Journal of Computer and Communications, 2022, 10, 11-21
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Use of AI Voice Authentication Technology Instead of Traditional Keypads in Security Devices

Deepak Ramesh Chandran

Iris Energy LLC, Edison, USA
Email: cdr22@me.com

How to cite this paper: Chandran, D.R. (2022) Use of AI Voice Authentication Technology Instead of Traditional Keypads in Security Devices. *Journal of Computer and Communications*, **10**, 11-21.
https://doi.org/10.4236/jcc.2022.106002

Received: April 19, 2022
Accepted: June 10, 2022
Published: June 13, 2022

Abstract

Traditional keypads and text-based passwords are vulnerable to scams and hacks, leading to enormous levels of embezzlement and frauds apart from various other threats to data security. AI based voice authentication holds unparalleled value for data protection, security, and privacy, by providing an effective alternative to traditional password-based protection. This paper reports the findings of a limited literature review that forms the basis for further research towards enhancing the reliability and security of AI voice authentication. Based on the findings of the review of existing literature, this paper proposes that integration of the blockchain technology with the AI voice authentication can significantly enhance the data security, starting from mobile devices to the security of big agencies and banks. The key processes in implementing an AI voice authentication system are proposed as a conceptual model, to facilitate further research for implementation.

Keywords

Artificial Intelligence, Voice Authentication, Blockchain, Data Security, Automatic Speech Recognition, Voice Biometrics

1. Introduction

Amidst ongoing cyber-attacks, privacy issues, data breaches, and security issues, AI (artificial intelligence) is gaining unprecedented value. AI's contribution to facial recognition, content creation, and voice recognition alone has changed the dynamics of the whole web. We are observing a massive adaptation of technologies like Alexa, Siri, Amazon Echo, and Google Home. These technologies are changing the dynamics of web search, and the shift is from typing text to voice recognition. In 1964-1965 Woody Bledsoe, Helen Chan Wolf, and Charles Bisson were the first group of people who took the initiative in automated facial recognition technology. Nowadays, all fields, including data security, surveillance systems, mobile and app development, e-commerce, and trading, are shifting toward facial recognition technology because of automation and better security [1].

According to the annual report of Internet Crime Complaint Centre (IC3) of FBI, crimes involving cyber-attacks and malicious cyber activities are steadily increasing over the years. In 2021, IC3 received 847,376 complaints involving cybercrimes, which was 7% increase from the year 2020. The potential losses from these complaints were estimated to be over $6.9 billion [2]. Before the world got its hands on using technology to get better financially, people on the other side of the law were also using it for that purpose. That's one of the main reasons we must make sure our financial system remains secure.

In 2021, from January to September, almost 281 million people were affected by ongoing data leaks and data breaches, according to the data provided by the Identity Theft Resource Center (ITRC) [3]. In the first half of 2021 alone, scammers and criminals could steal a total of £754 million, which was 30% more than the amount scammed in the corresponding period in 2020. Most of these scams were done by APP (Authorized Push Payments), but banks could save about £760 million by advanced security systems [4]. A recent IBM study suggests that almost 1/5th of data breaches occur due to compromised credentials. Their report states that by 2021, nearly 25% of industries will have implemented AI-based security systems, 40% will be implementing them, and 35% will suffer a data breach. With AI voice authentication, $3.81 million was saved [5].

The use of AI-based neural networks in spam detection, zombie detection, malware classification, denial-of-service (DoS) detection, computer worm detection, and forensic investigations is unparalleled. In the realm of AI, Artificial Neural Networks (ANN) is a computational mechanism that simulates functional and structural features and was proven to be at least 20.5 times faster in detecting DoS attacks. Another system called Intelligent Agent Applications works with an automated computer-generated response system that communicates, cooperates, and shares data in such a collaborative manner that it can detect all types of responses. Almost all cybercrimes and fraud work on some similar patterns, and with the identification of such patterns, we may be able to build an unbreakable system soon, with blockchain, AI, and cybercrime pattern alert mechanisms [6].

