BLOCKCHAIN AND LIGHTWEIGHT CRYPTOGRAPHY TECHNIQUES IN ELECTRONIC HEALTHCARE SYSTEM: A LITERATURE REVIEW

*Vandana V** [1], *Dr. S Veni* [2]

ABSTRACT

In the present era, healthcare sector is undergoing a significant transformation by embracing innovative advancements and adjusting to the changing landscape of digital technologies and global transitions. This transition is altering methods through which healthcare services are provided and received, leading to a fundamental change in industry. An essential element in healthcare is guaranteeing optimal security for sensitive patient information, which is crucial for upholding patient confidentiality & privacy. The integration of blockchain technology in conjunction with lightweight cryptography has attracted considerable attention for its potential to improve data security through decentralization and encryption mechanisms. By employing blockchain technology, Electronic Health Systems (EHS) improve patient data integrity & confidentiality, which facilitates sharing of medical information in Electronic Health Records (EHR) via online platforms. This sharing may encompass data from various sources like Internet of Things (IoT) devices as well as applications for mobile health. In instances where resources are scarce, such as in high-level cryptography scenarios, encrypting patient data can present challenges. Yet, lightweight cryptography methods present a more viable option for effectively safeguarding patient information. The primary aim of this review literature is to underscore significant function & effect of blockchain technology in EHR. Additionally, article intends to investigate application of lightweight cryptographic techniques such as EDSCA with SHA-256, utilization of blockchain technology in EHR systems, together with identification of potential research needs.

Department of Computer Science[1],
Karpagam Academy of Higher Education, Coimbatore, India[1]
vandanavijayan7@gmail.com
Department of Computer Science[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
venikarthik04@gmail.com

* Corresponding Author

Keywords: Blockchain, Lightweight cryptographic techniques, Elecronic Medical Record, SHA- 256, EDSCA, Smart Contract, Securiy, Privacy

I. INTRODUCTION

The global community is currently witnessing a noteworthy surge in volume of patients seeking medical attention, while simultaneously facing difficulties in ensuring an adequate supply of primary care physicians, healthcare providers, & medical personnel. This escalating situation poses a considerable challenge in maintaining sufficient healthcare services to address increasing requirements of general population. The capacity to manage substantial volumes of data rapidly has been enhanced by smart technology, which helps with disease diagnosis and identification. By employing blockchain technology, both patients and healthcare professionals can enjoy enhanced efficiency in data management. Blockchain serves as a decentralized and openly accessible digital registry that securely logs transactions across numerous computers, guaranteeingthe integrity of past records by preventing alterations without affecting subsequent blocks. Blockchain technology is currently utilized in the medical & biological domains. The integration of blockchain with the Lightweight Cryptographic techniques holds promise in guaranteeing the reliability of data. Lightweight cryptography refers to an encryption method that consumes fewer resources in terms of memory, power, and computation while providing secure solutions for resource-limited devices. Blockchain technology has been applied to address challenges faced by resource-constrained nodes, such as IoT sensors, which have restricted processing capabilities & energy resources. The design of lightweight cryptography emphasizes simplicity and a minimal footprint while maintaining an adequate level of security. Compared to conventional cryptography, it is anticipated to be more efficient and straightforward, though potentially less secure

EHR encompass patients' medical histories in a digital format, are stored by hospitals or clinicians indefinitely, providing a wide range of information like MRI reports, past exams, vaccinations, test results, and allergies, accessible only to authorized users for patient & healthcare provider use. Electronic health records, or EHRs, offer a straightforward way to store medical records and make it easier to access patients' traditional paper medical records electronically. Using this method, patients can help their family members, medical professionals, & additional authorized information consumers oversee, generate, regulate, & disseminate EHRs. When a patient has the ability to handle their electronic health records, health departments can derive substantial benefits, particularly when the patient seeks care at an alternative facility, other doctor may not have to redetermine the patient's previous health status.

To protect patient data, an effective access control protocol is necessary. Unauthorized individuals attempting to access the information would require the appropriate encryption key, which they do not possess. Furthermore, numerous efforts are underway to develop new technologies and methods for creating more environmentally friendly communication networks. The approach also addresses the need for reduced energy consumption. The implementation of an economical consensus mechanism for block addition can reduce overhead and promote information exchange.

