**JOIN (Jurnal Online Informatika)**
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 10 Number 1 | June 2025: 22-31
DOI: 10.15575/join.v10i1.1392

# Synergistic Disruption: Harnessing AI and Blockchain for Enhanced Privacy and Security in Federated Learning

**Sandi Rahmadika[1], Winda Agustiarmi[2], Ryan Fikri[3], and Bruno Joachim Kweka[4]**
[1,2,3]Department of Electronic Engineering, Faculty of Engineering
Faculty of Engineering, Universitas Negeri Padang, Sumatera Barat, Indonesia
[4]Cyber Studies, The University of Tulsa, United States of America, 800 S Tucker Dr, Tulsa, OK 74104, United States of America

**Article Info**

***Article history:***

Received June 11, 2024
Revised November 15, 2024
Accepted November 18, 2024
Published April 01, 2025

***Keywords:***

Artificial intelligence
Blockchain
Federated learning
Privacy
Smart contracts

**ABSTRACT**

Combining blockchain technology with artificial intelligence (AI) offers revolutionary possibilities for developing strong solutions that capitalize on each technology's own advantages. Blockchain technology makes self-executing agreements possible by enabling smart contracts, which reduce the need for middlemen and increase efficiency by precisely encoding contractual terms in code. By using AI oracles, these contracts can communicate with outside data sources and make well-informed decisions based on actual occurrences. Additionally, there is a lot of potential for improving machine learning and data interchange in terms of privacy, security, and transparency through the integration of blockchain with federated learning. In order to provide accountability and transparency, the blockchain's immutable ledger can painstakingly record every transaction that takes place during the federated learning process, from data submissions to model modifications and remuneration. Participants in federated learning networks also develop trust because of blockchain's transparency and resistance to tampering. Strong participant verification procedures are put in place to strengthen data integrity and model updates, which raises the system's overall reliability. In the end, this chapter examines novel research avenues for combining blockchain technology with federated learning, providing practical methods and strategies to improve transaction security and privacy and opening the door to a new era of reliable and effective machine learning applications.

***Corresponding Author:***

Sandi Rahmadika,
Department of Electronic Engineering, Faculty of Engineering
Faculty of Engineering, Universitas Negeri Padang
Jalan Prof. Dr. Hamka, Air Tawar Padang, Sumatera Barat, Indonesia,
Email: sandi@ft.unp.ac.id

## 1. INTRODUCTION

In contemporary society, the pervasive influence of data-driven technology has brought about substantial transformations in several sectors and our everyday experiences. Consequently, security and privacy issues have gained heightened importance and are now considered paramount [1]. The amalgamation of blockchain technology with federated learning presents itself as a potent remedy, providing a paradigm-shifting method to tackle these urgent concerns [2]. The integration of blockchain's immutability and transparency with federated learning's decentralized and privacy-preserving capabilities forms a mutually beneficial technological alliance [3]. Collectively, these advancements lay the groundwork for a novel era in applications driven by data, wherein individuals

are able to regain authority over their personal information, corporations may engage in secure collaboration on AI initiatives, and confidence in data processes is elevated to unparalleled heights [4]. This investigation examines the amalgamation of blockchain technology and federated learning, elucidating the potential for this fusion to transform the realm of security and privacy in the contemporary digital era [5][6].

Both blockchain and federated learning are designed to operate in a decentralized manner. The primary aim of the decentralized approach is to mitigate the challenges associated with communication bottlenecks and memory utilization in traditional centralized systems [7]. The dominant model of an intensely focused strategy (dependent on a single node) in wireless networks has been progressively transitioning towards decentralized methodologies, encompassing domains like financial services, healthcare records, various types of digital rights, and intellectual property [8]. Numerous analysts assert that smart contracts have the potential to establish a novel paradigm that fundamentally alters how parties draft contracts and engage in economic activities. The blockchain transactions executed successfully are openly accessible inside the network and can be retrieved by blockchain entities using the user interface [9] Therefore, it has been implemented in diverse scientific domains.

In contrast to traditional machine learning approaches, which involve central processing of the training model by clients, federated learning enables clients to construct the AI model by transmitting updated gradient values to the aggregating server while keeping the underlying dataset concealed. As a result, the preservation of privacy for customers is a deliberate feature of federated learning, ensuring that sensitive data remains confidential [10][11]. However, the current state of federated learning is characterized by a deficiency in the provision of appropriate incentive mechanisms that effectively incentivize clients to enhance AI models [12][13]. A number of applications fail to offer any form of compensation to its users. The utilization of blockchain technology, along with the incorporation of smart contract functionalities, presents a potential resolution for addressing challenges related to incentive mechanisms. It is essential to acknowledge that using smart contracts poses a potential risk to customers' privacy, as these contracts are transparent and easily accessible through the interface [14].

