Blockchain-Enabled Technique for Privacy Preserved Medical Recommender System

M. Ajaykumar
Assistant Professor, Guru Nanak Institute of Technology, CSE Department, Hyderabad.

ABSTRACT: With the proliferation of privacy issues surrounding the Internet of Medical (IoMT) recommender system data, this study presents a Secure Recommendation and Training Technique (SERTT) which is contingent on a combination of both federated learning and blockchain approaches. Firstly, the study presents a new framework for recording, sorting, and transmission of IoMT data while incorporating blockchain to ensure that the IoMT data transmitted to cloud servers is not made vulnerable by the sharing of the original data. Secondly, by utilizing medical data, the study designs a Recommender Data Management Neural Architecture (REDMANA) which is based on federated learning and model searching training framework. The proposed technique guarantees that the model gradients which are trained by each node are not disclosed all through the universal training and modelling procedure. This makes the raw data inaccessible to either the IoMT data provider or the user. Considering that the model ensures that users can only obtain their necessary inquiries, neither medical data suppliers nor users can obtain access to raw data. Thus, it reduces the issues of safeguarding medical data sets to the issues of securing data processing. Using numerical analysis and experiments the proposed technique is compared with other existing techniques, the result shows that the proposed SERTT system is efficient and secures recommender data management training and modelling technique and that it performs previously designed techniques as compared.

I. INTRODUCTION

A recommender system is a subclass of an artificial intelligent-based (AI-based) system for information filtering and prediction on a list of products for different organizations [1]. Generally, such kinds of systems are common big data applications. On the internet of medical things (IoMT) system, several hospitals extensively utilize the recommender system to obtain excellent recommendations based on the interest and requests of their patients. The recommender system can generate its recommendations through either collaborative filtering or content-based filtering. The former is a method of obtaining the list of predictions by establishing the interrelation between users' history and other users' interests, while the latter involves exploring both the user's profile and their corresponding items. Most hospitals and companies store users' confidential data and make use of collaborative filtering to achieve optimal recommendations. In this kind of recommendation, the profiles of different users are designed from their respective histories coupled with the user's rating. Consequently, there is the possibility of having the issue of data privacy in an AI-based system. Recently, hospitals gathered and save a massive quantity of patient data for future recommendations, however, patients are concerned about the privacy of their confidential data which are stored on different platforms (such as smart healthcare and other IoT devices). Nowadays, users' data can be disclosed through different means such as social media and through intrusion.

II. LITERATURE REVIEW

G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella has discussed that despite an increased focus on the security of electronic health records and an effort by large cities around the globe to pursue smart city infrastructure, the private information of patients is subject to data breaches on a regular basis. Previous efforts to combat this have resulted in data being mostly inaccessible to patients. Existing record management systems struggle with balancing data privacy and the need for patients and providers to regularly interact with data. Blockchain technology is an emerging technology that enables data sharing in a decentralized and transactional fashion. Blockchain technology can be leveraged in the healthcare domain to achieve the delicate balance between privacy and accessibility of electronic health records. In this paper, we propose a blockchain- based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while

preserving the privacy of patients' sensitive information. Our framework, named Ancile, utilizes smart contracts in an Ethereum-based blockchain for heightened access control and obfuscation of data, and employs advanced cryptographic techniques for further security. The goals of this paper are to analyze how Ancile would interact with the different needs of patients, providers, and third parties, and to understand how the framework could address longstanding privacy and security concerns in the healthcare industry.

K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander had discussed that Federated Learning is a distributed machine learning approach which enables model training on a large corpus of decentralized data. We have built a scalable production system for Federated Learning in the domain of mobile devices, based on TensorFlow. In this paper, we describe the resulting high-level design, sketch some of the challenges and their solutions, and touch upon the open problems and future directions. Federated Learning (FL) (McMahan et al., 2017) is a distributed machine learning approach which enables training on a large corpus of decentralized data residing on devices like mobile phones. FL is one instance of the more general approach of "bringing the code to the data, instead of the data to the code" and addresses the fundamental problems of privacy, ownership, and locality of data.