The primary contributions of research is to implement secure and privacy of blockchain using lightweight cryptography in electronic health records. In this approach SHA-256 & EDSCA is used to integrate blockchain. In blockchain- electronic health record (EHR) systems, SHA-256 serves an essential function in preserving data integrity & avoiding modifications. This algorithm generates a unique hash for each patient record, enabling detection of any unauthorized changes or tampering attempts.

The ECDSA algorithm serves two primary functions in these systems: verifying the authenticity of transactions and controlling user access. By employing lightweight digital signatures, ECDSA facilitates efficient authentication and data verification processes without imposing significant computational demands. Collectively, these encryption methods offer a robust, effective, & adaptable approach to safeguarding the confidentiality & authenticity of confidential medical information within a distributed ledger-based EHR framework.2. Literature Review

R.Sangeetha, B.Harshini, A.shanmu gapriya[9],The authors proposed the SHA-256 algorithm, utilized to encrypt all patient data into a singular A 256-bit encrypted string that will be included in block on Etherscan.

Ibrahim Adunadi, Ramaswamy Lakshmana Kumar[4], proposed blockchain security framework for effective & secure storage of EHRs. Patients have free access to EHRs & thorough, consistent records because to this approach. Here merklee tree hasing algorithm for connecting the former blocks.

A new block cipher method was proposed by Ravi Raushan Kumar Chaudhary & Kakali Chatterjee [1] for safe transfer of data from Internet of Things devices. Lightweight cryptography techniques are appropriate for IoT devices. The suggested technique relies on straightforward operations like as XORing, swapping, & splitting.

Hong Jiao wu,Ashutosh Dhar Dwicedi,Gautan Srivastava[14], suggested a blockchain-based approach to safeguard medical system privacy data, and through simulation experiments, demonstrated the method's superiority regarding the efficiency of information transmission and storage, as well as functioning of security controls. Security issues include key being unintentionally revealed during transmission. In order to protect user privacy, paper's internal storage information is stored using elliptic curve diffie-hellman key exchange.

Sobia Yaqoob,Muhammad Murad khan[16], Analyzed the primary issues presented by various healthcare stakeholders & explored the facets of blockchain technology that may mitigate those concerns.

According to authors, the suggested system has limitations that could be subject of further study.

Akifa Abbas, Rabia Aslam Khan, Hafiz Burhan UI Haq, Ahmed Naeem Akhtar[15], recommended using a robust encryption system that patients and medical professionals can both use efficiently. In EHRs, blockchain technology is

the most popular encryption method. Blockchain ensures EHRs and protects patient privacy through decentralization, cryptography, and hashing. The application and difficulties revealed a healthcare weakness or gap in BC.

Sandeep Saxena, Namita Arya, Sunil Kumar Bharti[2], Propose a straightforward & efficient blockchain-based system for e-healthcare to resolve these issues, together with lightweight & effective protocol for processing e-healthcare information via blockchain technology. Through a mechanism of reduced key complexity, protocol guarantees privacy of all entities. We follow data access rules & utilize symmetric encryption techniques to ensure recipient's or user's information security.

R. P.Puneeth, G. Parthasarathy[3],proposed Authorized data storage and transmission was formed by integrating blockchain function with the proposed IDSE (Intuitionistic Derivative Symmetrical Encryption) algorithm-based security mechanism. Reducing amount of encrypted data & enabling high-speed data transmission, key pattern extraction model based on Differential Hashing Patterns (DHP) was employed for key pattern generation.

Martin Parmar, Parth Shah[5], constructed a diverse IoT block chain system using both constrained & unconstrained nodes, including Raspberry Pis & a PC with enough processing power. The IBLWC approach was proposed by the authors. According to performance analysis, implementation of recommended strategy yields minimal average CPU utilization & latency during mining activities. To validate transactions, process can be optimized by augmenting number of blockchain network miners' nodes for enabling greater parallel processing.

III. RESEARCH METHODOLOGY

In e-healthcare systems, ensuring integrity, security, as well as confidentiality of data is paramount. The decentralized nature of block chain technology presents a promising approach to tackle these issues. This methodology examines how SHA- 256 cryptographic hash function & ECDSA (Elliptic Curve Digital Signature Algorithm) can be utilized to secure information within a block chain-based e- healthcare framework, together with the execution of smart contracts to automate procedures like patient consent & access control.

