A Novel Approach for Electronic Medical Records Based on NFT-EMR

https://doi.org/10.3991/ijoe.v19i05.37589

Mohanad A. Mohammed(✉), Hala B. Abdul Wahab
Computer Science Department, University of Technology, Baghdad, Iraq
Mohanad_ali1986@yahoo.com

Abstract—saving the patient medical record electronically is done via electronic medical records (EMRs) where all the patient-related information that consider private and sensitive is usually related to the treatment process, as well as the diagnoses process of a specific patient usually this information needs to be shared and re-submit by many peers doctors with each, In this paper, propose a novel approach for electronic medical records system using a non-fungible token (NFT) based on a customized permission blockchain built with secret sharing technology to reduce the key management overhead as well as provide a readable extension of the ledger to ensure it is easy to read and easy access from any type of computer. The system that uses NFT for electronic medical records (NFT-EMR) ensures easy access and guarantees availability, privacy, and security providing authority to the patient over his data as well as proof of ownership which is done using proof of secret shares and consistency this system can be used in real-world between hospitals and medical centers and within metaverse world. The NFT-ERM system was evaluated using the main evaluation factors used to evaluate blockchain and compared to the standard ERM system.

Keywords—blockchain, NFT, EMR, non-fungible token, electronic medical records, secret sharing

1 Introduction

Life with good health consider the basis of a happy life, and much research focuses on issues related to public healthcare within the social concern [1]. Save the medical history of patients using Electronic medical records (EMRs) is a very important activity related to healthcare where the current doctor can know the type amount of medicine as well as past surgeries and any other useful information to help the diagnosis and treatment, but this sensitive information should be secure and private and no one rather than authorized people can reach or add, information like name address, and blood type … etc. as well as the medical and clinical information such as laboratory reports, doctor decision, diagnoses, and previous surgeries within the patient's life. The EMR systems are used to improve the level of medical services provided to the patient and make the data available to all doctors and medical field workers and ensure the data will not lose for any reason, this can be compared to the traditional paper-based records which have many disadvantages such as damage, stolen, lost and sometimes availability [2].

The electronic system provides more flexibility, efficiency, and less error for both service provider and patient, merging the medical care services with technologies brings a lot of benefits to the healthcare interest but also reflects a lot of challenges related to this like low heterogeneity (interoperability) since in real life no way that a patient can limit their selves to one doctor or even one hospital since a lot of special specialties needed for different types of diseases treatments and observations within this case sharing medical record is mandatory, usually, EMRs related to one medical center is not available to other centers for many reasons one of them is lack of coordination between these centers this is a big issue that is needed to be addressed and solved, and also the patient does not have a level of control of their personal information and this may result in tampering or stealing of their information and they do not even know [3]. So, issues related to security and privacy and how to improve those fields as well as management and retrieving will be the main focus of this article using non-fungible tokens (NFT) on a customizable blockchain. Addressing the information security issues related to security and privacy of both medical records and EMRs, a system that is based on blockchain technology that provides data immutable, secure, efficient, and easy to retrieve and provides full control of patients above his data by using non-fungible token (NFT) which proves the ownership of patient on his\her data [4]. Many technologies can be integrated within the blockchain such as the internet of things [5] and artificial intelligence [6] as well as employ this technology within the metaverse world [7]. Using blockchain to overcome this issue and build distributed ledgers used as a non-fungible token (NFT) where data is securely saved within the blockchain and prove the ownership of this history to a specific person, in this paper a proposed NFT based on permissioned blockchain for saving and restoring the medical history of a specific patient.