Considering privacy awareness in wireless network contexts is essential when examining smart contracts and federated learning since it presents a significant problem that necessitates attention. This study investigates the methods employed to protect privacy in the context of cross-silo federated learning within wireless networks that are not deemed trustworthy. The case study focuses on an incentive scheme implemented on blockchain smart contracts. In this study, we also examine the existing protocols that facilitate the establishment of dependable and intelligent system orchestration for 5G networks and future iterations, which operate on a mobile edge computing architecture, artificial intelligence, and blockchain technology. This study comprehensively describes an incentive mechanism that ensures the inability to trace its origins. The mechanism is built upon utilizing Ethereum smart contracts and relies on the available data. A proportionate incentive scheme has the potential to motivate companies to contribute to the maintenance of cross-silo distributed ledger transactions consistently. The methods involved in decentralized transactions ensure that the persons involved cannot be linked to the transactions. In summary, the transactions occur in a manner that safeguards the confidentiality of the parties' information values, aligning with the principle of privacy preservation in decentralized techniques.

## 2. METHOD

### Blockchain and Federated Learning Fundamentals

This section delivers a comprehensive overview of the fundamental concepts pertaining to the decentralized ledger, blockchain, and federated learning. These approaches are considered groundbreaking in the field of trust technology, as they prioritize decentralization as a core element. The paper provides a comprehensive analysis of the integration of blockchain technology within the context of federated learning.

### *2.1. Decentralized Technology and Trust Perspectives*

The deliberate adoption of a decentralized strategy is causing a significant transformation in the role traditionally played by centralized systems in several scientific domains, including banking,

p-ISSN: 2528-1682
e-ISSN: 2527-9165

supply chain management, the automotive industry, and healthcare [15][16]. The decentralized strategy aims to remove the vulnerability associated with single-point-of-failure (SPoF) scenarios [17]. The decentralized approach encompasses blockchain technology and federated learning in the field of AI. These methods aim to enhance the accuracy of the global model by addressing various objectives in machine learning. Blockchain-enabled applications often leverage the SPoF characteristic by employing diverse consensus mechanisms [18][19]. The transaction data is documented within a decentralized ledger, preventing a singular authority's clandestine endorsement of occurrences [20].

The current smart contracts-based solutions, such as Ethereum smart contracts and Hyperledger chain code, are limited in handling complex computations required for real-world AI applications [21]. The developers can program the codes in such a way that they can function as self-executing programs without requiring input from third parties. The combination of AI with smart contracts has the potential to establish a decentralized interactive system that is both more resilient and efficient for the involved parties [22]. In summary, conducting a comprehensive investigation of smart contracts integrated with federated learning in systems that handle susceptible information, such as federated identification and digital forensics, is imperative [23]. Indeed, it is crucial to augment complementary protocols [24], [25].

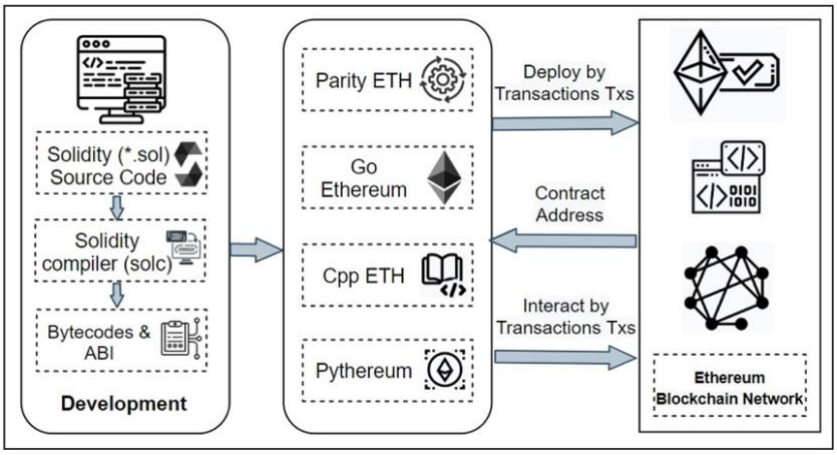


Figure 1. The present discourse concerns the framework encompassing the development, implementation, and interaction of Ethereum smart contracts

