A Novel Approach to Create a Secure Robust Blockchain Architecture using Lightweight Encryption Model for e-Healthcare Records

[1]Chandini A.G, [2]P.I Basarkod

[1]Assistant Professor, [2]Professor,
[1]Eelctronics and Communication,
[1]Reserch Scholar REVA University & Asst.Professor SJCIT, Chickballapura, India

***Abstract*: Data leakage in electronic health records could result in the compromise of patient privacy. Generally, data in EHRs remain unchanged once they are uploaded to the decentralized system, and thus, blockchain can be potentially used to facilitate the sharing of medical data. Different participating medical organizations and individuals can then access Electronic Health Records (EHRs) stored on the blockchain with a higher level of confidence. To develop a scalable lightweight framework based on blockchain technology to ensure data security, patient privacy, scalability, and integrity of the E-healthcare data. The sensitive data to be stored are hashed using the Enhanced Merkle tree (EMT) data structure to provide a digital fingerprint and the hashed values are stored in the blockchain. Encryption of sensitive data is highly important to ensure data privacy for the patients. In this work, an efficient lightweight fast and ideal lattice-based cryptography with Homomorphic Proxy Re-Encryption scheme is utilized to encrypt the sensitive data prior to storing it in the blockchain. Here a blockchain based searchable encryption scheme for EHRs is proposed. The index for EHRs is constructed through complex logic expressions and stored in the blockchain, so that a data user can utilize the expressions to search the index. As only the index is migrated to the blockchain to facilitate propagation, the data owners have full control over who can see their EHRs data. The use of blockchain technology ensures the integrity, anti-tampering, traceability of EHRs' index. Finally, the performance of the proposed scheme is evaluated, and the Proof of Work (PoW) consensus mechanism is followed to authenticate the new changes that are requested to be made to the data by different stakeholders.**

***Index Terms:* Blockchain technology, lightweight encryption, Electronic Health Record, Ethereum.**

I. INTRODUCTION

Block-chain technology has emerged as a key technology recently in the digital revolution of the healthcare sector and several research studies have identified blockchain potential for the healthcare ecosystem. It is ready to transform the way traditional medical systems and businesses have been engaged in the healthcare sector for the last several decades.

Information and Communication Technologies (ICTs) and blockchain are key enabling technologies for the decentralization and digitalization of healthcare institutions and provides modern and digitalized healthcare ecosystem to patients as well as service providers.In these applications, real-time updates to an encrypted, decentralized block-chain ledger are done to understand, monitor, and control medical information.

The Internet of Medical Things (IoMT) is an incorporation of medical devices and applications that are associated via networks. IoMT acts an important role in enhancing the health and giving medical facilities to the people all around the world [1, 2]. IoMT has the huge influence in daily life due to the exponential growth of IoMT. The health data of the patients are observed remotely and transferred to third party for a future use [3, 4]. The IoMT is a group of devices associated to the internet to get a health-related services [5]. Huge amount of sensitive health data in IoMT is needs to be secured. The major common issue of IoMT facing currently is privacy vulnerability and security [6, 7].

The common IoMT structure comprised of three layers are network layer, perception layer and application layer. Perception layer performs the operation of assembling health information with various devices. Network layer is utilized to collect the input data from the perception layer and transferred to the application layer. The application layer incorporates the medical data and solves the user demand [8].

IoMT is the future source of medical healthcare frameworks, where each medical system is joined and screened over the internet through healthcare professionals [9]. This provides the enhanced health care in lowest cost. IoMT is an incorporation of medical things with IoT [10]. In IoMT, different encryption approaches are used to provide the security [11, 12]. Currently, the available existing machine learning approaches are not providing better security due to the growth of IoMT. They need further enhancement to provide better security [13]. Blockchain has a broad range of applications and a great attention in the healthcare area. The blockchain concept is used to ensure the security, trust, and integrity in data transmission [14]. In an IoMT healthcare system, main objective is to secure the distributed data over an organization which is controlled by blockchain.

