SECURE ELECTRONIC HEALTH RECORD MANAGEMENT WITH BLOCKCHAIN

J Vekatarao[1]
[1]*Dept. of Computer Science and Engineering Sree Vidyanikethan Engineering College*
Tirupati, India venkatrao.j@vidyanikethan.edu

Prathima Chilukuri[2]
[2]Assistant professor, School of computing (IT), Mohan Babu University Tirupati,
Andhra Pradesh,prathima.ch@vidyanikethan.edu, Orchid id: 0000-0002-2468-6305

Putta Vishnu Vardhan[3]**, Pasam Dwarakamayee**[4]**, Neelam Vijayalakshmi**[5]
Dept. of Computer Science and Engineering,Sree Vidyanikethan Engineering College
Tirupati, India
421pvv@gmail.com ,vijayaneelam6669@gmail.com , dwaraka.pasam@gmail.com

Abstract— Patient health records that are stored digitally on a network are known as electronic health records (EHRs). EHRs provide several chances to enhance clinical practice performance metrics, patient care, and upcoming medical study. In the current era of smart suburbs, the techniques employed to stock EHRs have proven quite defenseless. Data breaches by hackers and other parties are simple to accomplish. Moreover, neither patients nor healthcare professionals have access to the information. These methods are incapable of balancing data security with data accessibility. However, blockchain technology could be able to overcome these problems. Blockchain establishes an immutable ledger system that allows for transactions to occur in a decentralized way. The essential properties of blockchain technology namely transparency, decentralization, and security enable any software program produced with it safe and inaccessible to unauthorized parties. Data tampering is nearly difficult on a blockchain network. In this work, we demonstrate a framework for implementing EHRs employing blockchain technology, with the goal of making EHRs safer and more private. Using cryptographic methods and decentralization, blockchain technology will keep command of information access. Moreover, it preserves the delicate balance between data accessibility and data privacy. The primary goal of this work is to frame security and data privacy challenges in E-healthcare**.**

Keywords— Blockchain, Decentralization, Privacy, EHRs, Hyperledger, Security

I. INTRODUCTION

There are numerous facets of human life that have been impacted by the progress in technology during the past several decades. It was helpful for numerous facets of our lives, including healthcare. The healthcare industry has made significant progress in recent years. These days, our medical records could be kept online. Clinicians were able to diagnose patients more accurately, patient-physician communication improved, and In an emergency, patients might call doctors immediately [1]. Patients might reach doctors in different locations because of computerized records. Yet, along with the benefits of contemporary technology, there were also downsides to this innovation. By giving hackers greater hacking tools to access and change documents, information technology's significant advancements have benefited hackers. As a result, the danger to the safety of patient privacy and medical information is rising right now [2]. In this research, we suggest a solution to protect the electronic health records and preserve patient's privacy from attacks.

Digital documents called “electronic health records” (EHRs) includes the patient's medical background. A hospital or a practitioner maintains electronic medical records throughout time by storing them digitally on an electronic media [3]. Electronic medical records include every relevant piece of clinical data that is important to a patient's care that is documented with a particular healthcare professional, such as MRI reports, records of prior physical tests, and vaccinations. It is straightforward for a doctor or a patient to access the records and they are only available to people who have been given permission. These can be forwarded with certain other care professionals from many health care organizations for improved healthcare. It enhances the typical storage techniques of medical data on paper, that are prone numerous dangers such as natural catastrophes, theft, war, illegal modification, and so on. With EHRs, information may be accessed automatically, possibly improving the clinician's productivity. An overview of EHR is given in Fig. 1.

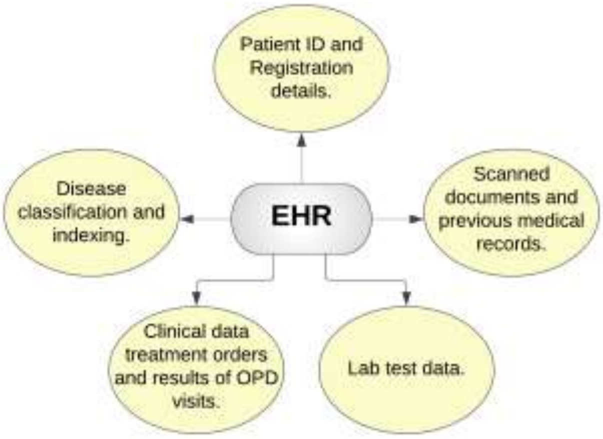
Patient ID and Registration details.
Disease classification and indexing.
EHR
Scanned documents and previous medical records.
Clinical data treatment orders and results of OPD visits.
Lab test data.

Fig. 1. Overview of an Electronic Health Record

The development of healthcare is greatly aided by EHRs. They have increased the quality and accessibility of health information by reducing record errors. They also help patients make better decisions by allowing them to access medical information at any point of time. This decreases the potential of repeating testing, delaying treatment, and making patients more aware [4]. EHRs have enabled doctors and patients to engage instantly whenever required, which has reinforced their relationship. They have boosted patient engagement and improved care coordination. Medical professionals may take judgements that are quicker and more accurate, and treat sick people as fast as it is practical since the data is readily available.

Yet, with the development of IT, the digital information became prone to attacks from unauthorised users. These criminals access patient records and personal information using modern software including hacking tools, alter the information to exploit it for personal advantage or to hurt patients. As a result, there is an urgent necessity to securely keep patients' private details and medical data and protect them [5]. Nowadays, the cloud-based method EHR storing is not very safe and can be accessed by experienced hackers [6]. In order to appropriately secure health information and safeguard their privacy from unauthorised users, there has been a growing demand in recent years. Employing a blockchain-based approach for EHRs is a practical way to store records securely over a network.

