity and security. Because Fog Computing is distributed, edge data security needs to be tighter. Because Fog nodes are spread out and face many different kinds of threats, traditional security measures might not work for them. This shows how blockchain can't be changed and is open to everyone. No one can dispute the data and transactions on a blockchain. Because blockchain is open to everyone, bad behavior can be found and maybe even stopped. On the other hand, machine learning models like SVMs and RFs can effectively analyse data. They can be taught to spot threats to network safety or to improve how the network works. In addition to blockchain's auditable record, these models can check data and transactions as well. This makes Fog Computing safe and effective. AI and Blockchain also make Fog Computing more valuable. Blockchain protects data that has been pro-cessed by AI, which can analyse huge amounts of data, in a way that can't be changed. Together, these technologies make Fog Computing more secure and make it possible for edge applications to understand their surroundings. When AI machine learning models and Blockchain technology are combined in fog computing, it creates a solution that is good for data analytics, privacy, and security. This convergence is expected to lead to the next generation of Fog Computing, which gives data-driven insights without sacrificing security or trustworthiness. This study explored the synergy between Artificial Intelligence (AI) and Blockchain technology in enhancing privacy preservation and security within the realm of Fog Computing. By integrating sophisticated AI algorithms like Support Vector Machines (SVM) and leveraging the inherent security features of blockchain through consensus decision-making and zero-knowledge proofs, the research demonstrates a robust approach to securing fog computing environments. This combination not only fortifies data integrity and confidentiality but also ensures efficient and decentralized data pro-cessing, which is pivotal in fog computing paradigms. Future research should focus on optimizing blockchain's scalability in fog layers, enhancing SVM efficiency for real-time processing, and developing more advanced zero-knowledge proofs for diversified fog computing applications.

References

[1] Ferrag, M.A., Derhab, A., Maglaras, L., Mukherjee, M., Janicke, H.: Privacy-preserving Schemes for Fog-based IoT Applications: Threat models, Solutions, and Challenges. 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT) pp. 37–42 (2018)