Integrating AI voice authentication with the blockchain technology can not only ensures privacy but can also prevent data breaches. Passwords entered by hand and knowledge base authentications are traceable and vulnerable to hacking. Issues like forgetting passwords, the use of the same password, time consumption, and locked accounts are all annoying problems people face in current verification procedures [7]. However, the most pertinent question is: how can blockchain technology be adopted at scale before it can be integrated with AI to create security systems? A large scale can be achieved with some adjustments. Currently, the system is capable of retaining all financial transactions, but privacy is very critical. Blockchain technology can achieve more than anyone ever imagined, by establishing a security key and a way to manage it. It can be a step toward creative destruction. For this to happen, all current users must agree on a user agreement and rights guide under which they will be part of the blockchain system. Creating rights is the only way to encourage people to create a supervisory authority in the current blockchain system. This is because blockchain technology can permeate all industries. While it is not an easy process, it is critical to deal with tax evasion, cyber fraud, and money laundering occurring on a blockchain under the privacy umbrella. It simply means that security and supervisory duties can only be coordinated, if everyone is in agreement. A working group has already been formed by the Digital ID & Authentication Council of Canada [8].

This paper is proposing a conceptual model for implementing an AI voice authentication system integrated with the blockchain technology, based on a limited and targeted narrative review of the existing literature on block chain and AI voice authentication. This paper does not consist of a systematic review of the literature [9] and is limited to exploring the current level of knowledge in the relevant fields, as it informs author in ongoing research towards creating a robust system for implementation. Using the findings from this narrative approach to the literature review [10], a conceptual model for implementing a blockchain based AI voice authentication system is developed and presented.

2. Literature on AI Voice Authentication

Traditional authentication systems suffer from various drawbacks that include having to remember many different login ids and passwords, inability to use when the user's hands are not free as in driving a vehicle, and the possibility of duplication and fraudulent misuse [11]. These drawbacks can be overcome by adopting human voice for user authentication. There are many algorithms gaining maturity for human recognition and authentication based on the voice [11]. Besides, voice is the only biometric feature which is capable of being stored, compared, and authenticated remotely-either through a phone or through the internet [12].

Today, the use of AI voice authentication technology in security devices extends beyond just technological innovation. With blockchain integration and AI voice verification, the user is only susceptible to APP (Authorized Push Payments). AI voice recognition systems like Siri and Google Home are going to have more than 8 billion users by 2023. Artificial intelligence technology will replace traditional keypads and typing technology, and the parameters on which it will be implemented are security, authentication, and privacy.

AI-based voice authentication is difficult to integrate with all security devices and systems to ensure data privacy. A first step can be taken with those devices where data compromise can be costly. Scams involving ATMs are common worldwide. Scammers employ various crimes, including the Lebanon loop, card skimming, and cash trapping. In this case, ATM owners need to stop the unauthorized deployment of these types of malwares on their ATMs. This can be solved by ensuring that only authorized users can run the code, see it, and use it to withdraw cash. ATM PC core BIOS must be protected with a code that can't be hacked or manipulated by anyone [13].

Smart cities will utilize the growing Internet of Things (IoT) technology to process and manage modern cities in the future. In future, applications and systems such as Google Business, cloud computing, geographic information systems, and big data will create the roots of modern urbanization. In simple terms, computer applications and digital systems are set to integrate from the commerce sector into the health sector, including all fields. But this digital system is not protected and is vulnerable to attacks by hackers and cybercriminals. For such cities to become a part of the future, two things are required, the first being active surveillance by AI integrated bots and human management teams to detect frauds and anomalous activity, and the second being the incorporation of a public blockchain, supervised by a regulatory authority on the rights and duties agreements [14].