Healthcare is comprised of various entities like healthcare providers, patients, medical data, and treatment details [15]. Moreover, Blockchain is a simple data structure provides unchangeable and irremovable transactions by generating a digital ledger. Currently, blockchain concept is attracted by the researchers due to of their various features [16]. Blockchain stores the data without any alteration of unauthorized users. This is important one for securing the sensitive health information of patients. Moreover, Blockchain is the solution for securing patient sensitive health data in IoMT [17].

II. Related Work

Bakhtawar Aslam et al. [21] introduced a blockchain and ANFIS combined IoMT for providing privacy on medical data. The combination of approaches improves the performance on data privacy. The introduced data protection is enhanced by the presented approach, and it was compared with different existing machine learning based approaches. However, the data encryption can be improved further by using different improved encryption approaches to attain good data security.

Roseline Oluwaseun Ogundokun et al. [22] introduced a crypto-stegno approach to provide security on medical data. The performance of the proposed security scheme was compared with existing schemes to validate the performance evaluation. The introduced encryption framework provides the data security in IoMT. However, the developed approach was lack in providing data security. Moreover, it can be improved by providing better data security approaches.

Aqsa Mohiyuddin et al. [23] developed a secured data storage using ANFIS framework. The introduced network provides the improved data security and evaluates the level of security. The proposed methodology enhances the data security and provides the secure data transmission. The security performance of the developed approach attains improved data security than the different existing approaches. Moreover, the security can be improved further using improved data encryption scheme.

Aitizaz Ali et al. [24] introduced a deep learning based homomorphic data encryption approach for keyword search in blockchain. The developed approach improves the data security in patient health records. The process of key encryption allows the users to access the data securely. The proposed approach attains the higher efficiency and security. The performance of data security needs to be improved further by using improved encryption schemes.

Izhar AhmedKhan et al. [25] introduced an effective model named as XSRU (simple recurrent unit)-IoMT. Bidirectional simple recurrent unit was using the criteria of skip connections to solve the gradient issue and attains the data security in IoMT. The developed model was effective in predicting the cyber threats in IoMT and providing better data security. This work provided a security among the health records by using machine and deep learning approaches. However, the security on sensitive health record was still in need. Therefore, innovative encryption approach was needed for a better data security.

The Electronic Health Record (EHR) systems are victimized with several security issues and are compromised in terms of data integrity and management. To provide a solution to this problem, Shahnaz et al. [26] introduced a framework based on blockchain technology. In that work, the blockchain was initially implemented for EHR and then secure storage for the EHRs was provided based on granular access rules for the users. One of the advantages of that method was that the scalability issue of the blockchain was reduced using off-chain storage of the records.

Another approach based on blockchain technology was put forth by Abunadi and Kumar [27] for secure and effective storage of EHRs. The medical information obtained for the doctors, insurance agents and patients were protected by meeting the security needs for even the third parties.

III. Motivation and Problem Statement

The medical area is becoming the fastest one by using the IoMT. With the prompt increase and diversity of IoMT nature, security is becoming a major problem. The health data preserved in IoMT needs better security in case of accessing the data by the users. Blockchain provides the assurance for information security and privacy in IoMT. The integration of blockchain with IoMT provides a decentralized form to maintain the growth of IoMT devices. The blockchain based data encryption approach guarantees the security of patient sensitive health information.

Blockchain is introduced as the best security framework in IoMT due to its distributed and high consistent nature. It provides better security of data access by the unauthorized users. In the blockchain concept, once the distributed ledger is updated, then it cannot be eliminated. Henceforth, recent cryptographic approaches using the blocks across the blockchain to preserve the data.

This makes the blockchain to achieve more security for exploitation in IoMT systems. Different blockchain based data security schemes are introduced by the researchers in the existing works. Still, the communication overhead, computational complexity and privacy needs more attention by using improved form of blockchain approach. Another challenge of using blockchain is storing health records in blockchain. The size of total blockchain is incredible and it is complicated one to handle the large data. Blockchain uses the hash values for the data instead of saving entire data. To overcome all this security related issues, an effective blockchain based data encryption in IoMT is proposed in this work.