Table 1. Summary of Tips & Tricks for a good Scientific Article

| Code | Parameters / Standards | Description |
|---|---|---|
| MRS 7 | Financial Flow Statements | Currency and its equivalents |
| MSFI 9 | Financial instruments (assets that can be traded) | Digital assets at appropriate value |
| MRS 40 | Real estate investments (with its natural resources) | Land and building investments |
| MRS 16 | Property, plant, and equipment (PP\&E) | PP&E physical or tangible assets |
| MRS 38 | Intangible assets | Identifiable non-monetary asset |
| MRS 2 | Supply / logistics | Supply chain |
| **IFRS Acceptance**: **MRS 7** = Not Acceptable; **MSFI 9** = Not Acceptable; **MRS 40** = Not Acceptable; **MRS 16** = Not Acceptable; **MRS 38** = Not Acceptable; **MRS 2** = Under certain conditions (conditionally) | | |

Figure 1 depicts the procedural aspects associated with the interaction, deployment, and development of the Ethereum smart contract. The Ethereum blockchain platform relies heavily on the Ethereum Virtual Machine (EVM) for its functionality and operational processes. The Ethereum network enables the implementation of smart contracts and decentralized applications by utilizing a decentralized, Turing-complete virtual processor. The EVM functions as the designated execution environment for all code deployed on the Ethereum blockchain. The essential aspects of the EVM encompass decentralized execution, Turing completeness, gas costs, deterministic execution, EVM instructions, state transfer, upgrades and forks, and security with audits. Each deployed function is

associated with unique addresses. Therefore, the entities possess the capability to engage with the contracts through transactions facilitated by several clients, like Parity and Geth, among others.

Table 1 presents the assessment of digital assets (specifically cryptocurrencies) in accordance with the International Financial Reporting Standards (IFRS). IFRS are widely utilized for financial reporting by enterprises operating in numerous nations across the globe. However, in the case of new and distinctive digital assets, it is possible that no established IFRS explicitly addresses them. In instances of this nature, corporations are obligated to employ prevailing IFRS principles and modify them to suit the distinctive attributes of digital assets. IFRS are essential for blockchain and the cryptocurrency industry for several grounds, such as global consistency, financial statement preparation, classification and measurement, fair value measurement, disclosure requirements, and to name a few.

### *2.2. Cross-Silo Federated Learning and Blockchain Integration*

Federated learning is a decentralized machine learning technique that facilitates the training of models over numerous decentralized edge devices or servers while ensuring that the training data remains localized and private. The high-level design of the federated learning technique can be seen in Figure 2. In the context of conventional machine learning, it is customary to gather and consolidate data in a singular location for the purpose of training. However, this approach may give rise to apprehensions regarding privacy and necessitate the transmission of substantial quantities of data to a central server [26][27]. Federated learning effectively mitigates these challenges by enabling the training of models to occur in a decentralized manner, either on individual devices or servers [28].

Cross-silo federated learning represents an expansion of the federated learning framework, with the objective of training machine learning models across numerous organizations or entities. Each entity retains its distinct data silo [29]. Traditional federated learning often emphasizes the training of models by utilizing data obtained from decentralized devices or servers within a singular enterprise. In contrast, cross-silo federated learning expands the scope of collaboration to encompass several organizations, enabling them to collectively train a model while maintaining the confidentiality of sensitive data.

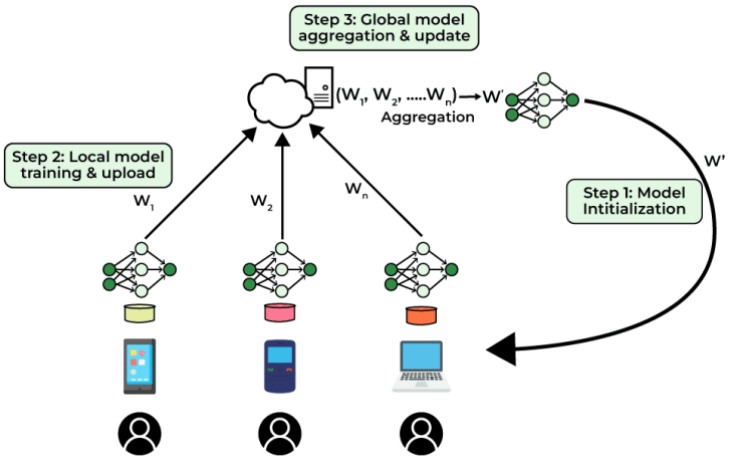


Figure 2. High-level design of federated learning technique. Every device trains the global model privately and uploads the new gradient values back to the aggregation server

