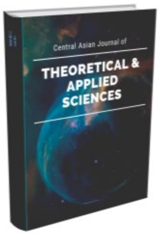

CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCE

https://cajotas.centralasianstudies.org/index.php/CAJOTAS
Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5317

Article

Secure and Efficient Data Sharing Using Blockchain and Deep Learning for Industrial Healthcare Systems

Zaid Mohammed Mortada[1], Ola Baqer Abdulhadi[2], Abrar Ali Hasan Al-Ameri[2]

1. Department of Postgraduate Studies, University of Kufa, Najaf, Iraq
2. Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

* Correspondence: zaidm.alhusaini@uokufa.edu.iq

Abstract: Secure, reliable, scalable communication of private data is a necessity for IoMT devices used in industrial healthcare. Classical centralized architectures are not able to cope with such demands due to their inadequacy on privacy, data integrity, scalability, and cyber security. In this context, a decentralized industrial healthcare data sharing scheme built on permissioned blockchains is offered to alleviate the above challenges. Using smart contracts in permissioned blockchains, the framework guarantees controlled access, tamper resistance of data storage and trusted information kindles transference. Moreover, Support Vector Machines (SVM) was adopted to use with the LSTM network for data analytics, behavior modeling and enhanced attack detection. In order to guarantees patient privacy, homomorphic encryption is embedded in order to process encrypted healthcare data in the cloud. Experiments demonstrate that the proposed approach can be more accurate, robust, and scalable than other deep learning and machine learning methods, which could provide an intelligent method to learn useful representation of industrial healthcare data for future work.

Keywords: Blockchain, Deep Learning, Data Sharing, Secure, Industrial Healthcare Systems, Internet of Medical Things (IoMT).

Received: 10 Nov. 2025
Revised: 10 Dec 2025
Accepted: 25 Dec 2025
Published: January 25, 2026

1. Introduction

An Internet of Things (IoT) based smart grid, smart network, smart city and healthcare system are among the applications and services that can be supported by the IoT [1]. Under the support provided by IoT technology, through realizing location barrier-free and automating manufacturing process, remote monitoring and real-time data communication facilitated superior performance to traditional industries [2]. Several types of physiological data can be recorded with IIoT in the current health system, such as blood pressure levels, electrocardiograms and temperatures [3]. Health care providers often aggregate and process industrial healthcare data, then send it to the cloud for long-term storage, or use it to diagnose and analyze patients in real time [4]. Currently, healthcare ecosystems are characterized by insecure devices and sensors transmitting, exchanging, and monitoring data continuously [5]. As a result of round-the-clock connectivity, healthcare systems are vulnerable to a wide range of security threats, such as data manipulation, denial-of-service attacks, eavesdropping, and impersonation [6]. Health care professionals may be exposed to the risk of incorrect diagnoses caused by data manipulation [7].

In addition, the current industrial healthcare system faces major privacy and data integrity challenges. Two types of data privacy attacks exist: active data privacy attacks (ADPAs) and passive data privacy attacks (PDPAs) [8]. A DPA attack alters, modifies or infers private information from two communicating entities (as when data poisoning occurs) [9]. During this type of attack, real-time modifications are made to patient health data. It is also possible to negatively impact AI-based data analytics and intrusion detection systems (IDSs) [10]. Blockchain technology is immutable and decentralized, and would be an interesting technology for a cryptocurrency such as Bitcoin. The trust on data is maintained by the use of a ledger, dispersed and decentralized. A blockchain can securely store data, retain audit trails with access controls, and manage access finely using smart contracts, cryptography and consensus mechanisms. Privacy, security and interoperability problems can be solved via blockchain. EHRs, health data-including images-and sensitive information should be shared with the patient's permission. Being decentralized in underlying nature, blockchain requires no intermediaries; generating higher efficiency at lower cost and forcing data to be more accessible. Because of medical challenges, for technological perspective three significant issues are present in healthcare: (1) data interoperability; (2) scalability and (3) security [11]. Excuses such as data sharing, information security and meaningful collaboration all apply to standard healthcare systems. With the advent of new technologies such as DL and BC, healthcare revolution is in the offing [12]. BC technology is commonly used for development of cryptocurrencies due to its attributes including immutability and decentralization