IV. Objective

1. To develop a scalable lightweight framework based on blockchain technology to ensure data security, patient privacy, scalability, and integrity of the E-healthcare data.
2. The sensitive data to be stored are hashed using the *Enhanced Merkle tree (EMT)* data structure to provide a digital fingerprint and the hashed values are stored in the blockchain.
3. Encryption of sensitive data is highly important to ensure data privacy for the patients. In this work, an efficient lightweight fast and ideal *lattice-based cryptography with Homomorphic Proxy Re-Encryption scheme* is utilized to encrypt the sensitive data prior to storing it in the blockchain.

V. Implementation

To design a role-based permissioned access control model for blockchain-IoT architecture to be used in EHR systems. To design a lightweight encryption model such as attribute based signature or re-encryption (also called revocation attribute based lightweight signature) (and/or homomorphic to implement the proposed blockchain architecture with decentralized ledger strategically interfaced with decentralized storage systems such as the Interplanetary File Systems (IPFS), Web3 (Web3 (or Ethereum Swarm, native base layer service of the Ethereum Web3 stack)) for higher scalability and interoperability. To simulate the overall proposed blockchain-IoT system with IoT signifying nodes or users with distinct roles and access-level.

To implement overall proposed blockchain-based EHR/PHR solution with faultless Smart Contract enabled Ethereum service or blockchain platform, and examine performance in terms of security, interoperability, scalability etc.

Block diagram of the Proposed System

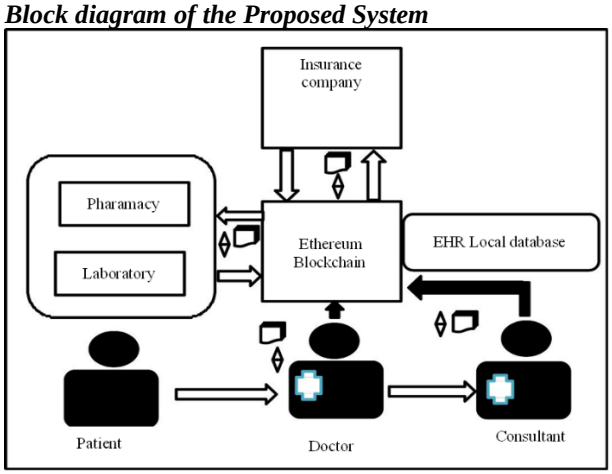

Fig. 1. Proposed block diagram

Figure 1 shows the medical prescription handling process by eliminating the long waiting time process, removing the fraud element from the system, and reducing the error rate made by doctor misinterpretations. A doctor writes a prescription for the patient and puts it to the patient's healthcare records via a smart contract.

The pharmacy then accesses this prescription through the smart contract on the Ethereum blockchain via permission granted by primary doctor and a patient. After accessing the prescription, pharmacy then issues the medicine along its expiry date and dosage use posted on to the patient healthcare records via smart contracts and then the medicine is ready for the collection by the patient. The smart contract features generally organize medicine satisfaction. By allowing patient's medical records to be posted on healthcare blockchain, a patient avoids having to carry the results of the laboratory on their own or arrange for records to be faxed to different care providers. He also ensures that all his health care providers have the necessary information to provide the best possible care. Laboratories reduce the regulatory expenses of printing and mail or fax each test result to singular suppliers.

Furthermore, labs and patients access the healthcare blockchain, where they may get installments from protection firms that counsel the transferred information to process claims or from pharmaceutical organizations that select the information for use in contemplates. Specialists and emergency clinics get access to brought together restorative information on their patients at no cost, decreasing authoritative work and costs.

Initially, a health system framework is developed in the proposed work which is patient centric, and the patients are offered with entire control over their health records. The proposed health system framework is built on a distributed ledger and the health records of the patients are stored in the IPFS.