3.1 Blockchain Technology in E-Healthcare

Blockchain technology has garnered lot of interest because of its potential for securely managing & storing EHRs. It provides a decentralized, transparent, and unchangeable record that guarantees patient data is fluently auditable and cannot be altered. Within the domain of e-healthcare, where data security and sequestration are crucial, blockchain is especially helpful. The medical field continues to be among majority prominent research domains in recent decades, with researchers constantly coming up with new & more dependable ways to support healthcare industry & community. various parties involved, including medical professionals, doctors, hospitals, patients, and others must safely, interoperable, & unaltered organize, access, & distribute health records. To demonstrate the authenticity of records, data provenance is also crucial. Blockchain is utilized in various contexts & possesses the ability to address primary challenges confronting healthcare sector. Nonetheless, to actualize real-time uses of this technology, additional targeted study is necessary.

3.2 Blockchain Ownership

Basically, two primary categories of blockchain: permissioned & permissionless. A permissioned blockchain is one that had been specifically designed by one or more authorities. The verification procedure may be conducted by a central authority or a consortium of trustworthy, pre-selected entities. Data access had been limited to authorized user group or coalition of blockchain-governing entities in this private setting. Efficiency & scalability are enhanced by a reduced number of players [18] [12]. Ultimately, these blockchains possess central authority. Because a 51 percent majority is needed to reach a consensus and it is simple to do so in this controlled environment, setup's centralization may allow for tampering [7]. Examples include Hyperledger, Ripple, and Eris [6]. Permissionless blockchains are inefficient & fully dispersed across numerous nodes [6]. People who utilize these blockchains are not required to obtain prior authorization in order to mine transaction blocks. For network tasks, anyone can donate their

processing power and receive payment in exchange. This blockchain is also referred to as a public blockchain because it allows general public to view & publish publicly visible transactions [18] [12]. Ethereum and Bitcoin are two instances of permission less block chains [8][16][11].

3.3 Features of Blockchain technology

a) Decentralization: The blockchain, distributed digital database, consists of many blocks that encompass transactions. Each network node possesses access to & usage of decentralized database. Because blockchain-based networks use end-to-end replications, they do not require a single point of failure, providing fault-tolerant design.

b) Immutability: The immutability of the blockchain makes it a permanent and unalterable network. A network of nodes is used by blockchain technology to function. A transaction cannot be changed or deleted after it has been recorded in blockchain. Because blockchain records are unchangeable & impenetrable, offering high level of security & confidence.

c) Consensus Mechanism: The consensus feature of any blockchain facilitates the network's ability to make prompt, objective judgments. A consensus method is used to make decisions so that the group of active nodes on the network may come to a conclusion more quickly & efficiently & ensure that system functions flawlessly . Nodes may not trust each other, but they may trust algorithm that makes decisions at center of network. Many consensus algorithms are available, each with advantages and disadvantages. A consensus mechanism is essential to any blockchain; without it, its value will be diminished.

d) Smart Contract: A set of terms or preprogrammed computer logic had been referred to as smart contract. Once encoded logic has been fulfilled, it automatically initiates transactions between parties. The blockchain is programmable and adaptable as a result of this implementation [6], [19], [13]. In order to facilitate management & administration, smart contracts are programmed [10]. Supply chains, insurance claims, and clinical trials can all use smart contracts [10]. To get certain results, clinical studies often involve a series of dependent stages. After network nodes reach an agreement, a smart contract that encodes each phase can be activated [23], [22]. Therefore, smart contracts may fully govern related processes while enforcing transparency and traceability.

