Journal of Soft Computing Paradigm (ISSN: 2582-2640)
www.irojournals.com/jscp/

Future Direction of AI in Block-chain for security systems – A Comprehensive Report

Haoxiang Wang

Director and Lead Executive Faculty Member, GoPerception Laboratory, Cornell University, Ithaca, USA

E-mail: wanghaoxiang1102@hotmail.com

Abstract

Currently, blockchain is a game-changing technology that's revolutionizing the way applications are built because it eliminates the requirement for trust between network peers. Global and immutable repositories created by blockchain technology provide non-repudiation and accountability of the stored data. Because of this, processing and maintaining enormous volumes of data with ever-decreasing latencies are becoming more difficult. Therefore, artificial intelligence and machine learning approaches have made substantial advancements, paving the way for next-generation network infrastructure. The decentralization and tamper-proof nature of blockchain technology make it ideal for data exchange and privacy protection. This study paradigm may improve computer network reliability while also allowing new distributed and knowledge-driven security services and applications. Numerous issues are addressed in this work, including new cryptographic models for healthcare applications, intelligent threat-detection systems and novel approaches to consensus building in blockchains.

Keywords: Blockchain, natural language processing, security system, artificial intelligence

1. Introduction

Internet of Things (IoT) devices, such as smartphones and satellite phones controls many sensors that connected in the home or industry environments through any digital networks. To keep up with ever-increasing demand and supply, social exchanges and marketplaces help to accelerate the development of new technologies at an ever-increasing pace.

DOI: https://doi.org/10.36548/jscp.2022.2.005
Received: 25.05.2022, received in revised form: 30.06.2022, accepted: 15.07.2022, published: 25.07.2022

Artificial Intelligence (AI) algorithms use data as input to extract important properties. However, data on the Internet is dispersed and controlled by a variety of stakeholders that lack trust in each other, making it difficult to authenticate or confirm the use of the data in a complex cyberspace. Enabling accurate big data and actual potent AI data to be shared in cyberspace is thus hard [1 - 5].

The three views of artificial intelligence examined in this study are:

- Natural Language Processing (NLP),
- Computer Vision, and
- Acoustic AI

Computer systems will be able to derive, summarize, translate, and synthesize precise text and voice after they've completed their task. Clinical professionals would be overwhelmed if they attempted to manually process and interpret this massive amount of data. Extracting crucial facts from text, classifying data, and mining opinions are all possible with NLP's help. To make sense of all of this new information, NLP uses machine learning to break it down into smaller, more understandable chunks. It may also assist physicians in their decision-making, locate the most essential patients, and categorize various illnesses.

Big companies are attempting to acquire as much relevant data as possible in order to maintain a competitive advantage in the information age [4, 5]. There is a significant danger of privacy leakage for data owners because of the built-in sensors in the devices of these large corporations, which gather personal data such as location information, web-searching activity and user calls [6, 7]. Because Chi-Yuan Chen, the associate editor who coordinated the article review and approved it for publication, used the data, the data's owners have no say in how they are used. Data abusers can't be found or punished since it's impossible to track or document how and by whom the data is being utilized [8]. An inability to adequately handle data makes it impossible to regulate the possible hazards linked with the obtained information. These are used in BC-based on functions and procedures. Incorporating these notions with internal corporate or organizational audits, a policy implementation operation provides validity, anonymity, and transparency. This system is less trustworthy by design, but it also offers fairness and transparency in transactional processes.

It's not the first study on blockchain in healthcare, but it's notably different from the others. An in-depth look into blockchain-based artificial intelligence healthcare applications in the Natural Language Processing, Computer Vision, and Acoustic AI areas, as well as the

promise of AI in healthcare, and the adversarial assaults they may face, is presented in this article. The research gaps that are being highlighted as a result of this also help to illuminate possible future research directions [9].