2 Blockchain technology

blockchain can be summarized as a distributed ledger work within a peer-2-peer network where each peer node has an updated copy of the ledger, within recent years blockchain became a trending technology that provides a huge impact on society and businesses since it has been used within different fields such as administration, financial healthcare, supply chain and more to provide the required security and privacy [8], and later used as a backbone for an application used within the metaverse to solve challenges related to metaverse and proof of ownership via non-fungible token (NFT) [7] and can be merged with artificial intelligence applications to improve the distributed networks [6] as well as merged to the internet of things applications to provide security and privacy [5]. Blockchain mainly consists of data elements called blocks which are linked to each other in a special way where each block within the chain contains the hashes of the previous block and so on to the first block which provides a strong method to insure consistency of blockchain and its data, the blockchain size grows rapidly and scalability one of the limitations related the o blockchain itself, each block contains the transaction data as well as a cryptographic hash of current data and a cryptographic hash of the previous block probably with the timestamp when it is recorded to the chain this help to the resistance of tampering attacks and make the blockchain immutable [8]. Each new block added to the existing chain results in a winning node that reaches a majority of acceptance from the peer nodes and solves complex mathematical operations to reach

a nonce and win the chance to add a block to the chain this scenario may change the reference to which consensus algorithm been used within the chain, since each business and party have their own need there is no universal blockchain that can provide all need and serve all industries and as a result of that different types of blockchain come to the market by researchers and enterprises with different internal rules and protocols reference to consensus algorithm, block content and more but the general structure remain the same three main types of blockchain results permissionless (public blockchain), permissioned (private blockchain), and hybrid blockchain [9–11].

2.1 Public blockchain (Permissionless)

Within this type of blockchain, anyone can join the network and can add data to the blockchain after solving the complex mathematical puzzle and finding the correct nonce without requesting permission as well as verifying and validating the specific transaction, Ethereum cryptocurrency considers a permissionless chain plus it is open source since developers can custom it to create their copy of blockchain with different required rules. The consensus algorithm used on the standard version of the Ethereum blockchain is the proof of work (POW) which is mainly based on mining where each minor should solve his complex math puzzle and find the correct nonce solution to win the right to add data to the chain computing the nonce consider the major energy consumption within the blockchain [12, 13]. Studies prove that PoW reaches a maximum of 60 transactions per second and consume energy equal to country consumption which may affect the scalability as well as the throughput of the algorithm [14] This lead to finding alternatives consensus algorithm rather than proof of work like proof of stake [15], proof of burn [16] and many other algorithms.

2.2 Private blockchain (Permissioned)

This type of blockchain is exclusive to a specific type of people only authorized people who have permission to add or retrieve data and no one outside the authorization cycle may join this cycle, any new user needs prior permission to join the network. The nodes who can participate in the consensus algorithm should be predefined, within this type of blockchain, the peer nodes need to be maintained and operated by the owner of the blockchain or a group of owners who share the managing of the blockchain but are not necessarily trusting each other. One of the algorithms used within the consensus algorithm of the Private blockchain is the Practical Byzantine Tolerance Algorithm (PBFT) [17], such a system can be merged with different techniques related to medicine such as covid-19 tracking [18, 19].

3 Non-fungible token (NFT)

The term NFT refers to any assets that can be owned digitally such as game items, videos, music, and much more this stuff is usually traded online on specific sites using cryptocurrency and proof of the ownership of these items using blockchain technology which is the underlying technology of Bitcoin and another cryptocurrency. A lot of projects come into using metaverse world items that should be digital this is why NFT

became very popular lately and it's market growth up to 41$ billion in 2021 [20]. NFT represent a digital contract that proves the ownership of data it is signed and proven using blockchain technology which cannot be tampered with or modified. NFT has many applications related to healthcare such as supply chain, genetic data, etc. NFT represent the digital certificate for an asset to ensure it is one of a kind and unique and no one owns this item rather than the current owner [21–26]

Using NFT as a medical record involves many challenges such as doctors and laboratory members are not familiar with the key distribution technique and cannot manage it for a huge number of patients and data included within the block and will be available to the doctors. Many technologies can be combined with NFT to improve the metaverse world such as artificial intelligence [21], advanced networks [22], and multimedia applications [23].