In the proposed health system framework, the historic health records of the patient are stored in different formats with the execution of smart contracts. The ledger creates the smart contracts for decentralized applications by modelling the blockchain. After defining the framework, the health records of the patients are hashed using the Enhanced Merkle Tree (EMT) data structure and the hash values are preserved in the blockchain. The health records are not directly stored in the blockchain instead, it is preserved in the IPFS in an encrypted form. The main reason behind this is to enhance the scalability and efficiency of the blockchain.

The original data is then preserved in the off-chain framework inside the IPFS. To preserve the data, it is initially encrypted. For data encryption, the proposed work utilizes an efficient lightweight public key encryption algorithm known as ideal lattice-based cryptography with Homomorphic Proxy Re-Encryption scheme which is robust to different attacks. This algorithm is capable of translating the ciphertexts of a particular encryption key to another encryption key thereby avoiding the necessity of completely revealing the data to the potential users. This algorithm functions by generating an encryption key with trapdoor at the initial stage and then the decryption key with re-encryption key is generated through trapdoor sampling. After encryption, the cipher text is then uploaded to the IPFS. For every change made to the data, new hash values are generated, and the smart contract is executed. Finally, the proof of work (PoW) consensus mechanism is followed to authenticate the new changes that are requested to be made to the data by different stakeholders. Building contracts to contain record ownership metadata, permissions, and data integrity. The system's blockchain transactions carry cryptographically signed instructions for managing these properties. State-transition functions of the contract carry out policies, only by legitimate transactions enforcing data alternation. These regulations can be structured to enforce any set of rules regulating a specific medical record as long as it can be computationally represented. For example, a policy may impose sending separate consent transactions from both patients and healthcare professionals before granting a third-party viewing permission. The designed a system based on blockchain smart contracts for complex healthcare workflows. Smart contracts have been designed for different medical workflows and then managing data access permission between different entities in the healthcare ecosystem.

RESULTS

The entire implementations of the work are carried out in the Python platform.

The major performance metrics such as encryption time, decryption time, key generation time, uploading time, downloading time, processing time, latency, etc. are computed and compared with the recent techniques related to blockchain based security enhancement for e-health data.

Dataset for the experiment was taken from data. World - https://data.world/datasets/health -

Data is from the COVID-19 California State Dashboard at https://covid19.ca.gov/state-dashboard/

date	area	area_type	populatio	cases	cumulative_cases	deaths	cumulative_deaths	total_tests
01-02-2020	Alameda	County	1685886	3	3	0	0	4
02-02-2020	Alameda	County	1685886	0	3	0	0	1
03-02-2020	Alameda	County	1685886	0	3	0	0	0
04-02-2020	Alameda	County	1685886	0	3	0	0	0
05-02-2020	Alameda	County	1685886	0	3	0	0	1
06-02-2020	Alameda	County	1685886	0	3	0	0	0
07-02-2020	Alameda	County	1685886	0	3	0	0	0
08-02-2020	Alameda	County	1685886	0	3	0	0	0
09-02-2020	Alameda	County	1685886	1	4	0	0	1
10-02-2020	Alameda	County	1685886	0	4	0	0	0
11-02-2020	Alameda	County	1685886	0	4	0	0	0
12-02-2020	Alameda	County	1685886	0	4	0	0	0
13-02-2020	Alameda	County	1685886	0	4	0	0	0
14-02-2020	Alameda	County	1685886	0	4	0	0	2
15-02-2020	Alameda	County	1685886	1	5	0	0	0
16-02-2020	Alameda	County	1685886	0	5	0	0	0
17-02-2020	Alameda	County	1685886	1	6	0	0	0
18-02-2020	Alameda	County	1685886	0	6	0	0	0
19-02-2020	Alameda	County	1685886	0	6	0	0	0
20-02-2020	Alameda	County	1685886	1	7	0	0	0