M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen had discussed that with rapid development of computing technologies, large amount of data are gathered from edge terminalsor Internet of Things (IoT) devices, however data trust and security in edge computing environment are very important issues to be considered, especially when the gathered data are fraud or dishonest, or the data are misusedor spread without any authorization, which may lead to serious problems. In this article, a blockchain-based trusteddata management scheme (called BlockTDM) in edge computing is proposed to solve the above problems, in which we proposed a flexible and configurable blockchain architecture that includes mutual authentication protocol, flexible consensus, smart contract, block and transaction data management, blockchain nodes management, and deployment. The BlockTDM scheme can support matrix-based multichannel data segment andisolation for sensitive or privacy data protection, and moreover, we have designed user-defined sensitive data encryption before the transaction payload stores in blockchain system and have implemented conditional accessand decryption query of the protected blockchain data and transactions through smart contract. Finally, we have evaluated the proposed BlockTDM scheme security, availability, and efficiency with large number of experiments. Analysis and evaluations manifest that the proposed BlockTDM scheme provides a general, flexible,and configureurable blockchain-based paradigm for trusted data management with tamper-resistance, which is suitable for edge computing with high-level security and creditability.

C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo had discussed that web security plays a very crucial role in the Security of Things (SoT) paradigm for smart healthcare and will continue to be impactful in medical infrastructures soon. This paper addressed a key component ofsecurity-intrusion detection systems due to the number of web security attacks, which have increased dramaticallyin recent years in healthcare, as well as the privacy issues. Various intrusion-detection systems have been proposedin different works to detect cyber threats in smart healthcare and to identify network-based attacks and privacy violations. This study was carried out because of the limitations of the intrusion detection systems in respondingto attacks and challenges and in implementing privacy control and attacks in the smart healthcare industry. The research proposed a machine learning support system that combined a Random Forest (RF) and a genetic algorithm: a feature optimization method that built new intrusion detection systems with a high detection rate anda more accurate false alarm rate. To optimize the functionality of our approach, a weighted genetic algorithm andRF were combined to generate the best subset of functionality that achieved a high detection rate and a low falsealarm rate. This study used the NSL-KDD dataset to simultaneously classify RF, Naive Bayes (NB) and logistic regression classifiers for machine learning. The results confirmed the importance of optimizing functionality, which gave better results in terms of the false alarm rate, precision, detection rate, recall and F1 metrics.

D. Ngabo, D. Wang, C. Iwendi, J. H. Anajemba, L. A. Ajao had discussed that the recent developments in fog computing architecture and cloud of things (CoT) technology includes data mining management and artificial intelligence operations. However, one of the major challenges of this model isvulnerability to security threats and cyber-attacks against the fog computing layers. In such a scenario, each of the layers are susceptible to different intimidations, including the sensed data (edge layer), computing and processing of data (fog (layer), and storage and management for public users (cloud). The conventional data storage and security mechanisms that are currently in use appear to not be suitable for such a huge amount of generated data in the fog computing architecture. Thus, the major focus of this research is to provide security countermeasures against medical data mining threats, which are generated from the sensing layer (a human wearable device) and storage of data in the cloud database of internet of things (IoT). Therefore, we propose a public-permissioned blockchain security mechanism using elliptic curve crypto (ECC) digital signature that that supports a distributed ledger database (server) to provide an immutable security solution, transaction transparency and prevent the patient records tampering at the IoTs fog layer. The blockchain technology approach also helps to mitigate these issues of latency, centralization, and scalability in the fog model.

Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood had discussed that Federated learning (FL) has experienced a boom in recent years, which is jointly promoted by the prosperity of machine learning and Artificial Intelligence along with emerging privacy issues. In the FL paradigm, a central server and local end devices maintain the same model by exchanging model updates instead of raw data, with which the privacy of data stored on end devices is not directly revealed. In this way, the privacy violation causedby the growing collection of sensitive data can be mitigated. However, the performance of FL with a central serveris reaching a bottleneck, while new threats are emerging simultaneously. There are various reasons, among whichthe most significant ones are centralized processing, data falsification, and lack of incentives. To accelerate the proliferation of FL, blockchain-enabled FL has attracted substantial attention from both academia and industry. A considerable number of novel solutions are devised to meet the emerging demands of diverse scenarios. Blockchain-enabled FL provides both theories and techniques to improve the performance of FL from various perspectives. In this survey, we will comprehensively summarize and evaluate existing variants of blockchain- enabled FL, identify the emerging challenges, and propose potentially promising research directions in this under-explored domain.

III. METHODOLOGY

The scope of implementing a blockchain-enabled privacy-preserving medical recommender system encompassesseveral key aspects. Firstly, it involves the design and development of a decentralized blockchain infrastructure capable of securely storing and managing sensitive patient data while ensuring compliance with healthcare privacy regulations. This infrastructure should facilitate encrypted storage of medical records, preferences, and consent preferences, utilizing techniques like homomorphic encryption and smart contracts to preserve privacy and enforce access control.

Disadvantages of existing system:

- However, patients are concerned about the privacy of their confidential data which are stored on different platforms (such as smart healthcare and other IoT devices).
- Nowadays, users' data can be disclosed through different means such as social media and throughintrusion attacks.

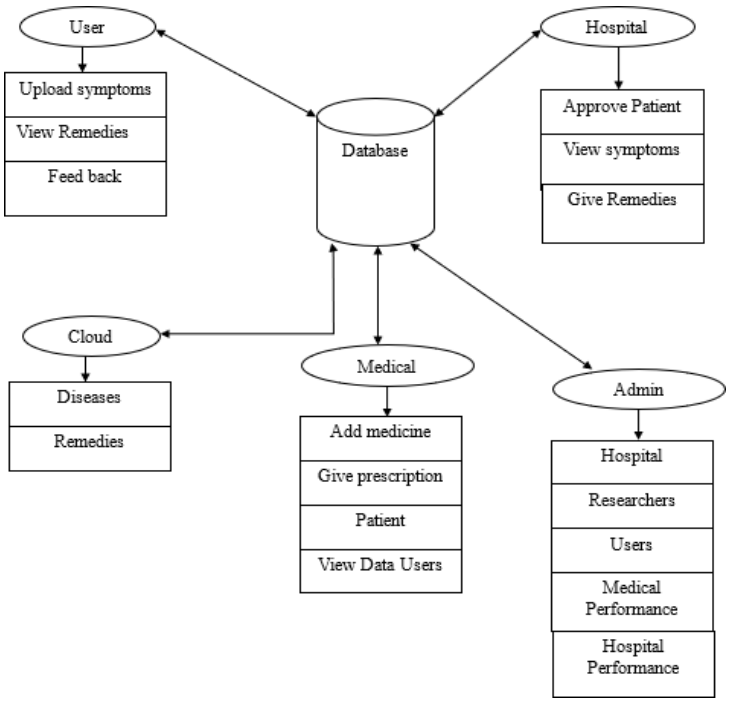
PROPOSED SYSTEM

- In this paper, this study proposes a recommender and data sharing framework which utilizes federated learning and secured medical guarantee systems.
- Proposing and implementing a blockchain-based recommender and training system which is referred to as Secured Recommender and Training Technique (SERTT), which locally stores data but uploads data directories and structures to the chain.
- Through federated learning, users are trained about the data which eventually produces a model instead of giving out the actual user data, thereby enhancing the privacy and security of user information.

Advantages Proposed System Advantages

- Providing more security
- Proposing and implementing a blockchain-based recommender and training system which is referred to as Secured Recommender and Training Technique (SERTT), which locally stores data but uploads data directories and structures to the chain.