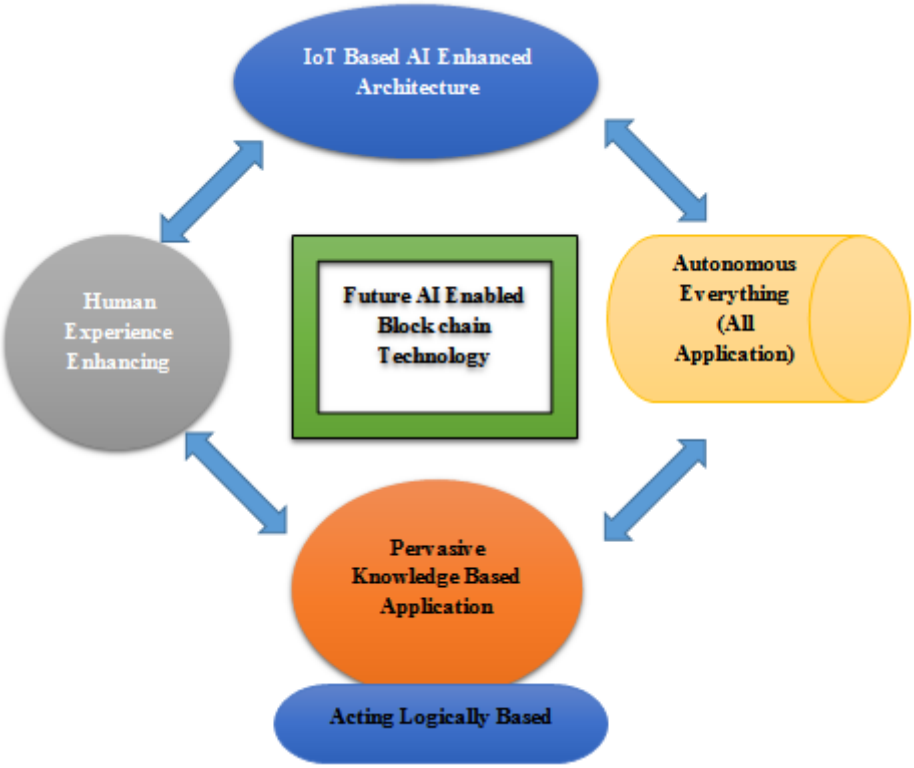

Figure 1. Future Blockchain Technology

2. Future Blockchain Technologies

The issues AI faces may be addressed in a variety of ways via Blockchain technology, as shown in Figure 1. Transactions are copied throughout the blockchain's ecosystem in a distributed ledger known as the blockchain. As information is encrypted, the blockchain's consensus system, smart contracts, and other security and privacy features are added. For one thing, it helps to establish user confidence. As a result, AI-based healthcare can develop trust, organize data, and facilitate resource sharing [10].

The peer-to-peer networks use blockchain technology to maintain a distributed ledger. Secure transaction records are kept on a distributed ledger. By storing local gradients on the blockchain, this feature enables safe distributed or federated learning on heterogeneous data. Intelligent contracts automate the execution of transactions in a dispersed network by eliminating the need for a third party or a central authority to step in and oversee the process. A smart contract is a piece of code that can be executed by any node in the network as soon

as the transaction is started. The transaction is verified through smart contracts. Smart contracts may be used to enforce data access policies. Smart contracts make it feasible to verify the identity of the user. Transactional data generates a block. Consensus algorithms are used by miners to add blocks to the blockchain. The block is mined via consensus methods. In order to participate, miners are required to work together to solve cryptographic riddles and then present their findings to the rest of the community. In AI-based healthcare systems, consensus algorithms may be used to make collective decisions on diagnosis and treatment. Linked cryptographically, blocks are unable to be changed or tampered with.

A study by Rawindaran et al., indicated that people's perceptions about machine learning (ML) and how it might be used are still developing [11]. The prediction of text in social media evaluations on many e-commerce are real-world instances of supervised learning, as are the correlations between a company's income and employees.