4 Shamir's secret sharing

Shamir secret sharing is one of the cryptographic algorithms used to generate unique shares related to specific secrets this is done by dividing the secret using a mathematical way ta o pre-specific number of parts and it is not necessary for reconstructing the secret to have all parts, only a number equal to min required a number of parts needed [27] This is very useful to secure a specific secret if it is needs to send via the communication channel. Equation 1 shows how the secret and shares work

$$f(x) = \mathrm{S} + \mathrm{a}_1 x_1 + \mathrm{a}_2 x_2 \tag{1}$$

Where s is the secret and a_1 and a_2 represent a random number used within the equation. Recalculate the secret of Shamir secret sharing reconstruction using Lagrange as shown in equation 2

$$f(x) = \sum yj \cdot lj(x) = y_0 l_0(x) + y_1 l_1(x) + y_2 l_2(x) \tag{2}$$

Where L is LaGrange [27] , using Shamir secret sharing as the backbone of a consensus algorithm employed in [28].

5 Proposed novel use of NFT for medical information systems

Employing NFT on a customizable blockchain to use as a unique patient medical history that can be accessed by the patient as well as different doctors and sharable between different clinical centers to read and add data to this record which makes the verification of patent history easier, faster and in real-time, using secret sharing method and proof of ownership known as proof of shares as well as encrypt the data within the blockchain with alGamal encryption algorithms. Although the blockchain-based system provides a decentralized system that holds medical records of the patient within the distributed environment the privacy of the user data still be a big challenge to deal with, since the reveal of user data using one of the data mining and data science technologies is not hard and consider a privacy issue. This, adds a new level to increase the security of the system by using an encryption technology named homomorphic encryption that could

apply mathematical operations such as addition or multiplication within the encrypted data without the need to decrypt it, Figure 1 shows the diagram of the proposed system that use NFT as storage of medical records of a single patient., this NFT-ERM consist of many phases, phase 1 is mandatory and phase 2 less frequent than phase one and also mandatory where phase 3 or phase 4 is up to doctor ,medical center, or medical specialist where it is executed reference to the requirement either adding data to patient record NFT-ERM or retrieve history data or both. The details of the four main phase's reference to NFT for electronic medical records (NFT-EMR) are as follows:

Phase 1 shares generation:

Each patient chooses a secret that is unique and unknown to everybody within the process (doctors, laboratory, clinical offices), this secret is used to generate shares using Shamir secret sharing, and these shares are distributed to all nodes within the network using one of the key distributing algorithms, a node represents any medical institute would like to access patient data for add or retrieving data. The secret and the shares can be changed easily since generating and distributing shares are applied within the same procedure. This phase is done less frequently than phase two, since shares and keys can be replaced and changed periodically, and a special key distribution method can be used to distribute these shares.