The following are the fundamental characteristics and principles behind cross-silo federated learning:

i. **Multiple data silos**. In the context of cross-silo federated learning, several organizations or entities possess distinct data silos that house potentially valuable data suitable for machine learning applications. These organizations engage in collaborative efforts to enhance a collective machine learning model while avoiding consolidating or centralising their respective datasets.

ii. **Privacy preservation**. The privacy issue remains a significant focal point in the context of cross-silo federated learning. Organizations refrain from sharing unprocessed data, opting to

p-ISSN: 2528-1682
e-ISSN: 2527-9165

engage in collaborative efforts for model training while ensuring their respective datasets remain localized. Data security is paramount, particularly when handling sensitive or regulated information, such as healthcare or financial records.

iii. **Model aggregation**. Model changes are disseminated inside the participating entities rather than exchanging raw data. Every entity trains its local model using its own dataset, calculates model updates, and distributes these updates with a central aggregator. Subsequently, the aggregator amalgamates the changes to generate an enhanced global model.

iv. **Secure aggregation**. Secure multi-party computation (MPC) and homomorphic encryption are potential techniques that can be employed to ensure the secure aggregation of model updates originating from diverse companies. This measure guarantees that the updates made to the model are kept confidential and restricted to each business.

v. **Data heterogeneity**. Interdisciplinary collaboration federated learning has the capability to address the issue of data heterogeneity that may exist among different enterprises. Any organisation's data may exhibit distinct distributions, forms, or properties. Federated learning methods have been specifically developed to effectively manage and accommodate the wide range of variability in the data, enabling the global model to adjust accordingly.

## 3. RESULT AND DISCUSSION

### Integration of Blockchain and Federated Learning: Privacy Awareness

Blockchain is a decentralized digital ledger technology that keeps track of transactions across numerous computers in a way that makes it impossible to change the data in the past without changing all subsequent blocks and the network's consensus. It is appropriate for applications needing trust and verification because of its security, transparency, and immutability.

A machine learning approach called federated learning allows several parties to work together to build a common model while maintaining localized data. Each participant trains the model on their own data, sharing just the model updates (gradients) with a central server rather than centralizing data in one place. Since sensitive data stays at its original source, this method improves security and privacy [30]. The feature differences between blockchain and federated learning can be seen in Table 2.

Table 2. The features differences between blockchain and federated learning

| Features | Blockchain | Federated Learning |
|---|---|---|
| Data handling | Centralized record of transactions; decentralized storage. | Data remains on local devices; only model updates are shared. |
| Privacy | Public or private visibility; transparency is a key feature. | Enhances privacy by keeping raw data local. |
| Consensus mechanism | Requires consensus among nodes to validate transactions. | No consensus; relies on local training and aggregation of updates. |
| Purpose | Primary used to secure transactions and record keeping | Aimed at collaboratively training machine learning models without data sharing. |
| Immutability | Transactions are immutable once recorded. | Model updates can be modified; integrity is maintained through aggregation. |

The typical machine learning approach continues to encounter several hurdles that require attention, particularly in the realm of privacy concerns. These challenges encompass issues such as membership inference attacks, data poisoning assaults, hostile clients, dishonest central aggregator servers, and the potential occurrence of SPoF. The membership inference attack involves using reverse engineering techniques by attackers to collect clients' private data through the exploitation of the updated model training process. In contrast, a poisoning attack has the ability to impact the global model by introducing maliciously crafted updated models during the collaborative training phase. In addition, the primary aggregator tasked with overseeing comprehensive system orchestration encounters difficulties in effectively addressing significant obstacles related to the SPoF issue [31]. The present study examines the advantages associated with the utilization of a blockchain-based federated learning strategy, which include, but are not limited to, the following:

i. The implementation of blockchain technology can effectively mitigate the risk of SPoF and facilitate the decentralisation process. This is achieved by substituting the centralised aggregation server with several blockchain nodes, which collectively perform the model aggregation function to establish a global model within the cross-silo federated learning system.
ii. The blockchain system's verification method serves to eliminate faulty data originating from rogue clients or other forms of assaults, such as inference membership attacks and data poisoning attacks, prior to its storage and aggregation as a global model. In this context, the global model will only incorporate legitimate data, whilst the verification system will identify and exclude incorrect data from local model updates.
iii. Blockchain technology enables the facilitation of decentralised transactions, wherein each transaction is assigned a timestamp and subjected to validation and storage by a specific consensus mechanism inside the distributed database network. Therefore, blockchain technology facilitates the automatic acquisition of an updated ledger by all players active in the network.
iv. The utilisation of blockchain technology, coupled with the implementation of smart contracts, is a viable solution to mitigate the issue of inadequate incentives within traditional cross-silo federated learning systems. In this context, blockchain technology enables the distribution of incentives, specifically rewards, to clients. Therefore, utilising incentive mechanisms can effectively motivate clients to actively and truthfully participate in the training process by using their computational resources, ultimately leading to enhancements in the overall performance of the global model.