Glowacki and Piotrowski [15] suggested a new architecture for voice identity distribution, to prevent any possible "unauthorized subscriber impersonation and unauthorized voice message edition". This architecture uses the data hiding technique to provide voice authentication. Another study conducted on the users of Google's wearable glasses found that it was possible to achieve user authentication with near perfect accuracy (99% detection rate and 0.5% false alarm rate after only an average of 3.5 user events) by combining a set of touch behavioral features and voice features [16]. Panda [17] presented an algorithm that allows voice authentication after analyzing the user voice from varied environmental conditions. Such advancements in the technology are increasing the reliability of voice authentication [18].

In addition to ATMs, there have been breaches at vaults, security agencies, and all types of businesses. A voice authentication system based on artificial intelligence will eliminate all these traditional hacks and scams. One can use voice authentication to create a bank vault that opens only when the cash delivery van arrives with a person whose voice acts as a password. There are a lot of possibilities and prospects of this technology as far as innovation is concerned. The vulnerabilities associated with traditional keypads will be eliminated in all fields and dimensions. Currently, it is not possible to increase the privacy of these security devices. However, with the integration of AI base voice verification and blockchain technology, a highly secure system can be created. Through blockchain, we will be able to create a protected private system that cannot be compromised without both end-user keys. It will be difficult for cyber scammers to compromise the system through AI voice verification. It will replace the traditional keypads and improve the privacy and security of the system.

Blockchain technology can be used as a fraud prevention tool [19]. The AI can be used to create a system where no transaction can take place until the user's identity is verified. A blockchain cannot do everything, but it can be an asset when it comes to ballot stuffing, Sybil, and continuous attacks. Use of blockchain can become the differentiating factor for applications from various domains, in terms of their security and privacy [20] [21]. By integrating AI with public rights and policy, it may be updated to a point where it can detect fraudsters and detect the patterns of their tactics. It could create an alarm system to remind the security system that something is amiss [22].

Most transactions, communications, and business are now conducted through handheld devices. Almost 2 billion people use mobile apps to pay their bills. Millions of users are being added to these numbers daily [23]. However, the majority of these mobile verification systems rely on keypad passwords, pattern locks, or even face recognition. The time has come for us to update our mobile security to a level where it's nearly impossible to crack. The current systems can be consolidated with a blockchain-based AI voice authentication security system. This will eliminate the risk of password theft, scams, and other vulnerabilities. The only way for someone to bypass a security system is when the user opens it with a voice authentication.

3. A Conceptual Model for Integration of Blockchain with AI Voice Authentication

As the review of existing literature showed, integrating with blockchain can significantly enhance the effectiveness of the AI voice authentication in minimizing threats to data security. Blockchain, however, is not accessible to all users unless they are part of a single transaction. With a surveillance body, rights and obligations agreement, and privacy protection, we can take blockchain-based AI security systems to a new level where they can be integrated with different systems across cities and countries.

Creating an AI voice authentication system that integrates blockchain is complex. The first step should be to develop a separate voice authentication system based on AI and build a blockchain-based matching database. This paper proposes a conceptual model on how to create and implement an artificial intelligence system.

3.1. Highlighting Voice Enrolment

Each of us has a unique voice, to be extracted and recorded by an AI algorithm. There are two major aspects of voice authentication.

3.1.1. Physiological Features

In this category, all physiological features like tone, pitch, and volume are analyzed and enrolled by AI.

3.1.2. Behavioral Features

This includes features like accents, regional dialects, and idiosyncrasies [24].

These voice features are detected by the sensor module of the AI voice authentication system. This sensor module can be a microphone, headphone, or device that can capture voice and break it into different features [25].

AI is now at a point where it can understand such diversified patterns, and the connected blockchain can act as a locker. Medical researchers are currently using decentralized blockchain databases in which AI-based machine learning algorithms can detect patterns and symptoms among patients through different types of imaging. A system was created to give doctors information about what is happening inside a patient based on images and collected medical data. The system they created involved:

1) Developing an artificial intelligence algorithm based on secure medical data obtained via smart contracts.

2) Using a distributed network of blockchains to train a global model using localized deep learning of CT scans, ECGs, EEGs, and other medical tests [26].