Fig 2: Dataset of COVID-19 20-22

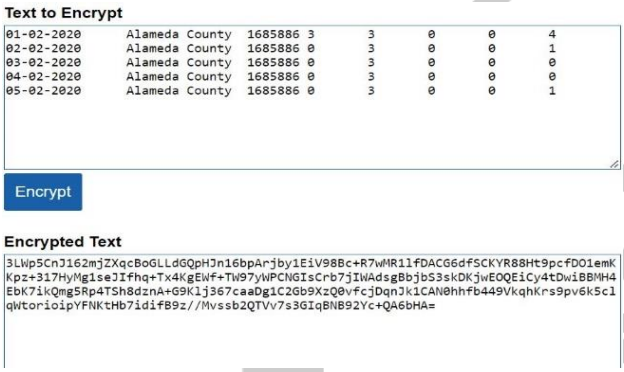

Fig 3: Encrypted Dataset

Datasets of COVID-19 is considered for evaluation. Dataset of three years from 2020 to 2022 is considered such that death rates were less (data considered where date rate was less).

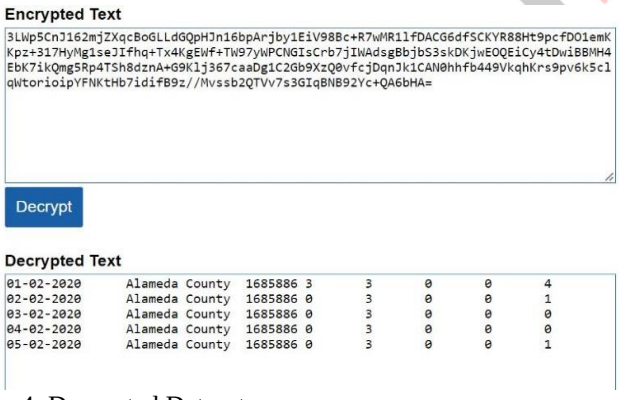

Fig 4: Decrypted Dataset

Dataset considered is first encrypted and decrypted and hashed with Enhanced Merkle Tree algorithm with minimal time, and that data is applied for lattice-based cryptography with Homomorphic Proxy Re-Encryption scheme in further extended work.

CONCLUSION

The very nature of a decentralized ledger makes them immune to a cyber-crime, as all the copies stored across the network need to be attacked at the same time for the attack to be successful. The simultaneous (peer-to-peer) sharing and updating of records make the whole process much faster, more effective, and cheaper.

In terms of Security: Data privacy is also importance because secure patient data has financial as well as legal implications as well as in Infrastructure: Sharing data require a centralized data source which increases the security risk and requires trust to a single centralized authority.

The main intention of the proposed work is to develop a scalable lightweight framework based on blockchain technology to ensure data security, patient privacy, scalability and integrity of the E-healthcare data. Initially, the private health data to be stored are hashed with the help of ***Enhanced Merkle tree (EMT)*** data structure. To improve the security, the hash values are encrypted by using an efficient lightweight public key encryption algorithm termed as ***lattice-based cryptography with Homomorphic Proxy Re-Encryption scheme.*** After the completion of encryption process, the secured information is uploaded to the IPFS. For every change made to the data, new hash values are generated, and the smart contract is executed. Finally, the ***proof of work (PoW)*** consensus mechanism is followed to authenticate the new changes that are requested to be made to the data by different stakeholders with is enabled in further extended research.

VI. ACKNOWLEDGMENT

My completion of this Research work could not have been accomplished without the support of my Ph.D. Guide, Dr P.I Basarkod, Reva University and HOD Dr B.N Shobha, SJC Institute of Technology, Chickballapura.

Thank you for allowing me time away from you to research and write. Thanks to my parents Dr Uma B Gopal, Late K. Gopalakrishna and Husband Mr. Prabhu Kumar A, Mother-in-law, and child. The countless times you kept the children during our hectic schedules will not be forgotten.

Finally, my deepest gratitude to my Friends and colleagues. Your encouragement when the times got rough are much appreciated and noted. It was a great comfort and relief to know that you were willing to provide management of our household activities while I completed my work.

My heartfelt thanks.

REFERENCES

[1] Usak, M., Kubiatko, M., Shabbir, M. S., Viktorovna Dudnik, O., Jermsittiparsert, K., & Rajabion, L. (2020). Health care service delivery based on the Internet of things: A systematic and comprehensive study. International Journal of Communication Systems, 33(2), e4179.

