UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

ENHANCING DATA SECURITY REWARD MODEL REPUTATION IN BLOCK CHAIN USING ARTIFICIAL NEURAL NETWORK

Ayuluri Sri Lakshmi[1],Prasad Devarasetty[2],M James Stephen[3], Anumula Sruthi[4]

[1]M.Tech Scholor, CSE Department, DVR & Dr.HS MIC College of Technology, Kanchikacherla, NTR District, AP, India

[2]Professor, CSE Department, DVR & Dr.HS MIC College of Technology, Kanchikacherla, NTR District, AP,India

[3]Professor, Andhra University, Visakhapatnam, Andhra Pradesh, India

[4]Assistant professor, CSE Department, Koneru lakshmaih education foundation, NTR district, Andhra Pradesh, india

ABSTRACT: This paper introduces a novel block chain-based approach for secure and efficient database management. Block chain technology, with its decentralized, immutable, and transparent nature, offers significant advantages over traditional systems, particularly in enhancing data security, integrity, and auditability. It takes large number of devices to collectively train a global model by collaborating with a server datasets on their respective premises. We design a decentralized attribute-based access control mechanism with an auxiliary Trust and Reputation System (TRS) for IoT authorization We present the research paper is developed practical privacy security analytics in information systems.With that note, this paper proposes a new model called Block Chain based Advanced Data Security-Reward Model (DSecCS) for enhancing data security and attack resistance. There has been a significant rise in the volume of information produced as well as the take different involved in its data type. We propose a mapping framework to employ a fine-tuned multilayer feed forward artificial neural network (ANN) and extreme learning machine (ELM) for role engineering in the SCADA-enabled IIoT environment to ensure privacy and user access rights to resources. The proposed model comprises of three sections, as, Construction of Intellectual CS Model, Confusion Model and Incorporation of Block-Chain.Support Vector Machine (SVM), k-nearest Neighbors (KNN), and Convolutional Neural Network (CNN) in terms of accuracy, false positive rate, false negative rate, precision, recall.

INDEX TERMS: Block Chain, Crowd sensing, Data Security, Reward, Data Privacy.

1. INTRODUCTION

The Information Technology (IT) and Advanced Communication models are used for observing, sensing, evaluating and integrating distinctive data in Smart Cities for performing intelligent and

smooth operations [1]. The production control system with industrial control and monitoring capabilities that provides multiple enterprise-related services. IoT applications is recently deployed in cross-industry applications based on the principles of public information services [2]. In this scheme, access control is enforced by the resource owner by searching the block chain for such records. In addition, the authors in [5] This introduction explores the fundamental principles of block chain technology and its potential benefits and challenges when applied to database management[3]. The advantages of collaborative learning they are two major concerns input data security and vulnerability of locally trained models to data leakage [4]. It was developed for monitoring transactions including decentralized digital currency every node in the P2P network can receive updated data regarding the different transactions validated in a decentralized and distributed database [5]. The selection of data security method is design of security preserving analytics algorithms. The protection techniques only provide room for limited operations on the obfuscated data complex algorithms is disintegrated to these simpler operations [6]. Formed and standardized by the National Institute of Standards and Technology (NIST) the SHA (Secure Hash Algorithm) gives ideal performance in maintaining data integrity process. Taking offline supervised learning is example datasets should be available to the model during the training process. This model is not usable unless the training process is completed [7]. Online continuous machine learning is useful for handling the learning process in large-scale machine learning tasks on dynamic systems such as IIoT systems [8]. Intrusion detection systems (IDS), leveraging machine learning algorithms and anomaly detection techniques, enable the timely detection and mitigation of malicious activities in IoT networks [9].