[2] Gowda, N.C., Manvi, S.S., M, B.: Blockchain-based Access Control Model with Privacy preservation in a Fog Computing Environment. 2022 IEEE International Conference on Elec- tronics, Computing and Communication Technologies (CONECCT) pp. 1–6 (2022)
[3] Chen, S., Zhu, X., Zhang, H., Zhao, C., Yang, G., Wang, K.: Efficient Privacy Preserving Data Collection and Computation Offloading for Fog-Assisted IoT. IEEE Transactions on Sustainable Computing 5, 526–540 (2020)
[4] Lai, C., Li, Q., Zhou, H., Zheng, D.: SRSP: A Secure and Reliable Smart Parking Scheme With Dual Privacy Preservation. IEEE Internet of Things Journal 8(13), 10619–10630 (2021)
[5] Zhonghua, C., Goyal, S.B., Rajawat, A.S.: Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing. J Super- comput (2023)
[6] Huynh-The, T., Gadekallu, T.R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q.V., Costa, D.B.D., Liyanage, M.: Blockchain for the metaverse: A Review. Future Generation Com- puter Systems 143, 401–419 (2023)
[7] Huynh-The, T., Gadekallu, T.R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q.V., Costa, D., Liyanage, M.: Blockchain for the metaverse: A Review. Future Generation Com- puter Systems 143, 401–419 (2023)
[8] Rajawat, A.S.: Blockchain-based Security Framework for Metaverse: A Decentralized Ap- proach. In: 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). pp. 1–06 (2023)
[9] Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J.P.C., Park, Y.: Intrusion De- tection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. IEEE Access 8, 3343–3363 (2020)
[10] Luong, T.D.: FedChain: A Collaborative Framework for Building Artificial Intelligence Models using Blockchain and Federated Learning. 2021 8th NAFOSTED Conference on Information and Computer Science (NICS) pp. 149–154 (2021)
[11] Rajawat, A.S., Goyal, S.B., Bedi, P., Verma, C., Ionete, E.I., Raboaca, M.: https://doi.org/10. 3390/math11030679
[12] Zerka, F.: Blockchain for Privacy Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging (C-DistriM). IEEE Access 8, 183939–183951 (2020)
[13] Dave, M., Rastogi, V., Miglani, M.: Smart Fog-Based Video Surveillance with Privacy Preservation based on Blockchain. Wireless Pers Commun 124, 1677–1694 (2022)
[14] Alzoubi, Y.I., Gill, A., Mishra, A.: A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. J Cloud Comp 11, 80–80 (2022)
[15] Shah, K., Chadotra, S., Tanwar, S.: Blockchain for IoV in 6G environment: review solutions and challenges. Cluster Comput 25 (1927)
[16] Li, W., Wu, J., Cao, J.: Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J Cloud Comp 10, 35–35 (2021)
[17] Krishnamoorthy, S., Dua, A., Gupta, S.: Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. J Ambient Intell Human Comput (2021)
[18] 18. Amiri, Z., Heidari, A., Navimipour, N.J.: (2022), https://doi.org/10.1007/s10586-022- 03738-5
[19] Singh, A., Satapathy, S.C., Roy, A.: AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope. Arab J Sci Eng 47, 9801–9831 (2022)
[20] Bagga, P., Das, A.K., Chamola, V.: Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions. Telecommun Syst 81, 125–173 (2022)
[21] Alfa, A.A., Alhassan, J.K., Olaniyi, O.M.: Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions. J Reliable Intell Environ 7, 115–143 (2021)
[22] Bhushan, B., Sahoo, C., Sinha, P.: Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Netw 27, 55–90 (2021)
[23] Alagheband, M.R., Mashatan, A.: Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives. J Supercomput 78, 18777–18824 (2022)
[24] Rejeb, A., Rejeb, K., Simske, S.J.: Blockchain technology in the smart city: a bibliometric review. Qual Quant 56, 2875–2906 (2022)
[25] Wang, C., Cheng, X., Li, J.: A survey: applications of blockchain in the Internet of Vehicles. J Wireless Com Network 2021, 77–77 (2021)
[26] Shafay, M., Ahmad, R.W., Salah, K.: Blockchain for deep learning: review and open chal- lenges. Cluster Comput (2022)
[27] Himeur, Y., Elnour, M., Fadli, F.: AI-big data analytics for building automation and manage- ment systems: a survey, actual challenges and future perspectives. Artif Intell Rev (2022)
[28] Li, D., Han, D., Weng, T.H.: Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. Soft Comput 26, 4423–4440 (2022)
[29] Elrahman, S.A., Alluhaidan, A.S.: Blockchain technology and IoT-edge framework for shar- ing healthcare services. Soft Comput 25, 13753–13777 (2021)
[30] Jiang, M., Qin, X.: Distributed ledger technologies in vehicular mobile edge computing: a survey. Complex Intell. Syst 8, 4403–4419 (2022)
[31] Su, W., Li, L., Liu, F.: AI on the edge: a comprehensive review. Artif Intell Rev 55, 6125– 6183 (2022)
[32] Selvarajan, S., Srivastava, G., Khadidos, A.O.: An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J Cloud Comp 12, 38–38 (2023)
[33] Zubaydi, H.D., Varga, P., Molnár, S.: Leveraging Blockchain Technology for Ensuring Se- curity and Privacy Aspects in Internet of Things: A Systematic Literature Review. Sensors 23, 788–788 (2023)
[34] Sameera, K.M., Vinod, P., Rehiman, K.A.R., Jifhna, P., Sebastian, S.: Blockchain Feder- ated Learning Framework for Privacy-Preservation. In: Rajagopal, S., Faruki, P., Popat, K. (eds.) Advancements in Smart Computing and Information Security. ASCIS 2022. vol. 1760. Springer (2022)