[2] Makkar, S., Singh, A. K., & Mohapatra, S. (2020). Challenges and opportunities of Internet of Things for health care. In A Handbook of Internet of Things in Biomedical and Cyber Physical System (pp. 301-314). Springer, Cham.

[3] Al-Turjman, F., Nawaz, M. H., & Ulusar, U. D. (2020). Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. Computer Communications, 150, 644-660.

[4] Parah, S. A., Kaw, J. A., Bellavista, P., Loan, N. A., Bhat, G. M., Muhammad, K., & de Albuquerque, V. H. C. (2020). Efficient security and authentication for edge-based internet of medical things. IEEE Internet of Things Journal, 8(21), 15652-15662.

[5] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2020). A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies, e4049.

[6] Girardi, F., De Gennaro, G., Colizzi, L., & Convertini, N. (2020). Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain. Electronics, 9(6), 884.

[7] Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. Internet of Things, 8, 100123.

[8] Aileni, R. M., & Suciu, G. (2020). IoMT: A blockchain perspective. In Decentralised Internet of Things (pp. 199-215). Springer, Cham.

[9] Yaacoub, J. P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 105, 581-606.

[10] Din, I. U., Almogren, A., Guizani, M., & Zuair, M. (2019). A decade of Internet of Things: Analysis in the light of healthcare applications. Ieee Access, 7, 89967-89979.

[11] Polu, S. K., & Polu, S. K. (2019). IoMT based smart health care monitoring system. International Journal for Innovative Research in Science & Technology, 5(11), 58-64.

[12] Putta, S. R., Abuhussein, A., Alsubaei, F., Shiva, S., & Atiewi, S. (2020). Security benchmarks for wearable medical things: stakeholders-centric approach. In Fourth International Congress on Information and Communication Technology (pp. 405-418). Springer, Singapore.

[13] Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). Security, privacy and trust in iomt enabled smart healthcare system: A systematic review of current and future trends. International Journal of Advanced Computer Science and Applications, 12(2), 731-737.

[14] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.
[15] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3.
[16] Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: securing internet of medical things (IoMT). Int. J. Adv. Comput. Sci. Appl, 10(1), 82-89.
[17] Jan, M. A., Cai, J., Gao, X. C., Khan, F., Mastorakis, S., Usman, M., & Watters, P. (2021). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. Journal of Network and Computer Applications, 175, 102918.
[18] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access, 7, 183339-183355.
[19] Avinashiappan, A., & Mayilsamy, B. (2021). Internet of Medical Things: Security Threats, Security Challenges, and Potential Solutions. In Internet of Medical Things (pp. 1-16). Springer, Cham.
[20] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2020). A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies, e4049.
[21] Aslam, B., Javed, A. R., Chakraborty, C., Nebhen, J., Raqib, S., & Rizwan, M. (2021). Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic. Personal and ubiquitous computing, 1-17.
[22] Ogundokun, R. O., Awotunde, J. B., Adeniyi, E. A., & Ayo, F. E. (2021). Crypto-Stegno based model for securing medical information on IOMT platform. Multimedia tools and applications, 80(21), 31705-31727.
[23] Mohiyuddin, A., Javed, A. R., Chakraborty, C., Rizwan, M., Shabbir, M., & Nebhen, J. (2021). Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. International Journal of Fuzzy Systems, 1-13.
[24] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. Sensors, 22(2), 528.
[25] Khan, I. A., Moustafa, N., Razzak, I., Tanveer, M., Pi, D., Pan, Y., & Ali, B. S. (2022). XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. Future Generation Computer Systems, 127, 181-193.
[26] Shahnaz, Ayesha, Usman Qamar, and Ayesha Khalid. "Using blockchain for electronic health records." IEEE Access 7 (2019): 147782-147795.
[27] Abunadi, Ibrahim, and Ramasamy Lakshmana Kumar. "BSF-EHR: blockchain security framework for electronic health records of patients." Sensors 21, no. 8 (2021): 2865.