A probable feature of this system could be using AI to detect human voices to verify security using facial features and incorporating it with the blockchain backend. The creation of an AI-protected blockchain system will not be impossible if a method for detecting diseases is developed with the help of a few medical tests.

AI voice enrolment uses a recording of the voice. Afterward, the recording is sent to a biometric engine, where multiple templates are combined to create a voice print used for identification. Whenever the user speaks, a specific key is generated based on the match of the voice. This key will open the other end of the key, ensuring the security system is unlocked. Multifactor AI voice authentication will replace traditional keypads and password codes and vulnerabilities [27].

In this system, there are five basic modules: sensor module, feature extraction module, feature matching module, database module and decision-making module (see Figure 1). As a result of combining these modules, a blockchain-based voice authentication database can be created step-by-step [25].

3.2. Speech Biometrics/Voice Biometrics

Voice biometrics is the science of identifying a specific person based on his voice. This identity verification system is not as easy as it sounds. More than 70 body parts are required to produce a unique voice; this AI voice authentication

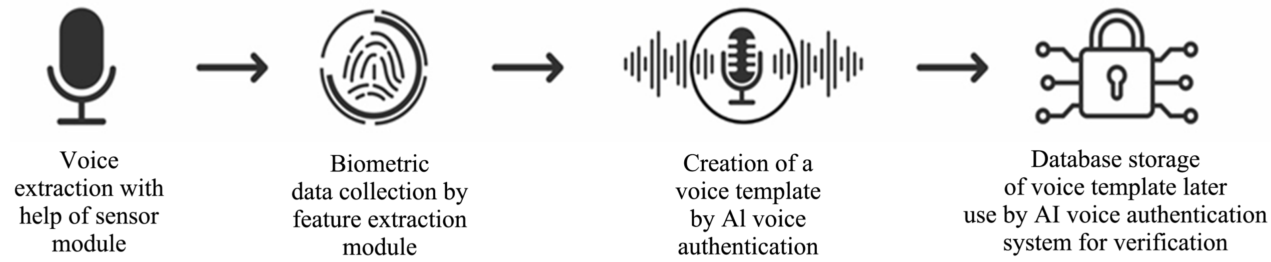
Voice extraction with help of sensor module
Biometric data collection by feature extraction module
Creation of a voice template by AI voice authentication
Database storage of voice template later use by AI voice authentication system for verification

Figure 1. Creation of blockchain based voice template for authentication.

system also involves pitch, volume, language, and style. When a person's voice is recorded, a specific biometric engine generates a voice template to merge multiple voice recordings. AI voice biometrics includes tone, volume, pitch, language, and many other factors that combine to produce the most accurate template for identification. The machine learning mechanism chooses the most suitable recordings to create such a template that can cover all possible input from the users. This feature extraction module is based on the extraction of sound clips and creating the most relevant template for identification. Compared to speech biometrics, in keypad biometrics there is no such multifactor association that can provide multiple layers of security for the user. Due to the integration of the blockchain, it is difficult to breach, unless the user opens it with their own voice [26].

3.3. Voice as Password and Automatic Speech Recognition

The voice template must be recorded and stored in a blockchain-enabled database. Based on this template, users will verify their voice input's accuracy. Putting it simply, AI matches the input voice with a template in the blockchain database based on the input information (**Figure 1**). After the two voices match, the security system automatically unlocks. There are features in this template that AI matches to ensure that the security system remains unbreakable. To verify the authenticity of the system, artificial intelligence analyses the voice input on its own based on the available template. Therefore, if the user is real, the system will unlock. The AI verifies the voice authentication by matching the available template in the database against the input voice to unlock the system.