Blockchain and federated learning are emerging technologies with the capacity to revolutionise multiple sectors. Integrating these two technologies presents innovative possibilities for augmenting data security, privacy, and cooperation inside data-centric applications. In general, there are three types of layers to achieve decentralized machine learning activities with a secure rewarding mechanism, as depicted in Figure 3. The first layer is the blockchain layer, where all recorded transactions are stored in the blocks, eliminating the need for central authorities. Once data is recorded on the blockchain, it becomes immutable and resistant to modification or deletion, guaranteeing the data's integrity. The term blockchain layer commonly denotes a distinct level or constituent inside the architectural framework of a blockchain network. It also includes decentralized storage like the InterPlanetary File System (IPFS).

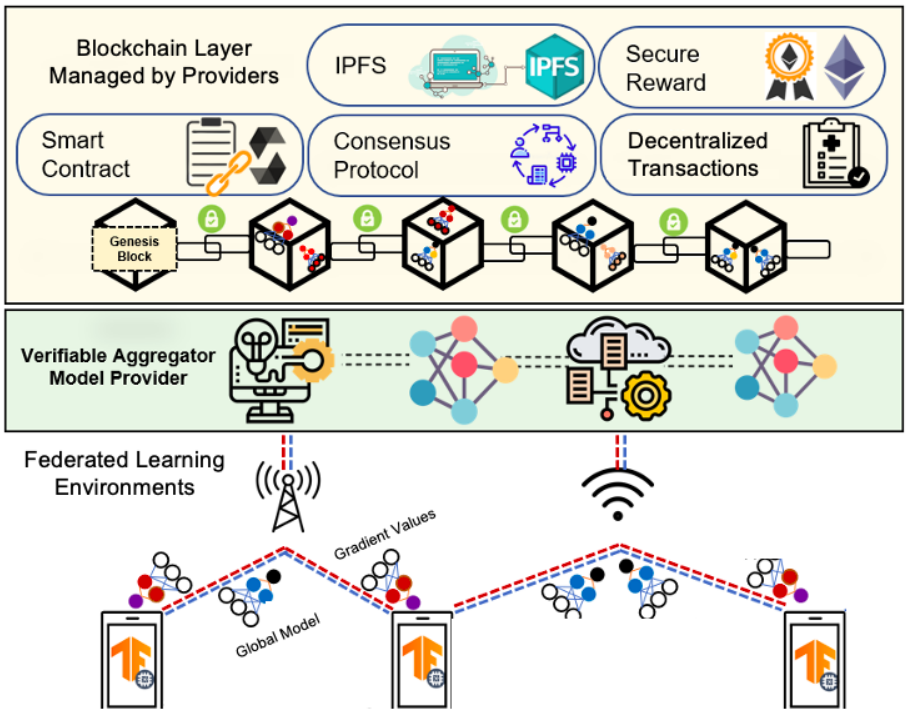


Figure 3. The integration of blockchain and federated learning. There are three layers: the blockchain layer, the verifiable aggregator model provider layer, and the federated learning layer.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