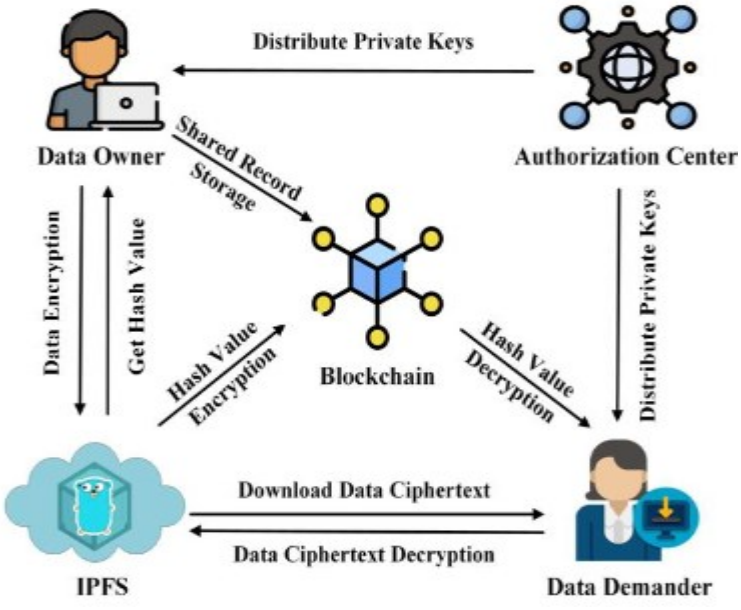

Figure1. Block chain-based traceable and secure data-sharing schema

2. RELATED WORK

There are myriad works are developed for handling the privacy issues in advanced communication models and transaction services. Crowd sensing is considered as an efficient tool for providing cost effectiveness [10]. The interconnected nature of multiple nodes systems forming a chain and every node stores a duplicate of the primary chain hackers is quickly access the information [11]. We focus on the building of security preserving data mining algorithms relevant to informatics and then analyse the candidate process. While discussing these process we will try to understand their intrinsic trade-offs many security cost and utility [12]. The recommended the model of security-preserving collaborative model learning using skyline computation referred to as PCML which relies upon papillae cryptosystem take threshold decryption and distributed skyline computation [13]. To fully utilize block chain's potential in IoT access control, some proposals have designed frameworks that aim to deliver decentralization by means of smart contracts proposed a framework that uses smart contracts to replace the centralized validation of access policies [14].

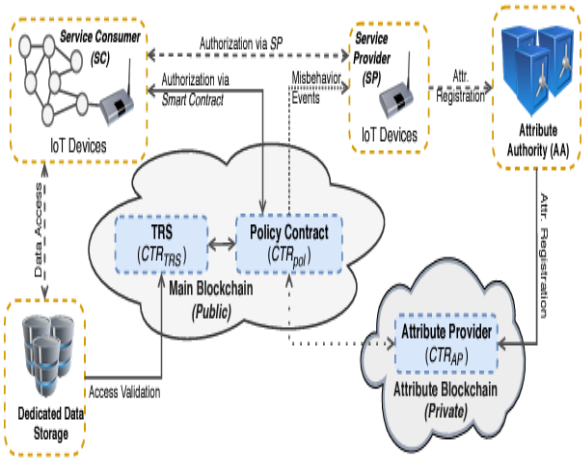

Fig. 2. Architecture of WCPS.

3. SYSTEM MODEL

Thet is challenging to develop a security architecture which can overcome this limitation using traditional methods such as access control, encryption, user authentication [15]. The ML prediction in HCPSs can provide customers with high-accurate prediction services in trained models and their owned data. We introduce the system and security models of VPMLP for edge enhanced HCPSs [16]. In all four scenarios we use a representative process control system called the Continuous Stirred Tank Reactor (CSTR) system is fluid temperature control system. The objective is to control the temperature of the liquid in the tank by modifying

the steam flow rate [17]. The implementation of the proposed block chain-based mitigation attacks (BBMDA) framework involves multiple components, including setting up the block chain network, developing smart contracts, integrating anomaly detection using the multitask transformer (MTT) model, and implementing mitigation actions[18].