3.4. Blockchain Integration

A blockchain-based security system means that the security system cannot be unlocked until the one-side key is verified through voice authentication by AI (**Figure 2**). Since blockchains are undatable, once a security system based on a verification procedure is created, one cannot change it. An AI voice authentication system that integrates blockchain will ensure the security system won't be compromised until the key is released by voice verification. The important thing

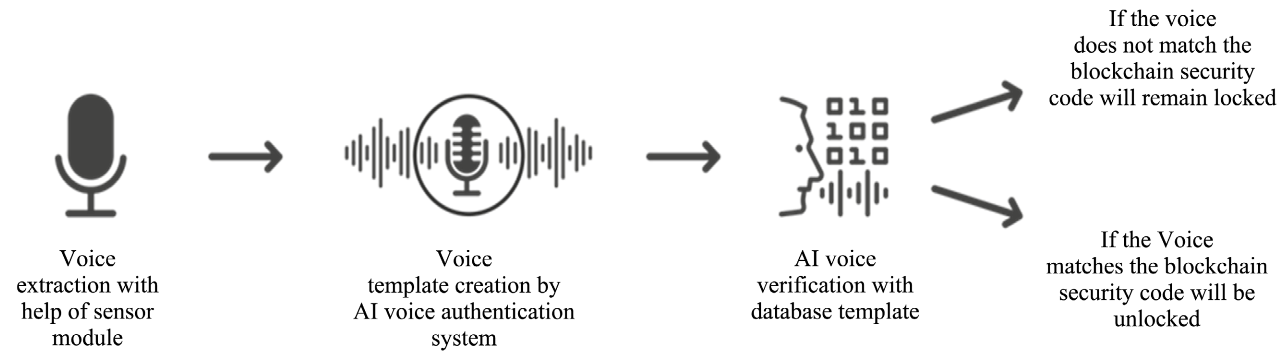
Voice extraction with help of sensor module
Voice template creation by AI voice authentication system
AI voice verification with database template
If the voice does not match the blockchain security code will remain locked
If the Voice matches the blockchain security code will be unlocked
010
100
010

Figure 2. Voice authentication against Blockchain based database template.

is how it works. Using machine learning mechanisms, AI will verify the voice, releasing the key and unlocking blockchain-based security systems [28]. Blockchain needs a stable organization that can oversee it at the state level to trace fraudulent activities back to their roots, which is only possible by integrating rights and duties with the users.

Voice authentication will ensure that only the authorized user can unlock the database, whether an ATM security code, a house security code, or an agency security code. There is no way anyone can unlock it except for APP (Authorized Push Payments). The old keypads will be eliminated here because of two major factors. The 1st factor is the security assurance. AI voice authentication ensure more security as compared to keypad codes because of no loopholes of breaching. The 2nd factor is blockchain integration that makes sure that the other end is safe and sealed until the voice is verified. We can merge blockchain with traditional keypads passwords, but it will not eliminate the scam and hacking threats. It will not be beneficial to adopt a blockchain database security system in such a case. However, by contrast, an AI voice authentication system with blockchain end eliminates all such concerns, giving users more than one reason for adopting this technological innovation.

4. Discussion

Blockchain voice authentication holds incredible potential. Nearly any field can benefit from it. There are many ways to implement security systems, from the security of an ATM to the security of a secret intelligence system. A high-security prison requires that only the warden and officers pass through cells. Elite prisons are occasionally subject to breakouts, but one can prevent these by using AI voice authentication lock technology based on blockchain. Hackers' risks and the risk of clever criminals getting an edge over the system will be eliminated.

The security of government agencies, secret services, and government associations can all be strengthened with the help of an AI voice authentication system. These days, it has become common that many orders require a code or approval from a higher-up to begin the process. Voice authentication and verification can make these orders more secure. Generally, security orders are transmitted using Morse code to verify that they are from the authorized sources. It can, however, be replaced with an AI-based voice verification system and can eliminate the risks of security and privacy. Morse codes, keypad codes and typing messages can all be eliminated with this new technology.

Data and document security are one of the major concerns nowadays. Documents shared between two parties should not be breached by a third party. In today's age of innovation, a country's secret documents are nothing less than an asset. Whether they are locked in a briefcase with a code or have digital locks, these documents can easily be compromised. With the integration of a voice authentication system based on artificial intelligence, sensitive documents can be more secure.