3.4 SHA-256's function in block chain technology

The cryptographic hash function SHA-256 produces 256-bit hash result from supplied data. In blockchain systems, it is especially important or guarantee immutability & integrity of data kept in the blocks. There are various applications for SHA-256 in the e-healthcare system.

i. Hashing Data: Every piece of healthcare data (e.g., patient health records, prescriptions, diagnostic reports) is hashed using SHA-256 before being kept in blockchain. Procedure insures how any alteration to original data will produce an entirely distinct hash, hence indicating any attempts at tampering [11].

ii. Block Generation: Every block in blockchain contains hash of preceding block, so connecting them into an unalterable chain. SHA-256 is employed in Proof of Work (PoW) consensus process, which miners use to validate blocks by solving complex mathematical puzzles[11]. Assuring blockchain's integrity & legitimacy.

iii. Secure Hashing in Smart Contracts: Smart contracts, which automate processes like patient consent and record access, also rely on SHA-256 for securely verifying conditions and transactions.When a patient gives consent to a healthcare provider to access their records, SHA-256 hash of consent agreement is created & recorded on blockchain for subsequent verification.

3.5 Procedure for Carrying Out SHA-256 Hashing:

This phrase suggests the steps involved in using the SHA-256 algorithm to convert data into a fixed-size string of bytes.

I. Preparation of Data: Medical records by approved healthcare providers, information such as patient ID, medical history, and prescriptions are gathered. The information is formatted to meet the blockchain network's requirements for structure.

II. To generate a distinct hash for each piece of data, SHA-256 method is utilized. The blockchain ledger is then where the hash is kept.

III. Verification: When accessing a patient's record, system rehashes data retrieved as well as compares same with blockchain's hash. When hashes are identical, there has been no alteration to the data.

3.6 ECDSA's role in blockchain.

1. Digital Signatures for Transaction Validation: When submitting new medical records, requesting access to patient data or authorizing a prescription, healthcare providers, patients, & administrators use ECDSA to sign their transactions. The private key generates digital signature that verifies sender's identity & assures message doesn't change while being transmitted.

2. Access Control in Smart Contracts: e-healthcare system, smart contracts might made to grant access to medical records only after the patient's or authorized personnel's digital signature has been validated using ECDSA. This guarantees that sensitive health data can only be accessed or modified by authorized parties.

3.7 Techniques for ECDSA Implementation.

i. Key Generation: Each participant utilized elliptic curve cryptography producing pair of public & private keys (healthcare provider, patient). While public key is distributed to authorized parties, private key is kept confidential.

ii. Generation of Digital Signatures: When a party must authorize transaction permission to view documents, they generate a digital signature for the transaction utilizing their private key.

iii. Signature Verification: Participants confirm legitimacy of signature, utilizing sender's public key subsequent to transaction being disseminated to the blockchain network. The transaction is approved if signature is authentic; else, it is denied.

iv. Smart Contract Execution: After a legitimate signature has been confirmed, smart contracts carry out predetermined actions, like allowing access to records or starting a new healthcare service.

4. Smart Contract Integration with E- Healthcare Blockchain.

Blockchain technology has been applied through mechanisms referred to smart contracts. Self-executing agreements in blockchain network have been called smart contracts[11] where terms are encoded directly into code. Smart contracts are essential for automating a number of tasks in the e- healthcare system, including such.

i. Patient Consent: The process of getting and documenting patient consent to access or share their health data can be automated with smart contracts. The smart contract ensures that request is documented in blockchain that right people have access after patient digitally signs the consent using ECDSA.

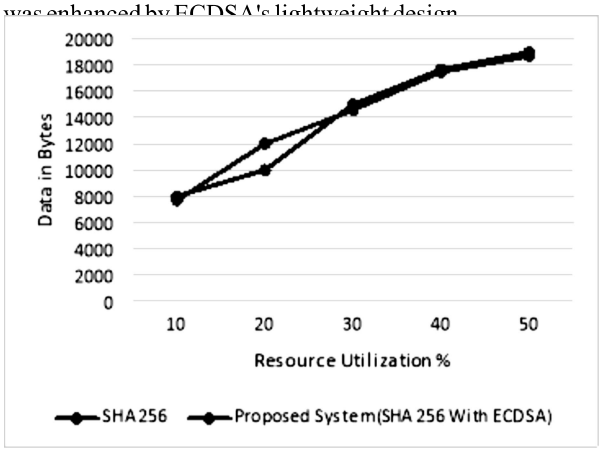
ii. Data Access Control: By enforcing stringent access control policies, a smart contract can grant patients or authorized healthcare provider's access to specific sections of their medical records based on predetermined criteria, like role or time-based limitations.