SYSTEM ARCHITECTURE



The system architecture for a blockchain-enabled technique in privacy-preserved medical recommendations integrates several key components: users, hospitals, medical professionals, cloud storage, and administrators, all interconnected through a central database. Blockchain technology ensures secure, immutable, and transparent transactions, preserving patient privacy and enhancing data security. Users can upload symptoms and receive remedies, while hospitals and medical professionals provide approvals, treatments, and prescriptions. Cloud storage offers a repository for disease and remedy information, and administrators oversee the system's performance, ensuring compliance and efficiency in medical data management.

MODULES:

User Interface Design: To connect with server user must give their username and password then only they can be able to connect the server. If the user already exits directly can login into the server else, user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

User: The owner of the data uses cloud storage service to store the files. Before data outsourcing, the owner of the data extracts the set of keywords from the file and encrypts in a safe index. The document is also encrypted to Encrypted text During the encryption process, the access policy is specified and embedded in the ciphertext to perform fine-grained access control. There will be 3 data owners in our paper, a public key and a secret key will be generated at the time of uploading the file.

Admin: This is the fourth module of this paper. In this module admin can also see all hospitals approved details. Admin can also have a user details. Admin can also see some researches in the medicines details. Admin can also see a hospital performance in the graph line according to the feedback we can calculate a performance.

Admin can also see a medical performance according to the patient's feedback given we can calculate the performance. It will all store at admin

Hospital: This is the Second module of this paper. In hospitals it can see all the patients of a diseases. Hospital can also see patient details. Hospital can see a remedy. And hospital can also take feedback of patients. Patients have a give a feedback of a hospital management and systems.

Cloud: This is the fifth module in the cloud we can stores all the data. In cloud we have store a diseases and remedies. If in real time cloud, we can store a admin part and cloud data in the cloud database. Now in our paper we can store in Mysql database.

IV. IMPLEMENTATION:

PRIVATE BLOCKCHAIN:

A completely private blockchain refers to a blockchain with writing permission only in the hands of one organization. Data access and writing have very strict permissions. In most cases, such data are not publicly readable. Essentially, compared with a system that is completely open and uncontrolled and guarantees network security through an encrypted economy, the private blockchain can create a system with stricter access control, and modification or even reading permissions can be limited to a few users. At the same time, this system retains the authenticity and partial decentralization of a blockchain. The private blockchain has limited read permissions, low transaction costs, easy-to-modify rules, and few nodes participating in blockchain activities, which make various operations in the private blockchain highly efficient.

Four Basic Algorithms:

Setup (1^{λ}):

The DO initializes the system locally, inputs the parameter λ, and outputs the master key k←{0,1}λ. The empty sets Map and EDB are initialized, where Map is used to record the updating and search status. The PPSE scheme uses the KC-IDC index structure, which is stored in the encrypted index set EDB in the form of (w, id) pairs, where w and id are the keyword and file identifier, respectively.

Search (k, Map, G, w):

As shown in Algorithm 2, the private blockchain forwards the received access control information to the DU, who then sends a search token to the private blockchain. After calculation, user Uj is determined as an authorized user. Then, the smart contract is called on the private blockchain to perform the search operation. First, an empty list LR is created to obtain the status information of the keyword. The DU generates a new token for the search keyword and judges ST. If it is equal to Y, then the keyword has not been updated after the search; otherwise, the updated index of this keyword has not yet been searched, and the latest index pointer, ptri, needs to be calculated.

Addition (k, G, Hash, map):

As shown in Algorithm 3, the DO obtains the update status corresponding to the keyword w. If S is equal to Y, then it represents the first update after the keyword search and that the number of searches that need to be updated is s. The new key is used to generate a new token and index pointer. Finally, S is set to N. Otherwise, it means that the key has not been searched after the update, and the previous key k and token can be used. The new index is identified after the pointer is connected to the previous pointer. After obtaining the encrypted data, the hash function operation is performed, and the obtained hash value is used as input to call the smart contract, adding the data to the private blockchain and uploading the corresponding encryption to the public blockchain at the same time. Then, the DO updates Map.

Delete (b1lo Ckno, db(w), edb):

As shown in Algorithm 4, the DO uses the block number blockNo as an input to call the deleted smart contract and execute the corresponding action according to the input block number. During the data deletion operation, the DO also deletes the encrypted documents in the public blockchain.