At three locations in Singapore and China, Schmetterer et al., demonstrated how an AI platform based on blockchain might be used to build real-world data transmission, model transfer, and model testing. It is developed and tested using retinal pictures from diverse multi ethnic populations in various nations. This diagnostic performance is more accurate because of deep learning algorithms; they used blockchain enabled AI infrastructure that ensures safe data transmission that is permanent and verifiable as well as transparent model transfer. However, data security is compromised as a result [12].

Automated detection of stomach infections using wireless capsule endoscopy frames has been studied by Khan et al. Convolutional Neural Networks (CNNs) are utilized to accurately predict gastrointestinal illnesses including ulcers and bleeding using a blockchain-based method [13]. Each layer has an extra block that protects data from being altered or tampered with. Texts like social media postings may have their emotional and tonal content classified using AI technologies, such as natural language processing (NLP), according to Pilozzi et al. These methods might be used to examine the public's impression of Alzheimer's disease. Data transport and storage systems like blockchain will allow patients more control over their information. Providing personal information to an organization that may use it to discriminate against them will be less of a concern for most individuals [14].

2.1 Purpose of this Review

With AI-based health care, the ability to better diagnose and treat patients will be enhanced via the use of data-driven learning and investigation. Additionally, this raises issues

of privacy, data management, and money generating from the sensitive information of patients. Establishing confidence in the data needed to train machine learning systems is essential. Those patients get timely support to address chronic or acute illnesses, and that treatment quality is excellent. Despite the immense promise of artificial intelligence and machine learning in medicine, there are a variety of adversarial assaults on NLP, computer vision, and acoustic AI that restrict its widespread use in real time. These assaults should not be accepted in sensitive sectors such as healthcare.

2.2 Evaluation Solutions

In the context of NLP, computer vision and acoustic AI, blockchain will safeguard against adversarial assaults. The combination of blockchain and AI-based healthcare has the potential to be transformational in terms of security and privacy. Existing blockchain-integrated AI-based healthcare applications are examined in this paper. The same is given a conceptual context. This contribution will help scholars better understand the potential of the blockchain in healthcare.

2.3 Intelligent Framework

These findings provide an intelligent framework for recognizing and detecting corrupted network packet data, which is consistent with the above. In order to help in the construction of the aforementioned framework, a literature study should be conducted to determine the most current methodology, strategies, and procedures. An intelligent automated technique is used to acquire network data at predetermined intervals, minimizing human interaction. All of this information is then put through its paces in order to determine whether or not it can really be implemented.

3. Security Systems

3.1 Blockchain Technology

The initiator signs each transaction, which is subsequently processed by the miner and validated. The transaction has been confirmed and is included in the block. Once the hash value of each transaction has been computed, it is repeated until a Merkle root can be found and written into the block header by adding the hash values together in pairs again. It is the Merkle root that is impacted by every update to the blockchain data. Thus, the immutability

of blockchain may be achieved. Hash and timestamps from earlier blocks are also preserved, creating a time-ordered chain [15].

3.2 Artificial Intelligence

Computer vision and natural language processing are only two of the numerous areas in which artificial intelligence is being studied. Modern AI relies heavily on machine learning to learn from and mimic human behavior and cognitive patterns as closely as possible. For a long time, researchers have been working on improving machine learning approach.

1. Deep learning,
2. Reinforcement learning, and
3. Federated learning are now part of a full technological framework.

3.3 Blockchain Solution for AI-based Healthcare

Allowing healthcare companies the ability to provide better and more efficient treatment to an increasing number of patients is one of the primary benefits AI may provide to the healthcare industry. Artificial intelligence may also assist healthcare providers in providing better care to patients by reducing stress and focusing on immediate needs. There is evidence to suggest that NLP. There are several advantages to using artificial intelligence in the healthcare business, but particular dangers continue to hinder its use in crucial applications. The attack surfaces of AI are data, classifiers, and algorithms. We've looked at a variety of assaults on text, graphics, and audio [16- 19].

Data, algorithms, and computing power are three key components of AI technology. Data is needed to train algorithms in order to produce classification models, and computer power is required throughout the training process. The data we have now comes from a variety of sources, including sensor systems, IoT devices.