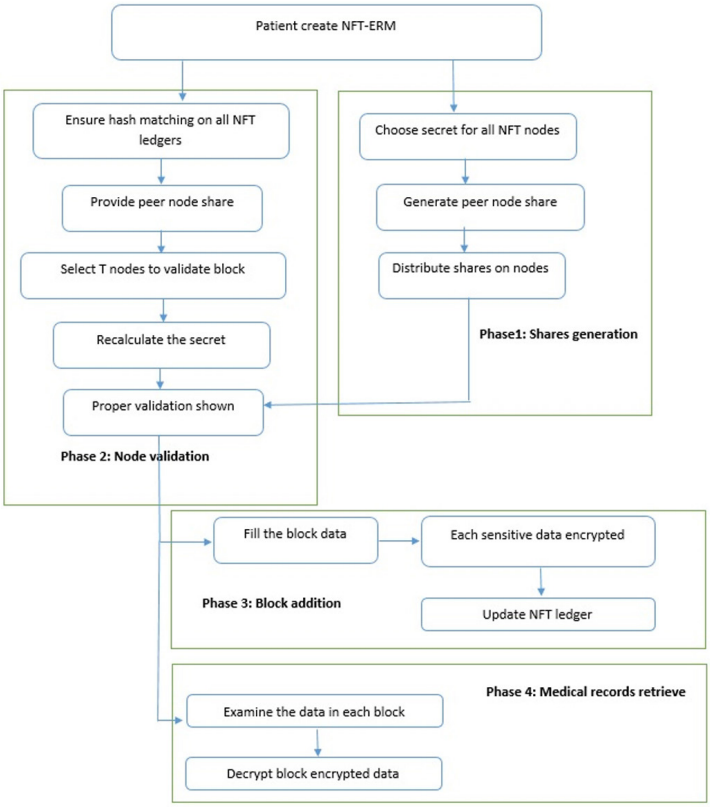

Fig. 1. NFT-EMR system diagram

Phase 2 node validation:

This phase ensures the validation of the node requires adding a new block to the NFT chain or trying to retrieve data from the existing NFT chain, this phase starts by comparing the hashes within the nodes, and when a mismatch occurs this means that the data of distributed ledger are not the same and further investigation required to check the consistency of the ledger data, if all the hashes are identical then the share required from the node used by a medical specialist as NFT-EMR to check the validity of the shares and validate the node within the network, then the user can select N nodes randomly to recalculate the secret and if a match occurs then the node is validated and the NFT-EMR medical specialist can add or read the existing data (either phase 3,4 or both). This node is mandatory each time a medical specialist need to access the NFT of a specific patient, since the operation of keys administration consider difficult for a huge amount of patient each patient can provide his share, and with the help to other centers node verification is done.

Phase 3 block addition:

If the NFT-EMR medical specialist would like to add new medical records related to the patient to the chain after validation the system required data to add to the chain and sensitive data relative to the identity and security of the patient are encrypted. In case of matching then the data need to be added to the chain, and to provide privacy to the data of the patient within the NFT-EMR then proper encryption is done using homomorphic encryption where addition and multiplication can be done on encrypted data, and the data encrypted before addition and decrypted after retrieve. This phase is executed only when a medical specialist would like to add new information to the NFT-ERM.

Phase 4 medical records retrieve:

If the NFT-EMR medical specialist would like to read existing medical records related to the patient from the chain after validation, the system shows data to read from the chain, and the patient's sensitive data are decrypted. The data within the block is encrypted using homomorphic encryption and need to decrypt to retrieve the real values related to the patient. Medical records retrieve: when the medical specialist would like to retrieve information from the NFT-ERM. Algorithm 1 summarizes the proposed system phases, each patient should hold a unique NFT that does not share any secret information with other patients like the first block contain personal information of the patient and each patient have secret that is not sharable with other parties even doctors who should hold a share number of each patient, since every patient can use his share and within help to other medical centers to verify and analysis.

Algorithm 1: NFT-ERM

Input: secret(s), threshold (t), number of shares M
Output: distributed ledger

Phase1: Shares generation using Shamir's secret sharing
Step1: randomly select numbers equal to t-1 if t=3 then two numbers selected k, p
Step2: set a0=s, and select number reference to t, a1=k, and a2=p
Step3: calculate shares using

$$f(x) = S + a1x + a2x2$$

D0=(1, N1) , D1=(2,N2) till Dm=(m,Nm)
Phase2: Node validation
Step4: Ensure hash matching on all NFT ledgers, if a match found go to step 5, otherwise exit()
Step5: Provide peer node share
Step6: Select T nodes to validate the block
Step7: Recalculate the secret of Shamir secret sharing reconstruction using Lagrange

$$f(x) = \sum yj.\ lj(x)$$

$$= y0l0(x) + y1l1(x) + y2l2(x)$$

Step8:if the reconstructed secret match go to step9, otherwise exit ()
Step9: if you would like to add information to user NFT-ERM go to phase 3 otherwise for retrieving NFT-ERM user information go to phase 4
Phase 3: Block addition
Step10: Fill in the block data
Step11: if needed encrypt sensitive data
Step12: Update NFT ledger
Phase 4: Medical records retrieve
Step13: Examine the data in each block
Step14: if needed decrypt encrypted data
Step15: exit()