2. Related Work

Health care is one of the sectors where blockchain technology shows great promise. In addition to being distributed and immutable, it addresses data integrity, interoperability, and security concerns. Due to the large amount of data generated by healthcare applications, blockchain technology presents a challenge. Author proposes a hybrid deep learning system which enables to achieve scalability and security of healthcare data management with blockchain technique. Blockchain can remedy healthcare using deep learning. The new study demonstrates that deep learning models can preprocess the blockchain-based healthcare without difficulty and securely [13]. Applications of blockchain to distributed systems: A survey [14]. It also provides deeper understanding about block chain's secure, privacy inside the framework reaching towards implementation. Deep learning was also suggested in the study as a way to improve performance and scalability. In addition, the study identifies blockchain-based healthcare platforms that employ hybrid deep learning algorithms for analyzing and securing data. In 2020, blockchain-based privacy and security enhancements will be introduced for healthcare data. [15]. Detecting anomalies and encrypting data can be improved utilizing deep learning models. Blockchain technology, a technology that is immutable, and deep learning, which is a technology that anticipates, are used in healthcare data security. In the author [16] proposed a scheme for offloading data. A Markov Decision Process (MDP) is used to formulate the most challenging problem, which is then solved using DRL policy search. As well as BC security audits, offloading decisions, computing resource distributions, and radio communication bandwidth, other factors are also taken into account. A novel DL-based secure BC (ODLSB) was presented by authors [17] to aid intelligent IoT and healthcare diagnosis. Medical images can be shared confidentially using the orthogonal OPSO technique. A disease detection algorithm was created using the optimum DNN (ODNN). In PBDL, permission BC and smart contracts are combined with DL methods, according to the author [18]. By utilizing PBDL's smart contract-based consensus model, transmission entities can be validated, registered, and verified using zero-knowledge proof. DL and BC-based architectures are used to construct a secured platform in [19]. An optimization algorithm called Bonobo is used to develop a BC leveraging technique that is optimal. Moreover, Feistel architecture is incorporated in the model to increase privacy protection. In addition, the intrusion is identified and prevented using a DRL technique.

Using BC entities (BC-i Health) for cost reduction and security enhancement, the authors propose an intelligent healthcare system [20]. Deep Q-learning was used to resolve the optimizer method as a MDP. A new BC-based system for medical diagnosis and transmission of data with DL-assisted medical data transmission is presented. By using the moth flame optimizer with ECC (MFOECC), the optimal key is generated for ECC. The use of SHA-256 hashing techniques in blockchain can be inefficient against malware and benign attacks when used in heterogeneous ICPS workflows. Although SHA-256-based deep learning models for blockchain technology are not malware-proof, they are optimal for workflows. A blockchain-enabled ICPS powered by LSTM and reinforcement learning is presented in this study for healthcare services in heterogeneous fog network networks. The study concludes that blockchain technology introduces a new pattern of hashing that prevents malware and cyber-attacks most effectively. In this study, the Markovian decision process was used to divide the scheduling problem into multiple states [21].

3. Proposed Methodology

During the experiments, steps have been taken to obtain the output of the system in accordance with the proposed methodology [22]. As part of step 1, IoT data is collected and sent to the cluster head using sensors. Step 2 involves transferring data through the blockchain. Following data encryption, homomorphic encryption is used, and then cloud computing is used. Data that is encrypted can be used for statistics and deep learning when homomorphic encryption is combined [23]. We extract key features from heart rates, ages, genders, weights, and heights. Feature-based and interaction-based classification is proposed using SVM. A validation model is then used to verify and validate the output [24].

3.1 Proposed Algorithms

In IoMT, sensors and medical devices are used to collect information about patients, medical equipment, and the environment. A variety of medical devices can be found in this category, including wearables, implants, monitoring devices, and more. Physiological, behavioral, and environmental data are captured, transmitted, analyzed, and used for further decision-making within IoMT systems by sensing. As well as vital signs and medication adherence, sensors can also monitor activity and the environment. It isn't widely recognized that distributed QEMR algorithms can be incorporated into IoMT.