3.4 Machine Learning

Supervised, semi-supervised, and unsupervised learning are the most common types of machine learning. Predictive models are built using training sets that are labelled. The Data sets with no labels are used for training. Unsupervised learning relies on figuring out whether the data has a divisible set by examining the data's hidden structure. For training and classification, semi supervised learning utilizes a small quantity of labelled data as well as a big amount of unlabelled data [20 - 22].

3.5 Mitigate Attacks Approach

In the face of more skilled hackers and bots, society has forced to turn to machine learning and artificial intelligence for help. In addition, an Intrusion Detection and Prevention (IDPS) system may assist machine learning learn how to distinguish between positive and bad patterns on the weblink. Data security requires a variety of ways. The ML via anomaly detection demonstrated to be more successful than signature-based zero-day detection in the market. The problem is that there is a huge gap that has to be addressed, maybe with new sorts of devices used by SMEs, such as open source and volunteers who utilize their expertise of the community to ensure that these devices are always up to date [23]. Figure 2 shows AI in Block-chain for security systems.

3.6 Healthcare systems with AI

Artificial intelligence is rapidly being incorporated into healthcare systems, but it is not a panacea for all problems. The healthcare industry, from infectious illnesses to cancer to radiography, is in serious need of change. Technology may be used in various ways to improve treatment accuracy, reliability, and effectiveness. When used appropriately, these therapies may be precise in a therapeutic setting. In order to do tasks that would normally need the use of human intellect, artificial intelligence relies on computer programs that include specialized instructions. Codified programming rules are what we mean by algorithms. An algorithm can be continually improved via machine learning. It is possible to increase the artificial intelligence's accuracy via the use of large amounts of data and dynamic processing. Artificial intelligence is capable of comprehending and interpreting language, recognizing objects, detecting noises, and developing patterns to solve problems [24, 25].

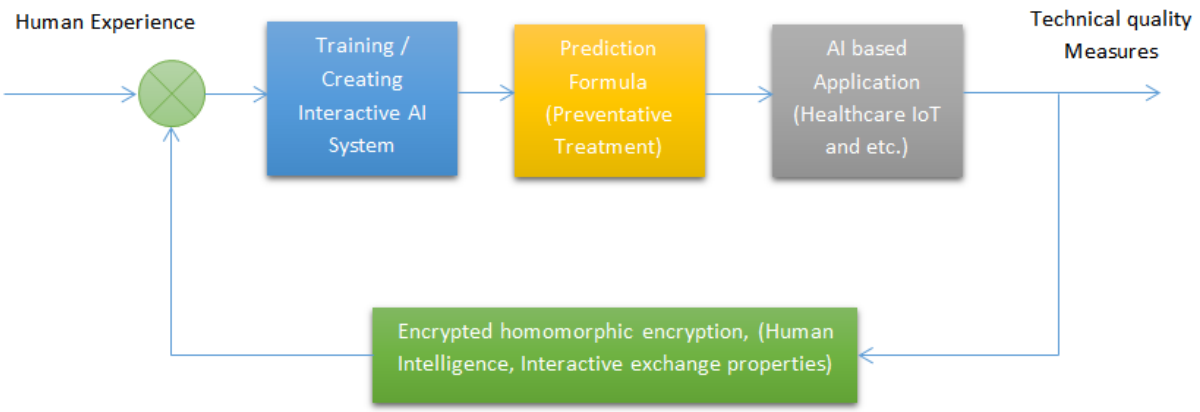

Figure 2. Future Direction of AI in Block-chain for security systems

4. Future Directions

For each form of severe respiratory illness, they've included synthetic cough samples that were cleverly produced using recent advances in generative adversarial networks. This has helped to balance and broaden the dataset. Predictive algorithms and clinicians may benefit from CoughGAN's simulated coughs, which represent serious pulmonary problems. Preventative treatment strategies and morbidity may be reduced by early and precise detection of advanced respiratory disorders such as chronic obstructive pulmonary disease by doctors. As a result, the system's ability to distinguish between benign and harmful sounds is compromised because of noise that interferes with accurate detection. In order to guard against malicious assaults, it has included two types of adversarial training: vanilla and a unique similarity-based training contribution. Adversarial training uses both real and made-up data to develop skills. However, the detector must be trained on a large amount of negative data.