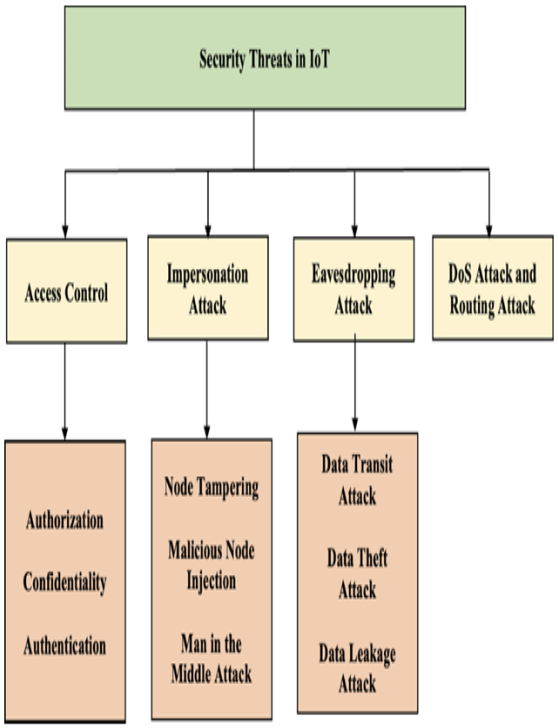

Fig. 3. Architecture of the CSTR System

4. PROPOSED SYSTEM

A novel block chain approach that integrates data compression and encryption enhance performance, security, and efficiency. By implementing advanced data compression techniques, the block chain can reduce the size of transactions and blocks, leading to faster transmission and reduced storage requirements across the networks[19].This problem is resolved by using attribute-based encrypted systems to provide a safeguard against such attacks [20]. Integrating the machine-learning-based automated role assignment is provide accurate modelling of user–role relationships making the system efficient and effective in terms of time and cost [21]. The Block chain technique in association with SHA-256 enables and accelerates security preserving patient centric cryptographic hash algorithms like SHA assures trustworthy transactions cryptographic hash algorithms [22].

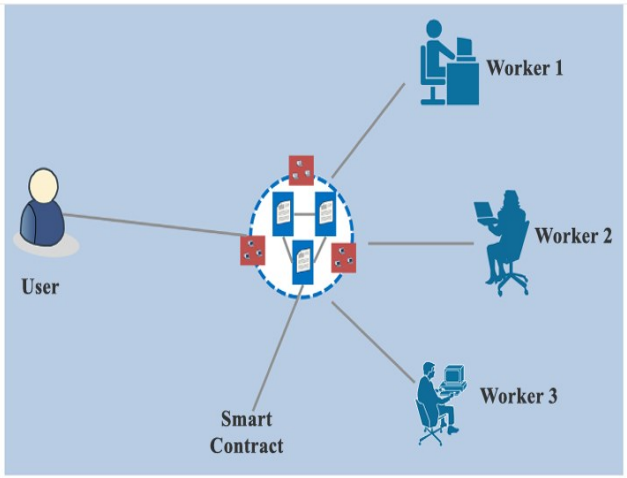

Figure 4: The elements of the proposed framework

1. Implementation of Block chain Technology in Network Applications

The section presents the complete working procedure of the proposed DSecCS Model. And, the associated block chain based Crowd sensing model which contains two major parts called participants and task managers [23]. The block chain was utilized to find a solution to the problem of information security. Present advancements in IoT and fifth-generation mobile networks (5G) is substantially increase the amount of big data collected by 5G-enabled industrial automation[22]. The building an efficient deep learning paradigm for IoT has several including a single point of failure the potential for IoT devices to leak personal information [24].

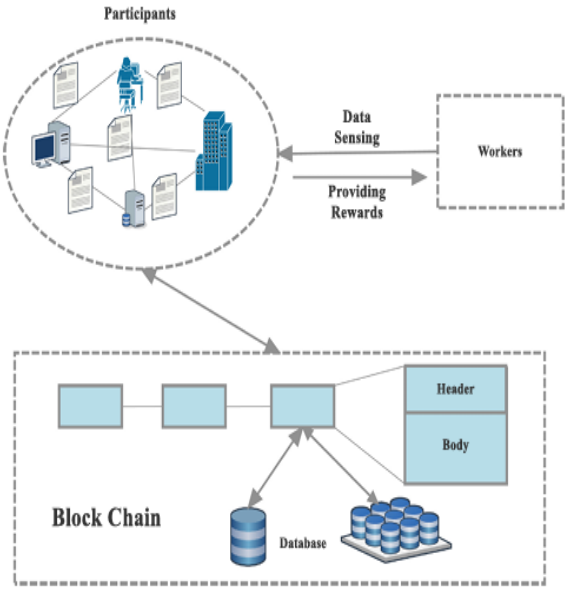

Fig. 4 Incorporation of Block chain in Crowd sensing Model.