6 Implementation

Simple implementation of the NFT-ERM system for all the phases, where medical records reference to single patient such as Vermiform appendix surgery and more where sensitive information related to him can be encrypted using homomorphic such as test results numbers and year of surgery.

Phase1: Shares generation this phase required a secret for all NFT nodes and generating shares to every node within the network which is executed such as

- What is your secrets? – 2000
- number of Shares: 5
- 1 2260
- 2 2708
- 3 3344
- 4 4168
- 5 5180

Where using standard Shamir secret sharing require to have a secret which for explaining purposes choose 2000 and number of shares required to derivative from this secret is selected as 5 and then 5 different shared generated and it corresponding share number.

Phase 2: Node validation.

- Previous hash codes matched, this message declares the consistency and match of all hashes within all the connected nodes.
- The available nodes should provide their share to re-compute the secret using the current node that would like to use the system share, Table 1 shows an example of nodes sharing their shares.

Table 1. An example of nodes sharing their shares

Share Number	Share
1	2260
3	3344
5	5180

- Selecting nodes equal to the threshold to regenerate the secret.
- Since the threshold set to 3 then we need three nodes to send their shares and corresponding number and then re-construct the secret and match (let's assume threshold is 3) such as:
  - Share Number – 1
  - Share value – 2260
  - Share Number – 3
  - Share value – 3344
  - Share Number – 5
  - Share value – 5180
  - 94 x + 166 x + 2000
  - Secret = 2000

Phase 3: Block addition data added to the chain as shown in Table 2 and each block can have this fields and more if needed, hash filed represent the hash code of the current block which is calculated using sha-256 and the data filed represent the patient data need to be added to the chain with the previous hash which represent previous block hash.

Table 2. NFT-ERM Block addition data

Block 1
hash: 308918a99ce5b97f86b872b580597bc0e937c7e45ce03bfa793c6c2cef0efb33
data: Vermiform appendix surgery 2003
previous hash: 528050fbf401cf8af5e46df7e110a0a022e1baebb7a9b6b0ea0ab0df7870b8b4
Block 2
hash: 95a68e84c8d4cf9dad6075b77310a9655253b9c071898b4c347fb9731f4ed52a
data: covid-19 2020
previous hash: 528050fbf401cf8af5e46df7e110a0a022e1baebb7a9b6b0ea0ab0df7870b8b4
Block 3
hash: 6bc5cb6345fe83b6162ba77284a11faecd7d8d0b1c06376f07051f87c92f43be
data: critical care unit CCU leak of oxygen due to covid19
previous hash: 528050fbf401cf8af5e46df7e110a0a022e1baebb7a9b6b0ea0ab0df7870b8b4

Phase 4: Medical records retrieve: when the medical specialist would like to retrieve information from the NFT-ERM, the data saved in phase 3 can be retrieved within the same format.

6.1 Evaluations

This system can be compared to the standard ERM systems as shown in table (3) for main characteristics such as:

- Reliability: if the main server down then the data of standard ERM cannot be accessible where in NFT-ERM data can be reached from any node within the network since it is based on distributed ledger
- patient easy access: the data saved within the ERM is exclusive to the clinical center and patient have no control or cannot access the data any time where in NFT-ERM using the distributed ledger the data can be accessed anytime and anywhere
- Security: the NFT-ERM is more secure than standard ERM since it is based on blockchain technology which provide high level of security.
- Privacy: the NFT-ERM having privacy like standard ERM since it is used homomorphic encryption technology which provide privacy to user data, and since it is used for IoT then only sensitive data will be encrypted.
- Immutability: NFT-ERM data cannot be modified since it added to the chain where in ERM it can be modify.
- Interoperability: the data of the patient exclusively owned by the medical center who provide the ERM where in NFT-ERM any medical specialist can access the data via the ledger.
- Monitoring: NFT-ERM can connect to any IoT device and record reading and ERM can connect to them but action daily monitoring cannot implemented in NFT-ERM since it is mainly designed to hold the medical history of patient.
- Scalability: the blockchain provide ability for high scalability and NFT-ERM based in lightweight blockchain technology which provide ability to scalability more.

Table 3. An evaluation of NFT-ERM and standard ERM

Characteristic	NFT-ERM	Standard ERM
reliability	More	Less
patient easy access	More	Less
security	More	Less
privacy	Accepted	accepted
Interoperability	Yes	No
Monitoring	less	More
scalability	more	less

7 Conclusions

Design of NFT-EM where each patient has his medical record that can be shared with other medical centers and specialists as well as using it to have medical advice online or via the metaverse world, the validation of the system is done via a secret shared between parties and reconstruction of the secret to insure authorization, further match is done to match the hashes of each node participating validation of the added block. Such a chain must be a private blockchain and no need for peer nodes within the NFT-EM to compete with each other to update the chain, a customizable blockchain is presented where the standard blockchain technology is modified to adjust the chain to meet the NFT-EM requirements.

8 References

[1] M. A. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," *Technology Innovation Management Review*, vol. 7, no. 10, 2017. https://doi.org/10.22215/timreview/1111

[2] D. Lefeuvre *et al.*, "Quality Comparison of Electronic Versus Paper Death Certificates in France, 2010," *Population Health Metrics*, vol. 12, no. 1, pp. 1–8, 2014. https://doi.org/10.1186/1478-7954-12-3

[3] M. Vukoli, "Rethinking Permissioned Blockchains [C]," in *ACM Workshop*. *ACM*, 2017. https://doi.org/10.1145/3055518.3055526

[4] J. Adamu, R. Hamzah, and M. M. Rosli, "Security Issues and Framework of Electronic Medical Record: A Review," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 565–572, 2020. https://doi.org/10.11591/eei.v9i2.2064

[5] T. A. Jaber and M. A. Hussein, "Study on known models of NB-IoT Applications in Iraqi environments," in *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 518, no. 5: IOP Publishing, p. 052013. https://doi.org/10.1088/1757-899X/518/5/052013

[6] T. A. Jaber, "Artificial Intelligence in Computer Networks," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 1, pp. 309–322, 2022. https://doi.org/10.21533/pen.v10i1.2616

[7] T. A. Jaber, "Security Risks of the Metaverse World," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 13, 2022. https://doi.org/10.3991/ijim.v16i13.33187

[8] S. Nakamoto and A. Bitcoin, "A Peer-to-Peer Electronic Cash System," *Bitcoin*, vol. 4, p. 2, 2008. https://bitcoin.org/bitcoin.pdf

[9] N. K. Tran and M. A. Babar, "Anatomy, concept, and design space of blockchain networks," in *2020 IEEE International Conference on Software Architecture (ICSA)*, 2020: IEEE, pp. 125–134. https://doi.org/10.1109/ICSA47634.2020.00020

[10] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[11] H. T. Salim and H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[12] D. Guegan, "Public Blockchain Versus Private Blockhain," 2017.

