

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

S. B. Goyal<sup>1,\*</sup>, Anand Singh Rajawat<sup>2</sup>, Manoj Kumar<sup>3</sup> and Purna Agarwal<sup>4</sup>

<sup>1</sup>Faculty of Information Technology, City University, Petaling Jaya, 46100, Malaysia

<sup>2</sup>School of Computer Science & Engineering, Sandip University Nashik, India

<sup>3</sup>University of Wollongong, Dubai, UAE

<sup>4</sup>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

Copyright © 2024 S. B. Goyal *et al.*, licensed to EAI. This is an open access article distributed under the terms of the [CC BY-NC-SA 4.0](#), which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetiot.5555

\*Corresponding author. Email: [drsbgoyal@gmail.com](mailto: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









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 pri k 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, pri k, 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 create 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 design 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 information. 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 Electronics, 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 Computer 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 Computer Systems 143, 401–419 (2023)
- [8] Rajawat, A.S.: Blockchain-based Security Framework for Metaverse: A Decentralized Approach. 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 Detection 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] 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 (BloT): 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 challenges. Cluster Comput (2022)
- [27] Himeur, Y., Elnour, M., Fadli, F.: AI-big data analytics for building automation and management 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 sharing 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 Security 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 Federated Learning Framework for Privacy-Preservation. In: Rajagopal, S., Faruki, P., Papat, K. (eds.) Advancements in Smart Computing and Information Security. ASCIS 2022. vol. 1760. Springer (2022)