Healthcare IT systems in India are presently uncoordinated. Because of a variety of digital solutions, interoperability issues develop. In order to build interoperability, it is challenging since healthcare institutions have distinct models and use different codes. The situation becomes worse when patients move providers for unknown reasons. Diagnostic tests and treatment processes must be repeated several times on patients, resulting in increased overhead expenses and dissatisfied patients. When working with encrypted data, homomorphic encryption is one of the most secure methods for protecting the data's privacy. The same results may be achieved with encrypted data as with unprotected data. Homomorphic encryption, on the other hand, does not compromise the anonymity or privacy of data in organizations. Homomorphic encryption may be used for secure outsourced storage and computation. If you think of asymmetric-key or public-key cryptography as a progression of homomorphic encryption, you're correct. Like homomorphisms in algebra, the encryption and decryption functions are homomorphisms between the plaintext and ciphertext spaces.

5. Conclusion

Digital systems, computing data, and the trust mechanisms that go along with them, all face several security challenges. As a consequence of these difficulties, new technology solutions have emerged. Strong solutions will be required when the cyber world changes even further. Because of its inherent characteristics, blockchain technology is well-suited for use in securing and distributing data. Even in AI-based healthcare, where data sharing and privacy

are in conflict, blockchain technology has a unique ability to resolve the issue. NLP, computer vision, and acoustic artificial intelligence may all benefit from a blockchain architecture that synthesizes these technologies. This assessment has discussed the current AI-based healthcare applications, adversarial assaults, and dangers in the existing technologies.

References

[1] L. Demetrio, A. Valenza, G. Costa, and G. Lagorio, "Waf-a-mole: evading web application firewalls through adversarial machine learning," in Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 1745–1752, Brno, Czech Republic, March 2020.

[2] E. Quiring, D. Klein, D. Arp, M. Johns, and K. Rieck, "Adversarial preprocessing: understanding and preventing image-scaling attacks in machine learning," in Proceedings of the 29th USENIX Security Symposium USENIX Security 20, pp. 1363–1380, Boston, MA, USA, August 2020.

[3] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: a secure blockchain-based data trading ecosystem," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 725–737, 2020.

[4] Y. Wu, Z. Wang, Y. Ma, and V. C. M. Leung, "Deep reinforcement learning for blockchain in industrial iot: a survey," Computer Networks, vol. 191, Article ID 108004, 2021.

[5] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: review and open research challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019.

[6] Z. Zhang, X. Song, L. Liu, J. Yin, Y. Wang, and D. Lan, "Recent advances in blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work," Security and Communication Networks, vol. 2021, Article ID 9991535, 2021.

[7] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: challenges posed by adversarial machine learning and the way forward," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998–1026, 2020.

[8] B. Biggio, L. Didaci, G. Fumera, and F. Roli, "Poisoning attacks to compromise face templates," in Proceedings of the 2013 International Conference on Biometrics (ICB), pp. 1–7, IEEE, Madrid, Spain, 4-7 June 2013.

[9] Y. Xing, C. Lv, X. Mo, Z. Hu, C. Huang, and P. Hang, "Toward safe and smart mobility: energy-aware deep learning for driving behaviour analysis and prediction of connected vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4267–4280, 2021.

[10] M. Dabbagh, M. Kakavand, M. Tahir, and A. Amphawan, "Performance Analysis of Blockchain Platforms: Empirical Evaluation of Hyperledger Fabric and Ethereum," Sep. 2020. doi: 10.1109/IICAIET49801.2020.9257811.

[11] Rawindaran N, Jayal A, Prakash E. Artificial intelligence and machine learning within the context of cyber security used in the UK SME Sector. In: AMI 2021— the 5th advances in management and innovation conference 2021. Cardiff Metropolitan University. 2021.