[13] J. Q. Kadhim and I. A. Aljazaery, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 01, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[14] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 3–16, 2016. https://doi.org/10.1145/2976749.2978341

[15] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data privacy management*, *cryptocurrencies and blockchain technology*: Springer, 2017, pp. 297–315. https://doi.org/10.1007/978-3-319-67816-0_17

[16] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-burn," in *International conference on financial cryptography and data security*, 2020: Springer, pp. 523–540. https://doi.org/10.1007/978-3-030-51280-4_28

[17] J. Polge, J. Robert, and Y. Le Traon, "Permissioned Blockchain Frameworks in the Industry: A Comparison," *Ict Express*, vol. 7, no. 2, pp. 229–233, 2021. https://doi.org/10.1016/j.icte.2020.09.002

[18] N. A. jassim and H. Salim, "Design and Implementation of Smart City Applications Based on the Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 13, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[19] A. A. Hussain, O. Bouachir, F. Al-Turjman, and M. Aloqaily, "AI Techniques for COVID-19," *IEEE access*, vol. 8, pp. 128776–128795, 2020. https://doi.org/10.1109/ACCESS.2020.3007939

[20] M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the NFT Revolution: Market Trends, Trade Networks, and Visual Features," *Scientific Reports*, vol. 11, no. 1, pp. 1–11, 2021. https://doi.org/10.1038/s41598-021-00053-8

[21] N. Alseelawi and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[22] I. A. Aljazaery and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[23] S. H. Abbood, and M. S. Rahim , "DR-LL Gan: Diabetic Retinopathy Lesions Synthesis using Generative Adversarial Network," *International Journal of Online and Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28005

[24] A. F. Al-zubidi, N. F. AL-Bakri, R. K. Hasoun, and S. H. Hashim, "Mobile Application to Detect Covid-19 Pandemic by Using Classification Techniques: Proposed System," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24195

[25] H. T. Hazim and H. Alrikabi, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[26] K. Vijayalakshmi, S. N. Bushra, N. Subramanian, and V. Ponnuramu, "Blockchain based Medical Record Storage and Retrieval using NFT Tracking System," in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2022: IEEE, pp. 01–08. https://doi.org/10.1109/ICOEI53556.2022.9776833

[27] Pang, Liao-Jun, and Yu-Min Wang. "A New (t, n) Multi-secret Sharing Scheme Based on Shamir's Secret Sharing." *Applied Mathematics and Computation*, vol. 167, no. 2, pp. 840–848, 2005. https://doi.org/10.1016/j.amc.2004.06.120

[28] Mohammed, M. A., and H. A. Wahab, "Proposed New Blockchain Consensus Algorithm," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no.20, pp. 162–176, 2022. https://doi.org/10.3991/ijim.v16i20.35549

9 Authors

Mohanad A. Mohammed, received the BSc and MSc degrees in Computer Sciences in 2007 and 2015, respectively from the University of Technology. He worked within the private sector in a field related to cyber security as well as artificial intelligence. He published many articles on information security and communications. His search interests are Mobile networks, cyber security, and cloud computing. Current Ph.D. student in Department Computer Sciences, University of Technology, Baghdad, Iraq (Department Computer Sciences, University of Technology, Baghdad, Iraq) (email: Mohanad_ali1986@yhaoo.com).

Hala B. Abdul Wahab, a Reviewer (R) of IEEE since 2010. Was born in Basra, Iraq in 1969. She received a B.S. Degree in 1990 in computer science, from Basra University, and M.Sc. degree in 2001 in computer science, from Technology University, and a Ph.D. degree in 2006 in computer science security from the department of computer science, University of Technology, Baghdad, Iraq. She received a professor's degree in 2018 from the University of Technology. From 1991 to 1995, Dr. Hala was a lecturer assistant in the computer science department at Basra University, Iraq. From 1995 to 2020, she was a lecturer in the computer science department at the Technology University, Iraq. Author of more than 65 articles. And her research interests include Information and Network Security. Prof. Hala is a co-author of the "PGP Protocols and its Applications" book in IN TECH 2012. (Department of Computer Sciences, University of Technology, Baghdad, Iraq) (email:110005@uotechnology.edu.iq).

Article submitted 2022-12-21. Resubmitted 2023-01-24. Final acceptance 2023-01-24. Final version published as submitted by the authors.