5. Conclusion

Looking at the state of developments in technology, the traditional keypad will eventually be replaced by AI voice technology. AI voice technology is the next technological step in privacy and security. The mass adoption of voice assistants like Siri, Alexa, and Google Assistant is already happening, and the same will happen with the security system soon. But as far as blockchain secrecy and decentralization are concerned, it will remain an open question. Without a model of rights and duties, there is no way to utilize public information to trace perpetrators and criminals unless AI is integrated in a manner that allows it to do so on its own. Further research will be required in developing robust systems for integrating blockchain technology with AI voice authentication and for creating protocols and controls acceptable to all the global stakeholders.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Kaur, P., Krishan, K., Sharma, S.K. and Kanchan, T. (2020) Facial-Recognition Algorithms: A Literature Review. *Medicine, Science and the Law*, **60**, 131-139. https://doi.org/10.1177/0025802419893168

[2] Internet Crime Complaints Center (2021) Internet Crime Report 2021. Federal Bureau of Investigations. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[3] Novinson. M. (2021) The 10 Biggest Data Breaches of 2021. CRN. https://www.crn.com/slide-shows/security/the-10-biggest-data-breaches-of-2021

[4] UK Finance (2021) Half Year Fraud Update. https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

[5] Krasnokutsky. E. (2021) Artificial Intelligence (AI) Biometric Authentication for Enterprise Security. MobiDev. https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security

[6] Dilek, S.H., Çakır, H. and Aydın, M. (2015) Applications of Artificial Intelligence Techniques to Combating Cybercrimes: A Review. *International Journal of Artificial Intelligence & Applications* (*IJAIA*), **6**, 21-39. https://doi.org/10.5121/ijaia.2015.6102

[7] ID R&D (n.d.) Frictionless Biometric Authentication Software. ID R&D. https://www.idrnd.ai

[8] Wolfond, G. (2017) A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review*, **7**, 35-40. https://doi.org/10.22215/timreview/1112

[9] Massaro, M., Dumay, J. and Guthrie, J. (2016) On the Shoulders of Giants: Undertaking a Structured Literature Review in Accounting. *Accounting, Auditing & Accountability Journal*, **29**, 767-801. https://doi.org/10.1108/AAAJ-01-2015-1939

[10] Rother, E.T. (2007) Systematic Literature Review X Narrative Review. *Acta Paulista*

de Enfermagem, **20**, 5-6. https://doi.org/10.1590/S0103-21002007000200001

[11] Zheng, Y. and Zhao, S. (2016) A Usable Authentication System Based on Personal Voice Challenge. 2016 *International Conference on Advanced Cloud and Big Data* (*CBD*), *IEEE*, Chengdu, 13-16 August 2016, 194-199.

[12] Aizat, K., Mohamed, O., Orken, M., Ainur, A. and Zhumazhanov, B. (2020) Identification and Authentication of User Voice Using DNN Features and i-Vector. *Cogent Engineering*, **7**, Article ID: 1751557. https://doi.org/10.1080/23311916.2020.1751557

[13] Kasanda, E. and Phiri, J. (2018) ATM Security: A Case Study of Emerging Threats. *International Journal of Advanced Studies in Computers*, *Science and Engineering*, **7**. https://www.researchgate.net/publication/330133482_ATM_Security_A_case_study_of_Emerging_Threats

[14] Lv, Z., Qiao, L., Kumar Singh, A. and Wang, Q. (2021) AI-Empowered IoT Security for Smart Cities. *ACM Transactions on Internet Technology*, **21**, 1-21. https://doi.org/10.1145/3406115

[15] Glowacki, M. and Piotrowski, Z. (2012) Architecture of the Integrated System for Voice Identity Distribution. *Proceedings of* 19*th International Conference on Microwaves*, *Radar & Wireless Communications*, Vol. 2, 542-545. https://doi.org/10.1109/MIKON.2012.6233590