5. SERVICE PROVIDER

The training process aims to learn the patterns and dependencies in encrypted network traffic data, enabling accurate classification of normal traffic de-authentication attacks, and other anomalies [25]. A possible remedy is introduce another honest-but-curious party, called crypto service provider (CSP), is manage secret keys decrypt intermediate results, and assist SP to finish the modelling task to framework in SP and CSP learn models over encrypted/masked data and the generated models are only decidable by the individual users [26]. Block chain provides a decentralized platform for IoT applications which avoids the chances of a single point of failure. In general, Blockchain technology is defiant to data modification.

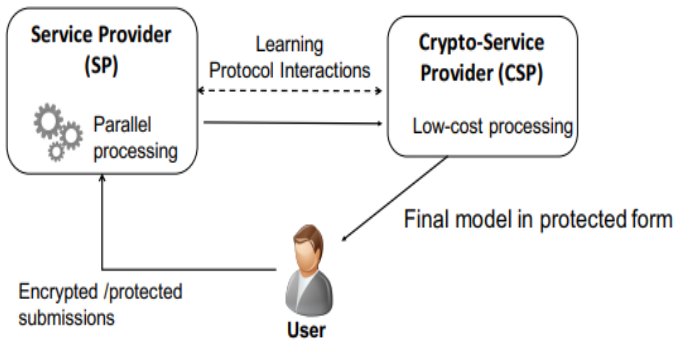

Figure. 5 Cryptographic Service Provider (CSP) and SP with preserved security

1. **Structure of SHA-256 Algorithm SHA-256**

Algorithms:

Input: Block of Message

Output: Fixed Size bits

Step 1: Pre-Processing

i). Indexing and Padding with 0's until data is a multiple of 512, less 64 bits.

Step 2: Initialize Hash Values

ii). Now create hash values

Step 3: Initialize Round Constants

iii). Similar to step 2, we are creating constants. This time, there are 64 of them.

Step 4: Chunk Loop

IV). The following steps for each 512-bit "chunk" of data from our input.

Step 5: Create Message Schedule

V). Copy the input data entry is a 32-bit word

Step 6: Compression

vi). Initialize variables hash values respectively

Step 7: Modify Final Values

vii). after the compression loopand change variables to them.

Step 8: Concatenate Final Hash

Viii). Combine them all together to get fixed length bit size

SHA-256 hashing calculation elaborated the official NIST standard there are main two steps in the SHA-256 calculation. Pre-measure of the first messages by message cushioning to extending the directive for the round calculation [27]