3.2 Mathematical Model

Here is how the mathematical model looks:

$$objective\ Function: \underset{x_1, x_2}{max 3_{x1} + 5_{x2}}$$

$$\begin{aligned} Subject\ to:\ & 2_{x1} + 4_{x2} \leq 10 \\ & x_1 + 3_{x2} \leq 7 \\ & x_1, x_2 \geq 0 \end{aligned}$$

An optimization problem can be formulated for the mathematical model:

$$Objective:\ \max \sum_{i \in S} \sum_{j \in J} D_{ij}.B_{ij} \tag{1}$$

$$Subject\ to: \sum_{j \in J} U_{ij} \leq M, \forall i \in S \tag{2}$$

$$U_{ij} = D_{ij}.B_{ij}, \forall i \in S, j \in J \tag{3}$$

$$B_{ij} \in \{0,1\}, \forall i \in S, j \in J \tag{4}$$

3.2.1 Proposed Framework

Blockchain-enabled healthcare systems can benefit from hybrid deep learning techniques. By integrating these technologies, healthcare data can be managed and analyzed efficiently while still maintaining its integrity and privacy [25].

- **Blockchain Infrastructure:** The framework utilizes blockchain infrastructure to record medical data on a decentralized immutable ledger. Nodes keep and validate the double spending blocks. Blockchains can be employed to store medical history, diagnoses and treatments traceable and tamper proof.
- **Permissions Blockchain-Based Framework:** Blockchain technology allows for permission-based control and security of health data. Smart contracts are used to enable access to and sharing of information between healthcare participants. A granular access control system allows patients to manage access to their medical records in a confidential manner [26].
- **Hybrid Deep Learning Models:** To analyze healthcare data, deep learning and blockchain technology are combined. Convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs) have been developed to diagnose diseases, predict outcomes, and detect abnormalities [27].
- **Secure Model Training and Sharing:** Following the framework, privacy preserving deep learning models are trained and shared. This mode of raw data" not-shared and shared model training based on decentralization is referred to as federation. Various privacy methods are available to secure private information in model learning phase.
- **Scalable Data Processing:** Using this framework, scalability challenges in healthcare systems can be addressed by processing and analyzing distributed data. By using multiple deep learning models on a distributed blockchain network, large volumes of healthcare data can be processed and analyzed efficiently. Despite expanding volumes of data and computational demands, the system remains scalable due to its distributed approach [28].
- **Security Measures:** In order to protect against a variety of threats and attacks, a number of security measures have been included in the proposed framework. Data transmission and storage are protected by encryption, participants' identities are verified by authentication, and security risks are identified and mitigated by anomaly detection algorithms. Additionally, proof-of-stake and proof-of-work cryptographic mechanisms can be integrated into the framework to enhance consensus.

By combining deep learning and blockchain technology, healthcare becomes more scalable and secure. Furthermore, it enables secure, auditable, and powerful analytics powered by deep learning. Besides enabling secure, auditable data storage and sharing, it also provides deep learning-based analytical capabilities.

Various IoT devices can be handled by automated systems with a high level of reliability. Managing and distributing IoT devices that are large requires automation and control expertise. As part of the hybrid deep learning approach, SVM and LSTM are both used. A model trained with IoT data is also stored in LSTM and records the IoT massive data set. LSTMs are designed to predict user behavior as well as attack chances inside the network.

Users can also classify data using support vector machines (SVMs). As part of the proposed model, IoT sensor data is hashed on blockchain nodes and then cloud-hosted after homomorphic encryption. Smart contracts can be divided into two types: Local smart contracts [29] and Global smart contracts. Additionally, a local smart contract governs the organization's local domain. Using smart contracts governs global interactions with the system, making the proposed approach cross-domain and scalable. There are irregular gaps between consecutive time steps in LSTM, which is handled by the forget gate. LSTM networks are aggregated with time-decaying pooling strategies to predict the future. By using EHRs, LSTMs, and neural networks, we propose an end-to-end DaaS framework to memorize and predict long-term illness.