[12] L. Schmetterer et al., "Retinal photograph-based deep learning algorithms for myopia and a blockchain platform to facilitate artificial intelligence medical research: a retrospective multicohort study," 2021. [Online]. Available: www.thelancet.com/

[13] M. A. Khan et al., "A blockchain based framework for stomach abnormalities recognition," Computers, Materials and Continua, vol. 67, no. 1, 2021, doi: 10.32604/cmc.2021.013217.

[14] A. Pilozzi and X. Huang, "Overcoming alzheimer's disease stigma by leveraging artificial intelligence and blockchain technologies," Brain Sciences, vol. 10, no. 3. MDPI AG, Mar. 01, 2020. doi: 10.3390/brainsci10030183.

[15] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng, and N. Guizani, "Smart contract vulnerability analysis and security audit," IEEE Network, vol. 34, no. 5, pp. 276–282, 2020.

[16] M. Bhargavi, S. M. Katti, M. Shilpa, V. P. Kulkarni, and S. Prasad, "Transactional data analytics for inferring behavioural traits in ethereum blockchain network," in Proceedings of the IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 485–490, IEEE, Cluj-Napoca, Romania, 3-5 Sept. 2020.

[17] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in Proceedings of the 2019 International Conference on Management of Data, pp. 123–140, Amsterdam, Netherlands, June 2019.

[18] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. R. Choo, "Sidechain technologies in blockchain networks: an examination and state-of-the-art review," Journal of Network and Computer Applications, vol. 149, 2020.

[19] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory," IEEE Internet of $ings Journal, vol. 6, no. 6, pp. 10700–10714, 2019.

[20] J. D. Harris and B. Waggoner, "Decentralized and collaborative ai on blockchain," in Proceedings of the IEEE International Conference on Blockchain (Blockchain), pp. 368–375,

[21] Wang, Guojun, Jun Feng, Md Zakirul Alam Bhuiyan, and Rongxing Lu, eds. Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2019 International Workshops, Atlanta, GA, USA, July 14–17, 2019, Proceedings. Vol. 11637. Springer, 2019.

[22] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, and P. Li, "Ai at the edge: blockchain-empowered secure multiparty learning with heterogeneous models," IEEE Internet of $ings Journal, vol. 7, no. 10, pp. 9600–9610, 2020.

[23] Qi X, Zhang Z, Jin C, Zhou A. A reliable storage partition for permissioned blockchain. IEEE Trans Knowl Data Eng. 2021;33(1):14–27.

[24] Robertson E, Reeve KS, Niedzwiedz CL, Moore J, Blake M, Green M, Katikireddi SV, Benzeval MJ. Predictors of COVID-19 vaccine hesitancy in the UK Household Longitudinal Study. Brain Behavior Immunity. 2021.

[25] MacKenna B, Curtis HJ, Morton CE, Inglesby P, Walker AJ, Morley J, Mehrkar A, Bacon S, Hickman G, Bates C, et al. Trends, regional variation, and clinical characteristics of COVID-19 vaccine recipients: a retrospective cohort study in 23.4 million patients using Open SAFELY. 2021.

Author's biography

Haoxiang Wang is currently a director and lead executive faculty member of GoPerception Laboratory, Ithaca, USA. His research interests includes multimedia information processing, pattern recognition, machine learning, remote sensing image processing, and data-driven business intelligence. He has co-authored over 60 journal and conference papers in these fields on journals such as Springer MTAP, Cluster Computing, SIVP; IEEE TII, Communications Magazine; Elsevier Computers & Electrical Engineering, Computers, Environment and Urban Systems, Optik, Sustainable Computing: Informatics and Systems,

Journal of Computational Science, Pattern Recognition Letters, Information Sciences, Computers in Industry, Future Generation Computer Systems; Taylor & Francis International Journal of Computers and Applications and conference such as IEEE SMC, ICPR, ICTAI, ICICI, CCIS, and ICACI.