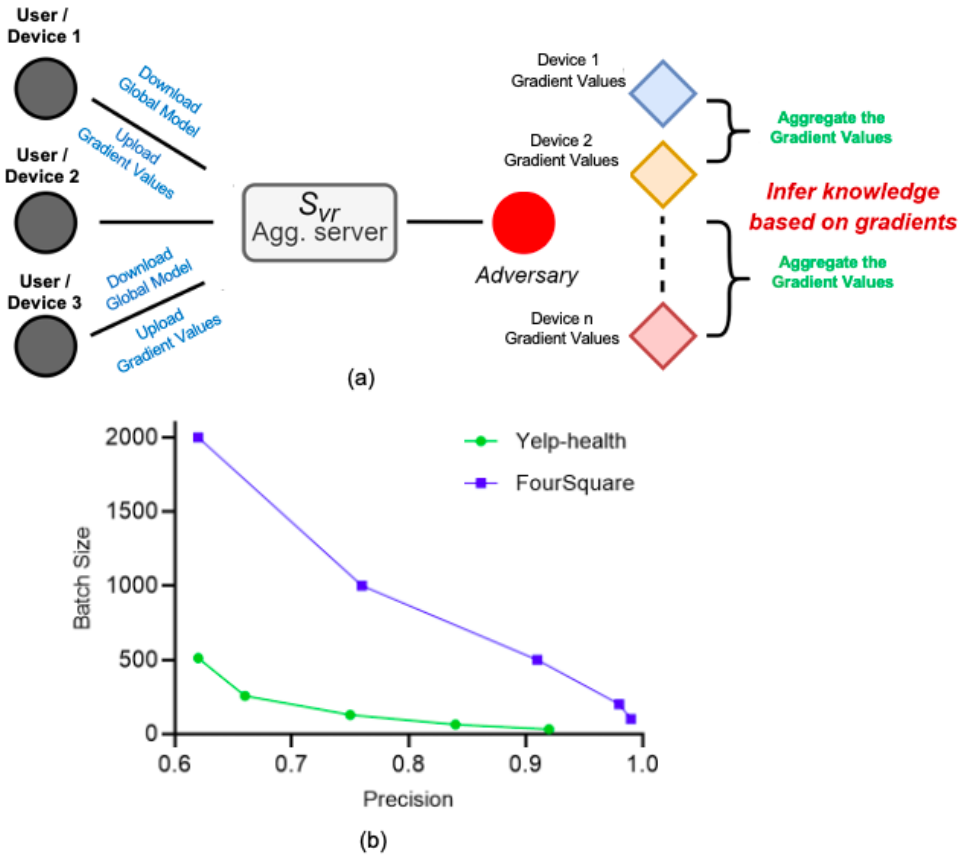


Figure 4. (a) The present study examines the phenomenon of inference membership attack within the context of a federated learning system. The adversary can infer the knowledge through the analysis of the gradients uploaded by users; (b) The results of inference membership attack.

Figure 4 (a) illustrates an overview of the inference membership attack, which involves inferring training data features inside a collaborative distributed learning setting. The adversary can capture the findings of the collaborative model. In broad terms, the disparity in value between the revised gradient derived from the users is equivalent to the cumulative updates contributed by all data owners. The adversary has the capability to acquire information about the dataset by disclosing the feature that is utilised to forecast the output, taking into account the input and its corresponding gradient values. The opponent gains knowledge of the parameters, enabling them to disclose the characteristics of the model that are not associated with the output. In summary, the adversary acquires information about the training dataset, including age, gender, patient health records, and to name a few.

The previous study (Melis et al., 2019) introduced a method for membership inference, which reveals unwanted details about the training data of a user. The opponent intends to disclose the training data, whereas the primary objective of collaborative learning is to safeguard user privacy. Therefore, the unauthorised disclosure of data poses a significant threat to the overall integrity and security of the system. Hence, in order to assess and examine the membership inference attack, healthcare-related data from *Yelp-health* and *FourSquare* data have been utilised. The evaluation process involves the selection of the 5,000 most frequently occurring terms for the *Yelp-health* dataset and identifying 30,000 important locations within the *FourSquare* dataset. The initial stage involves the adversary constructing a bag-of-words model, a commonly employed technique in natural language processing. The target refers to the training data that the user wants to infer. The data is subsequently partitioned into batches, enabling the attacker to construct a batch bag of words. If the examination outcomes are included in a collection of bag-of-words, the adversary can infer that the input originated from the same collection.

The outcome of the inference attack is illustrated in Figure 4 (b). In summary, with the increase in batch sizes, there is a corresponding rise in the generation of false positives by this particular attack.

Pseudonymous blockchain and federated learning are two discrete concepts within technology and data privacy. Pseudonymity refers to the practice of identifying users through the use of pseudonyms or aliases rather than their actual real-world identities. Within the realm of blockchain technology, individuals have the capability to generate cryptographic addresses or keys for the purpose of representing their identities. Although the addresses in question are not explicitly linked to tangible individuals, all transactions linked to these addresses are candidly documented on the blockchain. Within the framework of federated learning, transactions commonly pertain to the transfer of model updates or aggregated model parameters among the devices or servers involved in the process. These transactions facilitate the integration of knowledge from all participants into the global model while maintaining raw data's localisation and privacy. Federated learning transactions differ from blockchain-based financial transactions. The primary emphasis lies on the exchange of model updates and the collective enhancement of machine learning models while upholding the need to protect data privacy.