V. EXPERIMENTAL RESULTS

HOME PAGE

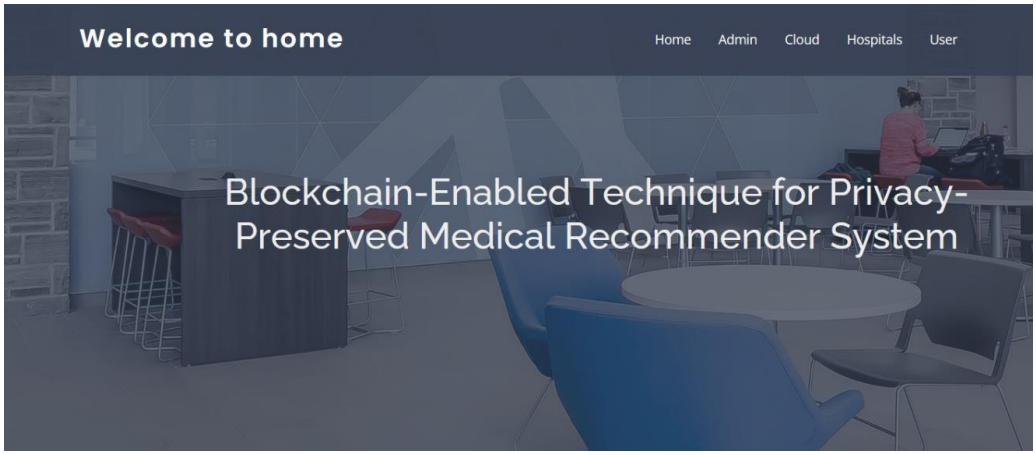


Figure: The Home Page for the Recommender System

- It Consists of registrations and logins for Admin, Cloud, Hospital and Users

USER LOGIN PAGE

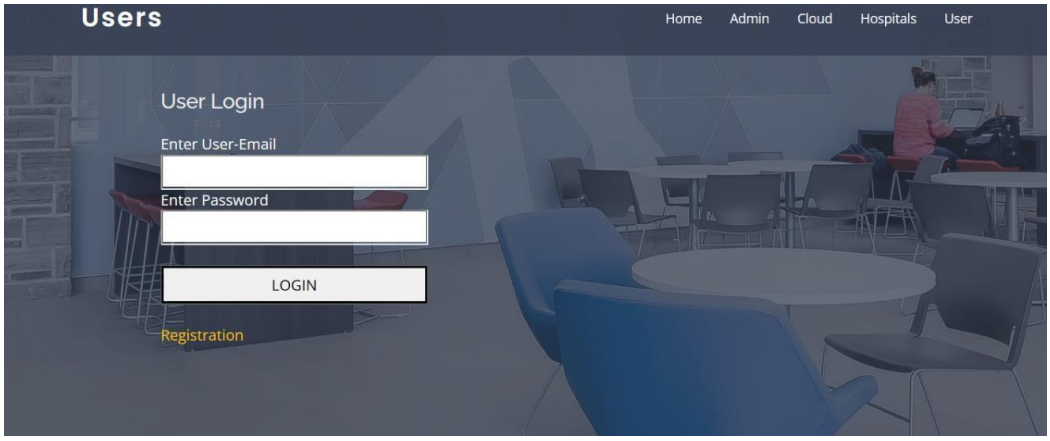


Figure: User's Login Page

DISEASE UPLOAD PAGE

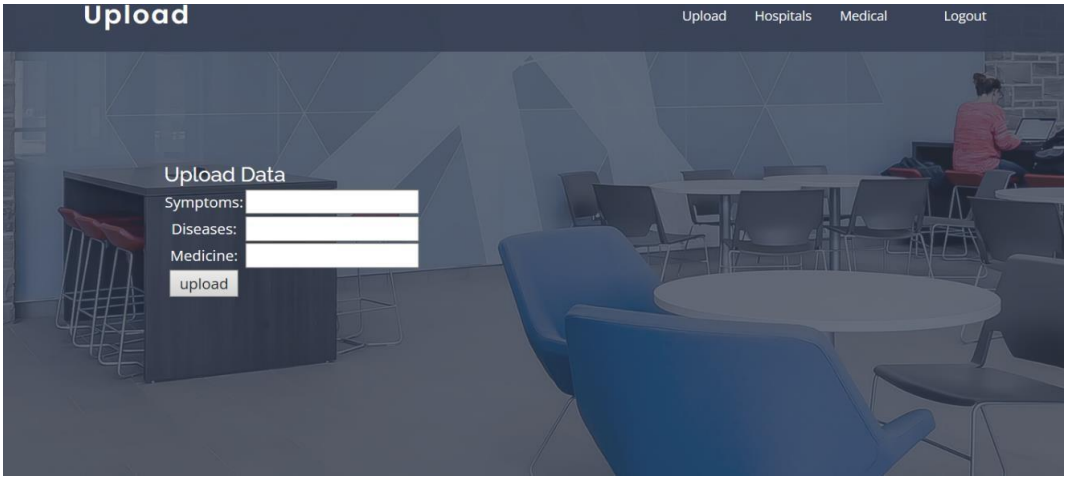


Figure: Page to Upload disease data

- Users can upload their disease from the given options.

HOSPITAL VIEW PAGE

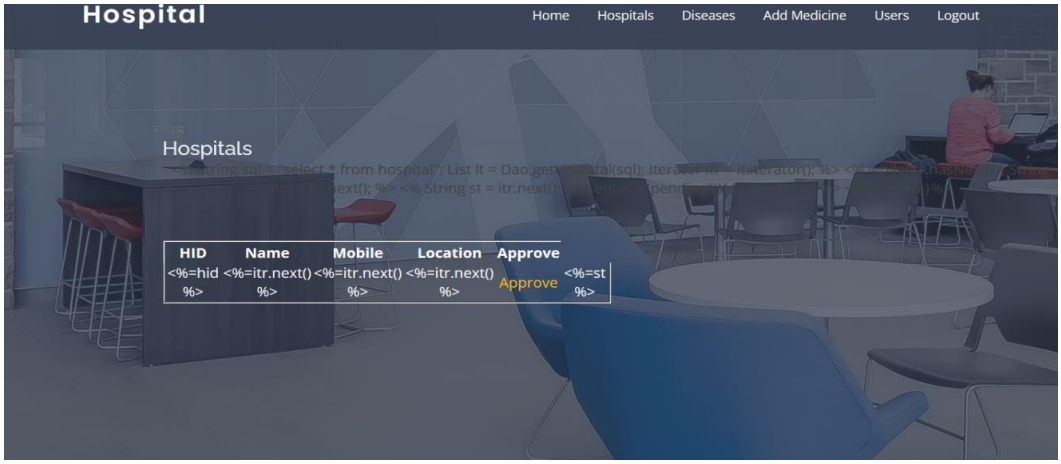


Figure: Viewing the Hospital Page

Hospital can fetch the data where the hospital is approved or not.

VI. CONCLUSION

Traditional privacy-preserving SE schemes rely on cloud servers to complete search operations. In this study, based on blockchain technology, a decentralized security model is designed to solve the problems of original malicious servers and attacks from malicious users. Compared with the existing verification schemes, the PPSE does not require the DO to verify, nor does it require them to send the results to a third party for verification. Using the blockchain itself to store data can obtain correct and immutable results. At the same time, we store the encrypted index in the private blockchain while outsourcing the corresponding encrypted documents to the public blockchain, and the access control mechanism is introduced to improve the query efficiency and the security of the encrypted data. The safety analysis indicates that the scheme meets the safety requirements, and the experimental results obtained concerning our prototype demonstrate the practicability of our scheme.