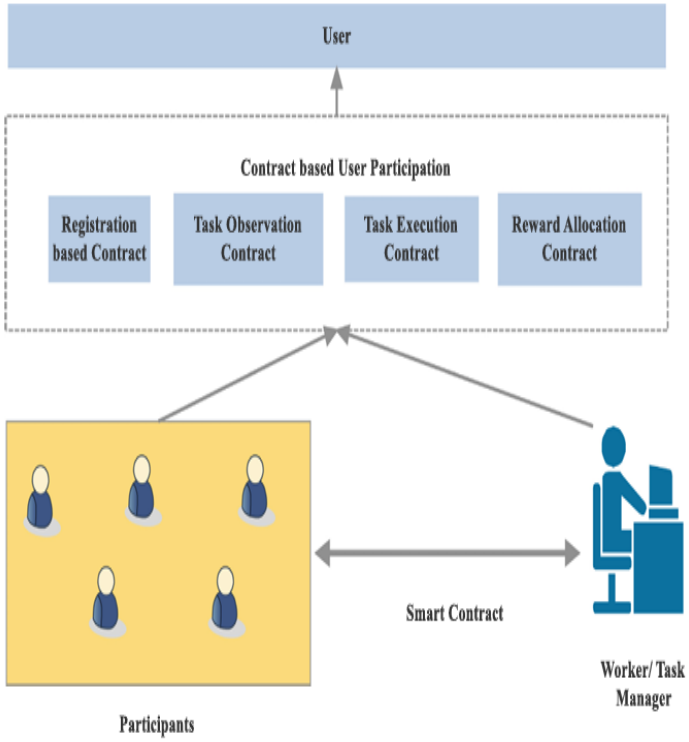

Fig.6. SC-SetforUserParticipation

6. EXPERIMENTAL RESULTS

The performance of the proposed block chain-based mitigation of dis authentication attacks (BBMDA) framework was evaluated and compared with that of other widely used techniques, namely, support vector machine (SVM), k-nearest neighbours (KNN), and convolutional neural network (CNN), using simulated datasets for different IoT nodes. The simulations are executed at the different security levels with different sizes of the query vectors and the result some of the schemes is designed for neural network services for the sake of fairness these schemes are adjusted to the same scale of LR in the same reflect the similar tendencies on the execution time of these schemes under different security levels.

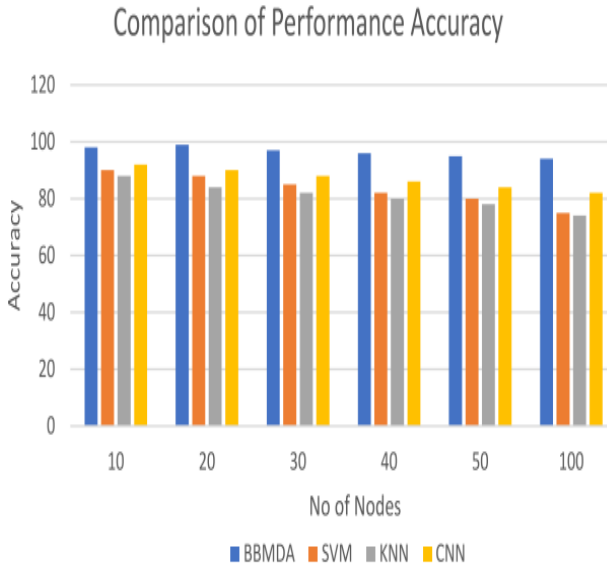

Fig. 7: Execution Time of each sub-task in Verifiability with increasing Fog nodes

7. CONCLUSION AND FUTURE WORK

Block Chain based Advanced Data Security Reward Model (DSecCS) is developed for MCS. Additionally, the model effectively combines the block chain model for developing the mobile crowd sensing model to can resist various attacks. The security model is risk the desired algorithms quality and audience of the models must be conducted. Depending on the desired analytics and privacy level an additional party such as a cryptographic service provider might need to introduce to a framework. The security of SPRITE is analysed under an honest-but-curious setting where the cloud is untrustworthy. We implemented a proof-of-concept in a public Ranke by test network interconnected with a lab-scale tested. The technology matures it is likely to become an integral part of the future of data management, transforming to store, manage, and secure information,

8. REFERENCES

[1] R. Iqbal, T. Maniak, F. Doctor, and C. Karyotis, “Fault detection and isolation in industrial processes using deep learning approaches,” IEEE

Transactions on Industrial Informatics, vol. 15, no. 5, pp. 3077–3084, 2019.

[2] M. A. P. Chamikara& Peter Bertok & Ibrahim Khalil &Dongxi Liu & Seyit Camtepe& Mohammed Atiquzzaman. (2020). A Trustworthy Framework for Privacy-Preserving Machine Learning in Industrial IoT Systems 10.1109/TII.2020.2974555. IEEE Transactions on Industrial Informatics. pp.1–1.

[3] Fatima Hussain & Rasheed Hussain & Syed Hassan & Ekram Hussain (2020). Machine Learning in the Security of the Internet of Things: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials. pp.10.1109/COMST.2020.2986444. IEEE Communications Surveys & Tutorials. pp.10.1109/COMST.2020.2986444.