The current generation of smart contracts, exemplified by Ethereum smart contracts, is limited to executing basic computational tasks and falls short in meeting the demands of real-world artificial intelligence applications. The presence of smart contracts on the blockchain enables parties to encode self-executing codes without the need for third-party intervention. Nevertheless, the problem pertaining to conventional contracts addressing the aforementioned aspects has been resolved. (i) The process of execution is now in progress. In the event that both parties are in mutual agreement with the specified conditions, the smart contract will autonomously execute the programmed instructions without any external intervention. The blockchain system ensures the availability of data records, as it maintains a comprehensive history of transactions. (iii) The efficiency of the smart contract is notable. The execution occurs rapidly, typically within a few of seconds. The cost is minimal. The utilisation of this approach eliminates the need for physical documentation and reduces reliance on external entities. The implementation of smart contracts effectively mitigates the need for user facilitation by minimising instances of user error and fraudulent activities. The integration and innovation of artificial intelligence (AI) in smart contract technology has the potential to offer a robust and streamlined approach to decentralised systems, facilitating engaging experiences for all involved parties.

## 4. CONCLUSION

Ensuring users' privacy is a vital principle in implementing the intelligent cross-silo federated learning system across untrusted edge networks. This study has introduced the concept of privacy awareness in decentralized methodologies as viable strategies to mitigate the linkability issue in blockchain and federated learning methodologies. The significance of these concerns arises from the fact that while the current schemes offer diverse privacy approaches, they do not adequately address the issue of linkability inside the systems. Therefore, this study highlights the additional protocols to implement in federated learning and blockchain smart contracts. In addition to considering the advantages of the proposed approach, it is also essential to examine the future implications of the centralized aggregation server's involvement in computing the gradient values. The aggregation server is susceptible to experiencing bottleneck problems, which might result in it becoming an SPoF due to the fundamental nature of the centralized method. Hence, this study highlights the substitution of centralized aggregation servers with distributed computing entities utilizing blockchain technology in the foreseeable future.

## ACKNOWLEDGEMENTS

The authors would like to thank Lembaga Penelitian dan Pengabdian Masyarakat Universitas Negeri Padang for funding this work with a contract number : 1776/UN35.15/LT/2024.

## REFERENCES

[1] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *ACM Comput Surv*, vol. 52, no. 3, pp. 1–34, May 2020, doi: 10.1145/3316481.

[2] M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: A Blockchain System for Private and Secure Federated Learning," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 7, pp. 1513–1525, Jul. 2021, doi: 10.1109/TPDS.2020.3044223.

[3] D. C. Nguyen *et al.*, "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges," *IEEE Internet Things J*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021, doi: 10.1109/JIOT.2021.3072611.

[4] D. Li *et al.*, "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey," *Soft comput*, vol. 26, no. 9, pp. 4423–4440, May 2022, doi: 10.1007/s00500-021-06496-5.

[5] Z. Li, J. Liu, J. Hao, H. Wang, and M. Xian, "CrowdSFL: A Secure Crowd Computing Framework Based on Blockchain and Federated Learning," *Electronics (Basel)*, vol. 9, no. 5, p. 773, May 2020, doi: 10.3390/electronics9050773.

[6] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: a systematic literature review," *Artif Intell Rev*, vol. 56, no. 5, pp. 3951–3985, May 2023, doi: 10.1007/s10462-022-10271-9.

[7] S. R. Pokhrel and J. Choi, "Federated Learning With Blockchain for Autonomous Vehicles: Analysis and Design Challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020, doi: 10.1109/TCOMM.2020.2990686.

[8] S. Wang, X. Tang, Y. Zhang, and J. Chen, "Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts," *IEEE Access*, vol. 7, pp. 109439–109453, 2019, doi: 10.1109/ACCESS.2019.2933860.

[9] H. R. Hasan and K. Salah, "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts," *IEEE Access*, vol. 6, pp. 65439–65448, 2018, doi: 10.1109/ACCESS.2018.2876971.

[10] S. Rahmadika and K. H. Rhee, "Enhancing data privacy through a decentralised predictive model with blockchain-based revenue," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 37, no. 1, p. 1, 2021, doi: 10.1504/IJAHUC.2021.115104.

[11] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered Federated Learning: Challenges, Solutions, and Future Directions," *ACM Comput Surv*, vol. 55, no. 11, pp. 1–31, Nov. 2023, doi: 10.1145/3570953.