[16] Peng, G., Zhou, G., Nguyen, D.T., Qi, X., Yang, Q. and Wang, S. (2016) Continuous Authentication with Touch Behavioral Biometrics and Voice on Wearable Glasses. *IEEE Transactions on Human-Machine Systems*, **47**, 404-416. https://doi.org/10.1109/THMS.2016.2623562

[17] Panda, S.P. (2019) Intelligent Voice-Based Authentication System. *Proceedings of Third International conference on I-SMAC* (*IoT in Social*, *Mobile*, *Analytics and Cloud*) (*I-SMAC*), *IEEE*, Palladam, 12-14 December 2019, 757-760. https://doi.org/10.1109/I-SMAC47947.2019.9032671

[18] Rashid, J., Teh, Y.W., Memon, N.A., Mujtaba, G., Zareei, M., Ishtiaq, U., Akhtar, M.Z. and Ali, I. (2020) Text-Independent Speaker Identification through Feature Fusion and Deep Neural Network. *IEEE Access*, **8**, 32187-32202. https://doi.org/10.1109/ACCESS.2020.2973541

[19] Thawre, A., Hariyale, A. and Chandavarkar, B.R. (2021) Survey on Security of Biometric Data Using Cryptography. *Proceedings of* 2*nd International Conference on Secure Cyber Computing and Communications* (*ICSCCC*), IEEE, Jalandhar, 21-23 May 2021, 90-95. https://doi.org/10.1109/ICSCCC51823.2021.9478120

[20] Miraz, M.H. and Ali, M. (2018) Applications of Blockchain Technology beyond Cryptocurrency. *Annals of Emerging Technologies in Computing*, **2**, 1-6. https://doi.org/10.33166/AETiC.2018.01.001

[21] Li, W., Zhou, S., Li, R., Zhang, K. and Wang, Y. (2020) Blockchain-Based Data Security for Artificial Intelligence Applications in 6G Networks. *IEEE Network*, **34**, 31-37. https://doi.org/10.1109/MNET.021.1900629

[22] Cai, Y. and Zhu, D. (2016) Fraud Detections for Online Businesses: A Perspective from Blockchain Technology. *Financial Innovation*, **2**, 1-10. https://doi.org/10.1186/s40854-016-0039-4

[23] Curry, D. (2022) Mobile Payments App Revenue and Usage Statistics. https://www.businessofapps.com/data/mobile-payments-app-market

[24] Pinto, R. (2021) Voice Authentication: How It Works & Is It Secure? 1Kosmos.

https://www.1kosmos.com/biometric-authentication/biometric-authentication-voice-authentication

[25] Amin, R., Gaber, T., Eltaweel G. and Hassanien, A.E. (2014) Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. In: Hassanien, A., Kim, T.H., Kacprzyk, J. and Awad, A., Eds., *Bio-Inspiring Cyber Security and Cloud Services: Trends and Innovations*, Intelligent Systems Reference Library, 70, Springer, Berlin, 423-446. https://doi.org/10.1007/978-3-662-43616-5_16

[26] Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W. and Ali, I. (2021) An Integration of Blockchain and AI for Secure Data Sharing and Detection of CT Images for the Hospitals. *Computerized Medical Imaging and Graphics*, **87**, Article ID: 101812. https://doi.org/10.1016/j.compmedimag.2020.101812

[27] ID R&D (n.d.) Voice Biometrics. ID R&D. https://www.idrnd.ai/voice-biometrics

[28] Dibaei, M., Xia, Y., Xu, X., Jolfaei, A., Bashir, A.K., Tariq, U., Yu, D. and Vasilakos, A.V. (2022) Investigating the Prospect of Leveraging Blockchain and Machine Learning to Secure Vehicular Networks: A Survey. *IEEE Transactions on Intelligent Transportation Systems*, **23**, 683-700. https://doi.org/10.1109/TITS.2020.3019101