Admissions to any i^{th}patient are sequence $S = (SD_1, SD_2, \ldots, SD_n)$ for EHR records $D = (D_1, D_2, \ldots, D_n)$. In admission SD_i, the diagnosis codes $(C_1, C_2, \ldots, C_n)$, are represented by a feature vector $\in_i \in R^m$ where m indicates the length of the vector. Accordingly, Δt indicates the period between previous admissions and current admissions. Every i^{th}patient, designated by Δ_{pi}, has a similar time-sequence recorded. Each patient's LSTM feature vector set looks like this:

$$F_{LSTM}^{i} = \{x_{c_i}, x_{I_i}, \Delta P_i, m_i\} \tag{5}$$

The LSTM calculates corresponding sequences of distributed illness states $\varrho_1, \varrho_2, \ldots, \varrho_n$ where $\varrho_i \epsilon R^k$, in this case, K is the vector dimension length. Adding these states to the middle layer is achieved by the multi-state weighted pooling function $WPool$ $(\varrho_1, \varrho_2, \ldots, \varrho_n)$ for n scales. Based on these pooled states, the top layer computes outcome probabilities as follows:

$$P(y|\varrho_{1,2,\ldots,n}) = P(LSTM(WPool)) \tag{6}$$

Based on outputs and record structures, $P(y|\varrho_{1,2,\ldots,n})$ is determined. It is possible to have a binary or multiclass record structure. A patient's diagnosis code D must fall between the ranges of 1 and $|D|$, and the intervention code F must fall between the ranges of 1 and $|F|$. As indicated by the embedding matrix size $n \times k$, it is the row element located at the $B \in R^{M \times |F|}$ column of the i^{th} column for the admission of a diagnosis, which is described as: $d_1, d_2, \ldots, d_n \in \{1to|D|\}$. Intervention vectors have been designated as $B_s^{I_1}, B_s^{I_2}, \ldots; B_s^{I_k}$ in the matrix, while embedded vectors have been designated as $A^{d_1}, A^{d_2}, \ldots, A^{d_n}$. Following is the maximum pooling definition: [30].

$$x_t^i = max\{A^{d_1}, A^{d_2}, \ldots, A^{d_n}\} \tag{7}$$

$$p_t^i = max\{B_s^{I_1}, B_s^{I_2}, \ldots; B_s^{I_k}\} \tag{8}$$

Normalized sum pooling can be described as follows [30].

$$\eta_t^i = \frac{A^{d_1} + A^{d_2} + \cdots + A^{d_n}}{\sqrt{A^{d_1} + A^{d_2} + \cdots + A^{d_n}}}$$

$$\omega_t^i = \frac{B_s^{I_1} + B_s^{I_2} + \ldots + B_s^{I_k}}{\sqrt{B_s^{I_1} + B_s^{I_2} + \ldots + B_s^{I_k}}} \tag{9}$$

LSTM input gate i controls the memory update of the Norm Pool. A candidate for admission into the LSTM network [30] is a person who meets the following criteria:

$$A_t = \frac{1,}{m_t}\sigma(w_i x_i + U_t h_{t-1} + b_i)$$

$$M_t = \begin{Bmatrix} 1, & admission\, unit A_t > 0 \\ 0, & admission\, unit A_t < 0 \end{Bmatrix} \tag{10}$$

A gate output is shown as o_t, and a weight matrix intervention is shown as p_o. Here are the equations that moderate output gate and illness forgetting [30].

$$o_t = \sigma(w_o x_t + u_o h_{t-1} + p_o p_t + b_o)$$

$$f_t = \sigma(w_f x_t + u_f h_{t-1} + p_f p_{t-1} + b_f) \tag{11}$$

$$f_t \leftarrow d(\Delta_{t-1:t} f_t), Where \Delta_{t-1:t} = |\log(e + \Delta_{t-1:t})^{-1}|$$

$$\aleph_i = \sigma\left(w_f x_t + u_f h_{t-1} + Q_f q_{\Delta_{t-1:t}} + p_f p_{t-1} + b_f\right) \tag{12}$$