[12] S. Rahmadika and K.-H. Rhee, "Unlinkable Collaborative Learning Transactions: Privacy-Awareness in Decentralized Approaches," *IEEE Access*, vol. 9, pp. 65293–65307, 2021, doi: 10.1109/ACCESS.2021.3076205.

[13] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey," *ACM Comput Surv*, vol. 55, no. 9, pp. 1–43, Sep. 2023, doi: 10.1145/3560816.

[14] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards Privacy in a Smart Contract World," 2020, pp. 423–443. doi: 10.1007/978-3-030-51280-4_23.

[15] C. Antal, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Distributed Ledger Technology Review and Decentralized Applications Development Guidelines," *Future Internet*, vol. 13, no. 3, p. 62, Feb. 2021, doi: 10.3390/fi13030062.

[16] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani, and X. Wei, "Blockchain Meets Federated Learning in Healthcare: A Systematic Review With Challenges and Opportunities," *IEEE Internet Things J*, vol. 10, no. 16, pp. 14418–14437, Aug. 2023, doi: 10.1109/JIOT.2023.3263598.

[17] S. Rathore, B. Wook Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *Journal of Network and Computer Applications*, vol. 143, pp. 167–177, Oct. 2019, doi: 10.1016/j.jnca.2019.06.019.

[18] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing Blockchain and AI With Metaverse: A Survey," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, 2022, doi: 10.1109/OJCS.2022.3188249.

[19] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. Alabdulatif, "A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data," *Comput Biol Med*, vol. 167, p. 107630, Dec. 2023, doi: 10.1016/j.compbiomed.2023.107630.

[20] A. Heidari, D. Javaheri, S. Toumaj, N. J. Navimipour, M. Rezaei, and M. Unal, "A new lung cancer detection method based on the chest CT images using Federated Learning and blockchain systems," *Artif Intell Med*, vol. 141, p. 102572, Jul. 2023, doi: 10.1016/j.artmed.2023.102572.

[21] D. Mahmudnia, M. Arashpour, and R. Yang, "Blockchain in construction management: Applications, advantages and limitations," *Autom Constr*, vol. 140, p. 104379, Aug. 2022, doi: 10.1016/j.autcon.2022.104379.

[22] S. JANG, S. RAHMADIKA, S. U. SHIN, and K.-H. RHEE, "PDPM: A Patient-Defined Data Privacy Management with Nudge Theory in Decentralized E-Health Environments," *IEICE Trans Inf Syst*, vol. E104.D, no. 11, p. 2021NGP0015, Nov. 2021, doi: 10.1587/transinf.2021NGP0015.

[23] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Networks*, vol. 152, p. 103320, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.

[24] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[25] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Ethereum Smart Contract Analysis Tools: A Systematic Review," *IEEE Access*, vol. 10, pp. 57037–57062, 2022, doi: 10.1109/ACCESS.2022.3169902.

[26] S. Shitharth *et al.*, "Federated learning optimization: A computational blockchain process with offloading analysis to enhance security," *Egyptian Informatics Journal*, vol. 24, no. 4, p. 100406, Dec. 2023, doi: 10.1016/j.eij.2023.100406.

[27] Y. Lin *et al.*, "DRL-Based Adaptive Sharding for Blockchain-Based Federated Learning," *IEEE Transactions on Communications*, vol. 71, no. 10, pp. 5992–6004, Oct. 2023, doi: 10.1109/TCOMM.2023.3288591.

[28] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Networks*, vol. 152, p. 103320, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.

[29] A. Hadi, S. Rahmadika, B. R. Fajri, G. Farell, K. Budayawan, and W. Lofandri, "Obscuring Transaction Information in Decentralized P2P Wireless Networks," *IEEE Access*, vol. 11, pp. 111053–111067, 2023, doi: 10.1109/ACCESS.2023.3321960.

[30] H. Zhang, S. Jiang, and S. Xuan, "Decentralized federated learning based on blockchain: concepts, framework, and challenges," *Comput Commun*, vol. 216, pp. 140–150, Feb. 2024, doi: 10.1016/j.comcom.2023.12.042.

[31] S. Ji, J. Zhang, Y. Zhang, Z. Han, and C. Ma, "LAFED: A lightweight authentication mechanism for blockchain-enabled federated learning system," *Future Generation Computer Systems*, vol. 145, pp. 56–67, Aug. 2023, doi: 10.1016/j.future.2023.03.014.