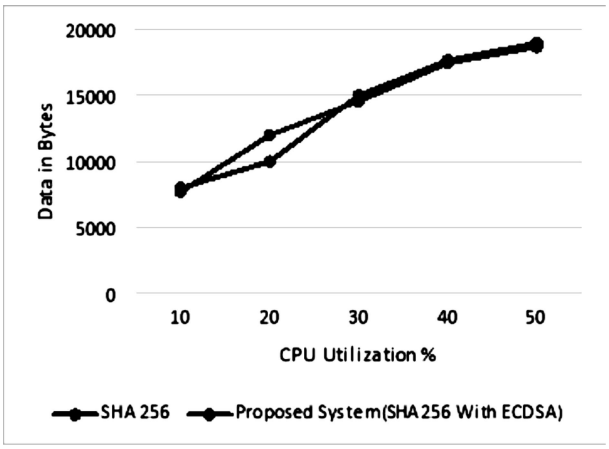
IV. RESULT AND DISCUSSION

Data integrity is guaranteed by the SHA-256 algorithm, which creates distinct and unchangeable hash values for every transaction or record. Any change to data results in

modifications to hash, which is easily detectable. Transactions were secured on two levels by combining SHA-256 hashing with ECDSA digital signing.

A completely transparent & traceable system for handling healthcare interactions was made possible by built-in features of blockchain technology, in addition to SHA-256 & ECDSA. Thus, proposed system shows, resource usage—in particular, CPU utilization—stayed within reasonable bounds. The overall effectiveness of the system was enhanced by ECDSA's lightweight design.





V. CONCLUSION AND FUTURE SCOPE

Integrating SHA-256 & ECDSA algorithms into blockchain-based e-healthcare systems has been shown to be a very successful way to guarantee data security, transparency, and integrity. The o utcomes show how they could be used to address important issues in themanagement of healthcare data. Further study & optimization are necessary to address concerns with scalability, energy efficiency, and regulatory compliance. Future research should concentrate on integrating blockchain technology with cutting- edge cryptographic methods and investigat ing hybrid models to improve system performance & flexibility in practical situations. Address regulatory issues while maintaining fundamental advantages of blockchain technology by implementing off-chain storage or zero-knowledge proofs. To guarantee sustainability, future systems should give priority to blockchain designs that use less energy.

REFERENCES

[1] Ravi Raushan Kumar Chaudhary, Kakali Chatterjee.” An Efficient Lightweight Cryptographic Technique for IoT based E- Healthcare System”. In 2020 IEEE 7th International Conference on signal processing and integrated networks(SPIN),978-1-7281-5457-6/20/$31.00@2020 IEEE.

[2] S. Saxena, N. Arya, S. K. Bharti and V. Dwivedi, "A Lightweight and Efficient Scheme for e-Health Care System using Blockchain Technology," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10111937. keywords: {Privacy; Protocols; Information security; Medical services; Information processing; Blockchains; Performance analysis; Health Care; Blockchain technology; Symmetric encryption; Miners; Communication overhead},

[3] R. P. Puneeth, G. Parthasarathy.” Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System”. IJE TRANSACTIONS B: Applications Vol. 36, No. 05, (May 2023) 925-933. doi:10.5829/ije.2023.36.05b.09

[4] Ibrahim Abunadi, Ramaswamy Lakshmana Kumar.” BSF-HER: Blockchain Security Framework for Electronic Health Records for Patients”. Sensors 2021,21,2865. https://doi. org/10.3390/s21082865.

[5] Martin Parmar, Parth Shah." Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application". International Journal of Electrical and Computer Engineering (IJECE), doi:https://10.11591/ijece.v13i4.pp4422-4431

[6] Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564. IEEE, 2017.

[7] Mettler, Matthias. "Blockchain technology in healthcare: The revolution starts here." In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-3. IEEE, 2016

[8] Daniel, Jeff, Arman Sargolzaei, Mohammed Abdelghani, Saman Sargolzaei, and Ben Amaba. "Blockchain Technology, Cognitive Computing, and Healthcare Innovations." Journal of Advances in Information Technology Vol 8, no. 3 (2017)

[9] RSangeetha,B. Harshini, A.Shanmugapriya, T.K.P.Rajagopal." Electronic Health Record System Using Blockchain.". International Research Journal of Multidisciplinary Technovation. ISSN 2582-1040(2019).