In an LSTM network, $\aleph_i$ represents the parametric projection. Using a softmax function $tmax(z) = \frac{e^z}{\sum_{z^t} e^{z^t}}$, hidden illness state h_t is now replaced with diagnosis code d_{t+1} for each discrete time step t. The n inputs, HPool is defined as $h_{1,2,\ldots,n}$and has the following equation:

$$h_{1,2,\ldots,n} = \frac{1}{s+1}\sum_{0=1}^{n} h_t \tag{13}$$

A single hidden layer is now used to feed the LSTM network's output to the neural network. LSTM is used to predict future diseases by stacking illness predictions. The one layer stack auto encoder is used to denoise these illness predictions to predict future diseases.

$$e_h = \sigma(h_t + n_h)$$
$$x_y = h_t a_n + b_y$$
$$P\left(y \backslash h_{1,2,\ldots,n}\right) = f_{prob}\left(x_y\right) \tag{14}$$

3.3 Proof of Concept (POC)

A permission-based blockchain system for healthcare can be used to validate and evaluate a hybrid deep learning model. Data-driven decision-making was demonstrated by using PoCs in healthcare scalability, security, and healthcare scalability [31]. Data storage and access control based on blockchains, along with real-time data analysis based on deep learning, were used in the POC. Regulatory authorities, healthcare providers, and patients were represented in the network. Access to and modification of health information could be controlled by enforcing permission-based access control mechanisms through smart contracts. Data sharing can be facilitated efficiently by using zero-knowledge proofs while maintaining patient confidentiality [32]. Modeling mathematically and designing security protocols follow the following phases. Using an IoT system requires the user to go through a number of phases before reading or sending data.

Phase 1: System Setup: During setup, various parameters are initialized, including those related to creating signatures and authenticating users. Below is an explanation of each phase:

The setup (a) is as follows: Input security parameters (a)

$$let\ (G_1)\ and\ (G_2)\ be\ two\ multiplicative \tag{15}$$

$$Assume\ (g_1), (g_2)\ are\ two\ generation\ of\ (G_1). \tag{16}$$

3.4 Encryption

Message M is the plaintext message, while cipher text C is the encrypted message. During encryption, E, a homomorphic encryption algorithm, comes together with K, an encryption key. The mathematical representation of cryptography is as follows:

$$C = E(M, K) \tag{17}$$

Using C as the cipher text, homomorphic encryption algorithm E generates a ciphertext M based on plaintext M and an encryption key K.

3.5 Decryption

In decryption, plaintext messages are recovered from cipher text by reversing the encryption. The decrypted plaintext $M'$and the cipher text C are shown below. It is important to note that a decryption algorithm (D) and a decryption key K' are part of the decryption process [38]. The mathematical representation of decryption is as follows:

$$M' = D(C, K') \tag{18}$$

After taking the cipher text C and decryption key K' into account, the plaintext message M' is produced using a decryption algorithm D. An equation defines block creation time and height as variables X1 and X2 [33].

4. Result and Discussion

When the training process is further enlarged, so is model accuracy (Figure 1). The network is noised in the first five epochs due to very low training and validation accuracy, meaning that it has not yet learnt relevant patterns. There is also a large performance improvement at 10 epochs, with training accuracy increased to 0.65 and validation accuracy at.85 that shows effective learning and good generalization. The model reaches its best and most robust performance at 15 epochs, with matching training and validation accuracies (0.90-90) indicating an adequate absence of overfitting in this case. Further, small changes are seen at epochs 20 and 25, but validation accuracy tends to decrease slightly, so overfitting is taking place. Overall, these results identify 15 epochs as the. Overall, these results highlight 15 epochs as the most suitable training duration, offering the best balance between accuracy and generalization.