[4] Parikshit N. Mahalle and Poonam N. Railkar, "Identity Management for the Internet of Things, " Identity Management for the Internet of Things, River Publishers, 2015, pp. i-xx.

[5] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in an Age of Machine Learning and Software-Defined Networking, " IEEE Internet of Things Journal, vol.5, no.6, December 2018, pp.4829– 4842, doi: 10.1109/JIOT.2018.2846040

[6] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model Inversion Attacks That Exploit Confidence Information and Basic Countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, page 1322–1333, 2015.

[7] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. Exploiting Unintended Feature Leakage in Collaborative Learning. In 2019 IEEE Symposium on Security and Privacy, pages 691–706, 2019.

[8] Zhibo Wang, Mengkai Song, Zhifei Zhang, Yang Song, Qian Wang, and Hairong Qi. Beyond Inferring Class Representatives: User-Level Privacy Leakage From Federated Learning. In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, pages 2512–2520, 2019.

[9] Huadi Zheng, Qingqing Ye, Haibo Hu, Chengfang Fang, and Jie Shi. BDPL: A Boundary Differentially Private Layer Against Machine Learning Model Extraction Attacks. In Computer

Security – ESORICS 2019, pages 66–83, 2019.

[10] Yaochen Hu, Di Niu, Jianming Yang, and Shengping Zhou. FDML: A Collaborative Machine Learning Framework for Distributed Features. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, page 2232–2240, 2019.

[11] Kang Wei, Jun Li, Ming Ding, Chuan Ma, Howard H. Yang, Farhad Farokhi, Shi Jin, Tony Q. S. Quek, and H. Vincent Poor. Federated Learning With Differential Privacy: Algorithms and Performance Analysis. IEEE Transactions on Information Forensics and Security, 15:3454– 3469, 2020.

[12] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Differentially Private Asynchronous Federated Learning for Mobile Edge Computing in Urban Informatics. IEEE Transactions on Industrial Informatics, 16(3):2134–2143, 2020.

[13] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. Practical Secure Aggregation for Privacy-Preserving Machine Learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, page 1175–1191, 2017.

[14] Stacey Truex, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig, Rui Zhang, and Yi Zhou. A Hybrid Approach to PrivacyPreserving Federated Learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, page 1–11, 2019.

[15] Yong Yu et al., “Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things,” EEE Wireless Communications, vol. 25, no. 16, pp. 12-18, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] Minhaj Ahmad Khan, and Khaled Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges,” Future Generation Computer Systems, vol. 82, pp. 395-411, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sophocles Theodorou, and Nicolas Sklavos, Blockchain-Based Security and Privacy in Smart Cities, Smart Cities Cybersecurity and Privacy, Elsevier, Chapter 3, pp. 21-37, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Lakshmana Kumar Ramasamy et al., "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," IEEE Access, vol. 9, pp. 128765-128785, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Bandar Alamri, Katie Crowley, and Ita Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," IEEE Access, vol. 10, pp. 59612-59629, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdullah Al Mamun, Sami Azam, and Clementine Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," IEEE Access, vol. 10, pp. 5768-5789, 2022

[21] G. Shah and A. Tiwari, "Anomaly detection in iiot: A case study using machine learning," in Proceedings of the ACM India Joint International Conference on Data Science and Management of Data, 2018, pp. 295–300.

[22] B. Yang, X. Cao, X. Li, Q. Zhang, and L. Qian, "Mobile-edgecomputing-based hierarchical machine learning tasks distribution for iiot," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2169–2180, 2020.

[23] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial iot systems," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6092–6102, 2020.

[24] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3559–3570, 2019.

[25] B. Chen, J. Wan, Y. Lan, M. Imran, D. Li, and N. Guizani, "Improving cognitive ability of edge intelligent iiot through machine learning," IEEE Network, vol. 33, no. 5, pp. 61–67, 2019.

[26] C. J. Watkins and P. Dayan, "Q-learning," Machine learning, vol. 8, no. 3-4, pp. 279–292, 1992.

[27] M. O. Duff, "Q-learning for bandit problems," in Machine Learning Proceedings 1995. Elsevier, 1995, pp. 209–217.