[10] Rabah, Kefa. "Challenges & opportunities for blockchain powered healthcare systems: A review." Mara Research Journal of Medicine & Health Sciences-ISSN 2523-5680 1, no. 1 (2017):45-52.

[11] Abhishek Kashyap, Akash Yadav, Vineet Bajaj, Yasim Khan, Sumit Arora, Lalit Maini. "Blockchain Technology in Healthcare: The Idea and What Lies Beyond" .MAMC Journal of Medical Sciences. Volume 8 ¦ Issue 3 ¦ September-December 2022, 45.

[12] Holbl, Marko, Marko Kompara, Aida Kami ¨ sali ˇ c, and Lili Nemec ´ Zlatolas. "A systematic review of the use of blockchain in healthcare." Symmetry 10, no. 10 (2018): 470

[13] Xia, Q. I., Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain." IEEE Access 5 (2017): 14757- 14767.

[14] Hongjiao W U,Ashutosh Dhar Dwivedi,Gautam Srivastav."Security and Privacy of Patient Information in Medical System based on Blockchin Technology",Vol 1,N0.1,Article,2020

[15] Hafiz Burhan Ul Haq, Akifa Abbas, Rabia Aslam Khan ,Ahmed Naeem Akhtar, Waseem Akram, Sabreena Nawaz, Faraz Imllak Mayo and Ahmad Iftikhar Bhatti ." E-Healthcare Using Block Chain Technology and Cryptographic Techniques: A Review".Paksithan Journal of Engineering and Technology,PakJET, ISSN (p): 2664-2042, ISSN (e): 2664-2050 Volume: 5, Number: 4, Pages: 21- 28, Year: 2022, DOI: https://doi.org/10.51846/vol5iss4pp21-28

[16] Sobia Yaqoob, Muhammad Murad Khan, Ramzan Talib, Arslan Dawood Butt, Sohaib Saleem, Fatima Arif, Amna Nadeem." Use of Blockchain in Healthcare: A Systematic Literature Review". (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 10, No. 5, 2019.

[17] A. Dhivya Bharathi P [2] PS. Hari Priya,P [3] PS. Naveen Kumar P [4] PMrs.W. Mercy," Framework of Parallel Healthcare System using SHA Algorithm". IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 8 Issue 3, March 2021 ISSN (Online) 2348 – 7968 | Impact Factor (2020)–6.72

[18] Peters, Gareth W., and Efstathios Panayi. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money." In Banking beyond banks and money, pp. 239-278. Springer, Cham, 2016.

[19] Mamoshina, Polina, Lucy Ojomoko, Yury Yanovich, Alex Ostrovski, Alex Botezatu, Pavel Prikhodko,

Eugene Izumchenko et al. ”Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare.” Oncotarget9, no. 5 (2018): 5665.

[20] Prashant Digambar Hakim, Vinod Moreshwar Vaze. "Blockchain for Secure Medical Records Storage and Medical Service Framework using SHA 256 – Verifiable Key". International journal of Intelligent Engineering and system. doi:https://www.imass.org/.

[21] Ensteih Silvia, Mohd Tajuddin.” E- Health Privacy and Security through ECC, SHA-256, and Multi-Authority Approaches”. JOURNAL OF Information Technology and Cryptography(2024). DOI: https://doi.org/10.48001/JoITC

[22] Griggs, Kristen N., Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, and Thaier Hayajneh. ”Healthcare blockchain system using smart contracts for secure automated remote patient monitoring.” Journal of medical systems 42, no. 7 (2018): 130.

[23] Benchoufi, Mehdi, and Philippe Ravaud. ”Blockchain technology for improving clinical research quality.” Trials 18, no. 1 (2017): 335.

[24] Janardhana Dasarigatta Rangappa1*, A.P. Manu 2, Shivanna Kariyappa3, Suhas Kamshetty Chinnababu4, Gururaj Harinahalli Lokesh5, Francesco Flammini6.” A Lightweight Blockchain to Secure Data Communication in IoT Network on Healthcare System”. International Journal of Safety and Security Engineering Vol. 13, No. 6, December, 2023, pp. 1015-1024 Journal homepage: http://iieta.org/journals/ijsse.