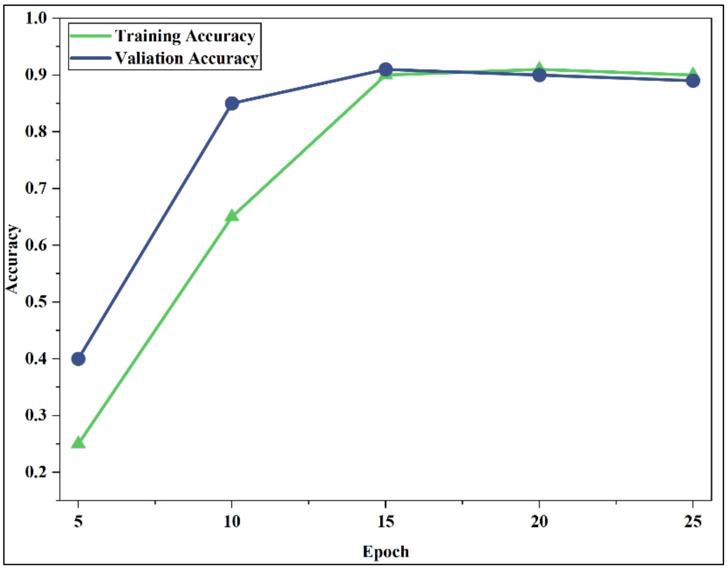

Figure 1: Training and Validation Accuracy across Epochs.

Training and validation losses fluctuate over training epochs as depicted in Figure 2. Both the training (9.23) and validation loss (9.02) are high at 5 epochs, indicating that convergence has not yet been reached for this model. There is a significant decrease by the 10-th epoch, where the training and validation loss become 8.93 and 8.94 respectively, indicative of very quick learning and good model fitting. The loss values tend to converge from 15 epochs and beyond with only minor upgrades, setting at 8.91 (for training) and 8.92 (for validation) at the 25 epochs. The training and test losses are quite similar for later epochs, I am sure the converging is stable and it generalizes well (without overfitting).

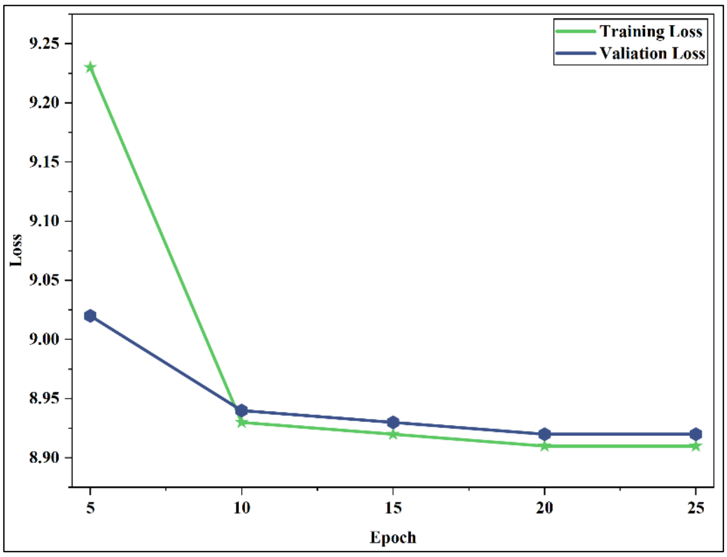

Figure 2: Training and Validation Loss across Epochs.

To compare the class-wise detection performance of various methods under different attack types, Figure 3 is presented. RF and DT reach very high precision on multiple classes, but make crucial mistakes, in particular on [MITM] and [Injection], which suggests that the detection capability is too weak. NB has a high variance in performance with low accuracy against more complicated attacks such as DDoS and XSS. BiLSTM consistently yields high and well-balanced accuracies over all classes suggesting to learn attack patterns well. Models Further the Proposed Model provides superior performance being almost perfect for all categories of attack hence it demonstrates robustness and a higher generalization.

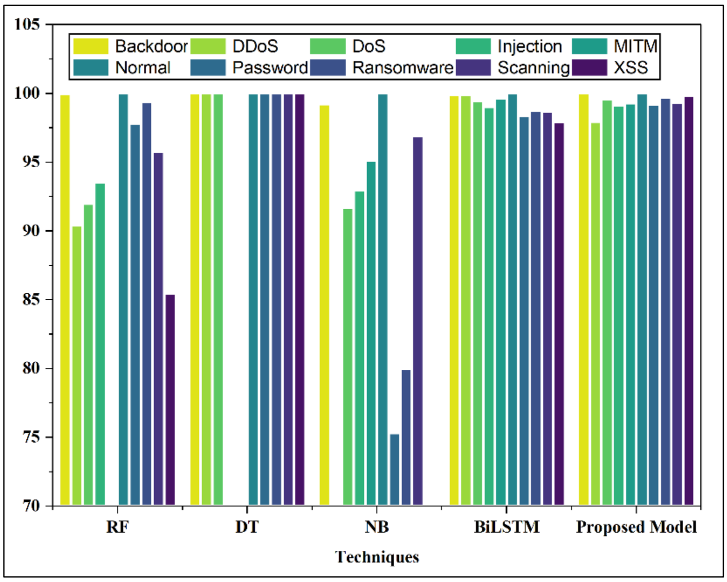

Figure 3: Class-Wise Detection Accuracy Comparison Across Different Techniques.