VII. FUTURE ENHANCEMENT

The safety analysis conducted reveals that our proposed scheme, leveraging blockchain-enabled techniques for privacy-preserved medical recommendations, satisfactorily meets the stringent safety requirements mandated for medical data handling. Through a comprehensive examination of potential vulnerabilities and risk mitigation strategies, our scheme ensures robust protection of sensitive medical information against unauthorized access and tampering.

VIII. REFERENCES:

[1] S. B. Patel, P. Bhattacharya, S. Tanwar, and N. Kumar, ‘‘KiRTi: A blockchain-based credit recommender system for financial institutions,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1044–1054, Apr. 2021.

[2] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, ‘‘Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,’’ Sustain. Cities Soc., vol. 39, pp. 283–297, May 2018.

[3] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K.-R. Choo, ‘‘A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems,’’ IEEE Access, vol. 6, pp. 28203–28212, 2018.

[4] R. Bosri, M. S. Rahman, M. Z. A. Bhuiyan, and A. Al Omar, ‘‘Integrating blockchain with artificial intelligence for privacy-preserving recommender systems,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1009–1018, Apr. 2021.

[5] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, ‘‘Blockchain for industry 4.0: A comprehensive review,’’ IEEE Access, vol. 8, pp. 79764–79800, 2020.

[6] D.Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, ‘‘A survey on blockchain for information systems management and security,’’ Inf. Process. Manage., vol. 58, no. 1, Jan. 2021, Art. no. 102397.

[7] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, ‘‘A blockchained federated learning framework for cognitive computing in industry 4.0 networks,’’ IEEE Trans. Ind. Informat., vol. 17, no. 4, pp. 2964–2973, Apr. 2021.

[8] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, ‘‘A blockchain-based trusted data management scheme in edge computing,’’ IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 2013–2021, Mar. 2020.

[9] L. Xu, T. Bao, and L. Zhu, ‘‘Blockchain empowered differentially private and auditable data publishing in industrial IoT,’’ IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7659–7668, Nov. 2021

[10] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, ‘‘Federated learning in mobile edge networks: A comprehensive survey,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

[11] L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. H. Nguyen, and C. S. Hong, ‘‘Federated learning for edge networks: Resource optimization and incentive mechanism,’’ IEEE Commun. Mag., vol. 58, no. 10, pp. 88–93, Oct. 2020.

[12] H. Kim, J. Park, M. Bennis, and S.-L. Kim, ‘‘Blockchained on-device federated learning,’’ IEEE Commun. Lett., vol. 24, no. 6, pp. 1279–1283, Jun. 2020.

[13] K. Maier-Hein, S. Ourselin, M. Sheller, R. M. Summers, A. Trask, D. Xu, M. Baust, and M. J. Cardoso, ‘‘The future of digital health with federated learning,’’ NPJ Digit. Med., vol. 3, no. 1, pp. 1–7, Sep. 2020.

[14] C. Iwendi, S. Khan, J. H. Anajemba, A. K. Bashir, and F. Noor, ‘‘Realizing an efficient IoMT-assisted patient diet recommendation system through machine learning model,’’ IEEE Access, vol. 8, pp. 28462–28474, 2020, doi: 10.1109/ACCESS.2020.2968537.

[15] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander, ‘‘Towards federated learning at scale: System design,’’ 2019, arXiv:1902.01046.

[16] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, ‘‘A survey on federated learning,’’ Knowl.-Based Syst., vol. 216, Mar. 2021, Art. no. 106775.

[17] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, ‘‘Security of things intrusion detection system for smart healthcare,’’ Electronics, vol. 10, no. 12, p. 1375, Jun. 2021.

[18] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, ‘‘A survey on security and privacy of federated learning,’’ Future Gener. Comput. Syst., vol. 115, pp. 619–640, Feb. 2021.

[19] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, ‘‘Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges,’’ IEEE Commun. Surveys Tuts., vol. 23, no. 3, pp. 1759–1799, 3rd Quart., 2021.

[20] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, and X. Zheng, ‘‘Privacy-preserving federated learning framework based on chained secure multiparty computing,’’ IEEE Internet Things J., vol. 8, no. 8, pp. 6178–6186, Apr. 2021.