Comparison of the global accuracy of various classification methods is shown in Figure 4. CART's accuracy is only 77%, showing that the method is ineffective for complex patterns. CNN, XGBoost and RF shows high accuracies (>98%), illustrating the reliable learning and classification ability. It can be seen that the Proposed Model achieves higher accuracy in comparison with all baseline models, even reaches 99.89%; thus the ability to make prediction and its robustness are well tested.

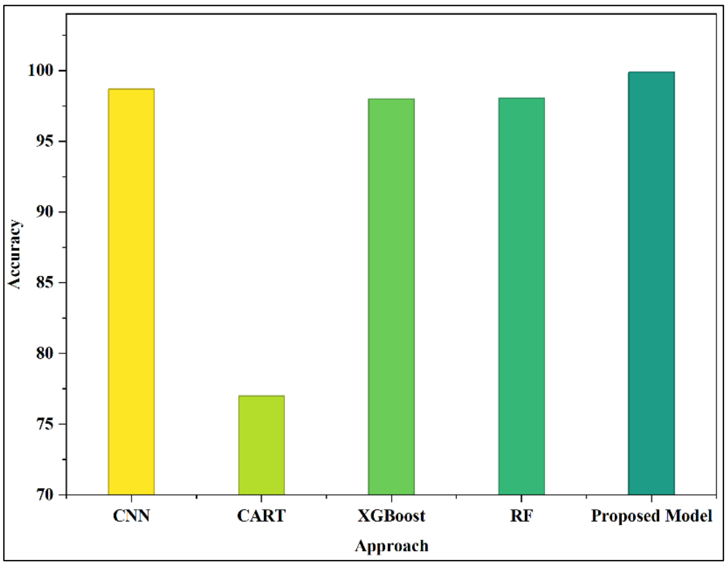

Figure 4: Accuracy Comparison of Different Classification Approaches.

5. Conclusion

We employed the permissioned blockchains and deep learning to construct an efficient, scalable, secure data sharing system in industrial health care. Smart contracts combined with blockchain technology guarantee the integrity of data, transparency, as well as fine-grained access control and thus streamline dependence on centralised solutions. The combination of these deep learning models, particularly LSTM and SVM, contributes to significantly improving intelligent data analytics, security monitoring (intrusion detection) as well as user behavior modeling in the IoMT. The operations of homomorphic encryption privacy also secure confidentiality on encoded healthcare data. The experimental results show that the proposed method achieves superior performance than state-of-the-art machine learning and deep learning based techniques. Enabling secure healthcare data management, the framework is also reliable, intelligent and scalable for industrial healthcare systems. Future work will focus on the reduction of computational overhead and extension of our framework to facilitate cross-domain compatibility as well as real-time federated learning.

REFERENCES

1. Dudeja, R. K., Bali, R. S. & Aujla, G. S. Secure and pervasive communication framework using Named Data Networking for connected healthcare. *Computers and Electrical Engineering* **100**, 107806 (2022).
2. Bhola, B. *et al.* Quality-enabled decentralized dynamic IoT platform with scalable resources integration. *IET Communications* **19**, e12514 (2025).
3. Vinayakumar, R. *et al.* A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities. *IEEE Trans. on Ind. Applicat.* **56**, 4436–4456 (2020).
4. Al-Turjman, F., Nawaz, M. H. & Ulusar, U. D. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Computer Communications* **150**, 644–660 (2020).
5. Aujla, G. S. & Jindal, A. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE J. Select. Areas Commun.* **39**, 491–499 (2021).
6. Farouk, A., Alahmadi, A., Ghose, S. & Mashatan, A. Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications* **154**, 223–235 (2020).

7. Rani, P. *et al.* Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System: *International Journal of E-Health and Medical Communications* **13**, 1–15 (2022).
8. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R. & Srivastava, G. P2TIF: A Blockchain and Deep Learning Framework for Privacy-Preserved Threat Intelligence in Industrial IoT. *IEEE Trans. Ind. Inf.* **18**, 6358–6367 (2022).
9. Alkadi, O., Moustafa, N., Turnbull, B. & Choo, K.-K. R. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal* **8**, 9463–9472 (2020).
10. He, D. *et al.* Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems* **21**, 49–60 (2015).
11. Mahajan, H. B. Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap. *Wireless Pers Commun* **126**, 2425–2446 (2022).
12. Sammeta, N. & Parthiban, L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. *Complex Intell. Syst.* **8**, 625–640 (2022).
13. Ali, A. *et al.* Performance analysis of AF, DF and DtF relaying techniques for enhanced cooperative communication. in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)* 594–599 (IEEE, Dublin, Ireland, 2016). doi:10.1109/INTECH.2016.7845056.
14. Hasnain, M. *et al.* Benchmark Dataset Selection of Web Services Technologies: A Factor Analysis. *IEEE Access* **8**, 53649–53665 (2020).
15. Kim, H., Kim, S.-H., Hwang, J. Y. & Seo, C. Efficient Privacy-Preserving Machine Learning for Blockchain Network. *IEEE Access* **7**, 136481–136495 (2019).
16. He, Q. *et al.* A Blockchain-Based Scheme for Secure Data Offloading in Healthcare With Deep Reinforcement Learning. *IEEE/ACM Trans. Networking* **32**, 65–80 (2024).
17. Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C. & Krishnaraj, N. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. *J Supercomput* **77**, 9576–9596 (2021).
18. Kumar, R. *et al.* Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Trans. Ind. Inf.* **18**, 8065–8073 (2022).
19. Malik, V. *et al.* Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks. *IEEE Access* **11**, 70110–70131 (2023).
20. Al-Marridi, A. Z., Mohamed, A., Erbad, A. & Guizani, M. Smart and Secure Blockchain-based Healthcare System Using Deep Q-Learning. in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)* 464–469 (IEEE, New Orleans, LA, USA, 2021). doi:10.1109/WF-IoT51360.2021.9595416.
21. Ren, L., Ning, X. & Wang, Z. A competitive Markov decision process model and a recursive reinforcement-learning algorithm for fairness scheduling of agile satellites. *Computers & Industrial Engineering* **169**, 108242 (2022).
22. Lazaroiu, C. & Roscia, M. Smart district through IoT and Blockchain. in *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)* 454–461 (IEEE, San Diego, CA, 2017). doi:10.1109/ICRERA.2017.8191102.
23. Lacity, M. C. Addressing key challenges to making enterprise blockchain applications a reality. *MIS Q. Executive* **17**, 3 (2018).
24. Sengupta, J., Ruj, S. & Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications* **149**, 102481 (2020).
25. Esposito, C., De Santis, A., Tortora, G., Chang, H. & Choo, K.-K. R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **5**, 31–37 (2018).
26. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics J* **25**, 1398–1411 (2019).
27. Kim, T. M. *et al.* DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System. *Applied Sciences* **11**, 1612 (2021).

28. Hang, L. & Kim, D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors* **19**, 2228 (2019).
29. Fan, K., Wang, S., Ren, Y., Li, H. & Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J Med Syst* **42**, 136 (2018).
30. Pham, T., Tran, T., Phung, D. & Venkatesh, S. Predicting healthcare trajectories from medical records: A deep learning approach. *Journal of Biomedical Informatics* **69**, 218–229 (2017).
31. Dwivedi, A. D., Srivastava, G., Dhar, S. & Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **19**, 326 (2019).
32. Singh, A. *et al.* Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication. *IEEE Trans. Consumer Electron.* **70**, 4898–4907 (2024).
33. Yi, A. C. Y., Ying, T. K., Yee, S. J., Chin, W. M. & Tin, T. T. InPath Forum: A Real-Time Learning Analytics and Performance Ranking Forum System. *IEEE Access* **10**, 128536–128542 (2022).