II. Related Work

Yeah et al [7] .'s investigation of user privacy in relation to blockchain technology for healthcare intelligence. They developed healthcare data gateway, together with a “data access control” for privacy. PSN-based healthcare was proposed by Zhang et al. [8] as a way of secured application, and two protocols were developed for the sharing and authentication of healthcare data. Xia et al. [9] demonstrated the “Medshare system” for managing security of access to health information using cloud-based services and a blockchain-based method. A blockchain-based mobile medical information sharing system was developed by Liang et al. [10], who also provided a safe “user-centric” approach to privacy and access control via a “channel construction” mechanism. A blockchain-based system for exchanging medical data was proposed by Jiang et al. [11], which also developed on-chain and off-chain verification for the system’s storage security. Data security solutions in healthcare industry were examined by Li et al. [12], who also offered memory management strategies to aid data management. In order to promote data security and privacy inside the system, Fan et al. [13] proposed blockchain-based patient medical information. An attribute-based encryption strategy was proposed by Wang and Song [14] for a secure health information sharing system. To ensure the accuracy and traceability of medical records, “smart contracts” were used. Blockchain was employed by Guo et al. [15] to provide a multi-user attribute-based signature approach for EHR management. They used a decentralised approach for more privacy in their attribute-based mathematical formulation in an effort to boost system security.

III. Methodology

A. Blockchain

This distributed ledger system is capable of efficiently logging transactions involving two parties. Each transaction is documented on a record, known as a block, which is then connected to other blocks using cryptography to generate a collection or a blockchain. The decentralised transaction can help with data management as well. Each block in a blockchain network consists of a timestamp, the preceding block's hash, a cryptographic hash, and transaction information. It is created in a way that makes it difficult to modify. To carry out secure network transactions, blockchain is employed. There has been a boom in research in blockchain technology and its possible uses since the technology was first developed in 2008. Due to its absence of centralised authority, which offers data integrity, transparency, and security without intervention from the third-party organisation overseeing the transactions, and as a result, its expanding popularity, it generates encouraging chances for conducting studies in several fields [16].

Any data altered later needs the change of all preceding blocks since the blockchain is a decentralised, “distributed ledger system” which might preserve transactions across multiple computers. This enables blockchain members to independently and reasonably authenticate transactions. The blockchain database is created on its own utilizing a “peer-to-peer network”. The vast majority of the network's consensus verifies their authenticity. It is designed in this manner to allow robust workflow. Its usage also avoids the issue of “double-spending”. This technology has properties such as transparency, decentralization, and security [17]. This enables it stand out as cutting-edge technology for efficiently and safely completing transaction processes.

B. Consensus Algorithm

Each block uploaded to the blockchain must be approved by all other nodes already enrolled on the network. To finish this task, a consensus mechanism is employed. They support the growth of network reliability and participant trust. PoS, PBFT, and PoW are common consensus algorithms [18].

C. Data Privacy in Blockchain

By the use of encryption, blockchain enables network security. A blockchain connects every block to the one before and the one following it. So, it is tough for a hacker to fiddle any record since, in a large network with a lot of blocks in a blockchain, doing so would require altering the blocks or records that are connected to the record that the hacker wants to alter or access.

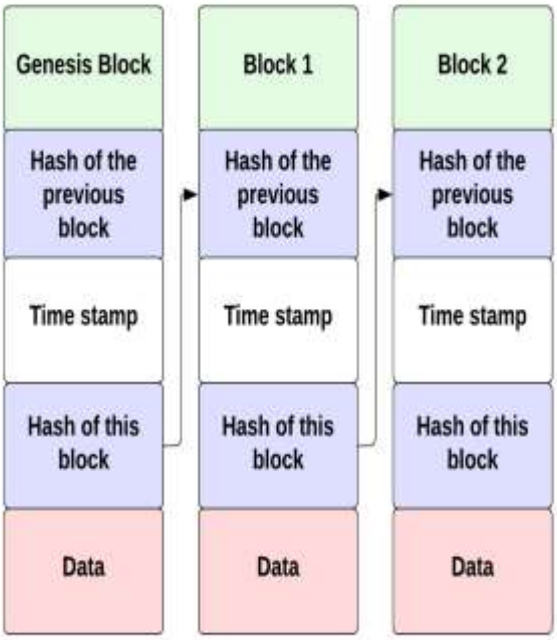

Fig. 2. Structure of a Blockchain

As shown in Fig. 2, the genesis block is the first block in any blockchain, and it acts as the base upon which other blocks are stacked chronologically. A date, a nonce, preceding block’s hash, and transaction data make up a blockchain block. They are utilized to create the hash of the given block employing “cryptographic methods”. Blocks on the blockchain have unique identities called hashes. These Hash pointers are also in charge of connecting a block to the past block by storing the previous block’s hash. Due to the relationship between each block and the one before it, the blockchain becomes immutable.

D. Decentralization in Blockchaim

As blockchains are decentralised networks, no one person or entity has control over the whole network. The blockchain network is not managed by a centralised system. Although every network node has a mirrored version of the ledger, only the network as a whole is able to make modifications to the ledger. The other network nodes that make up the network must concur before any transaction can be completed or changes to the data can be made. This attribute makes networks more secure.

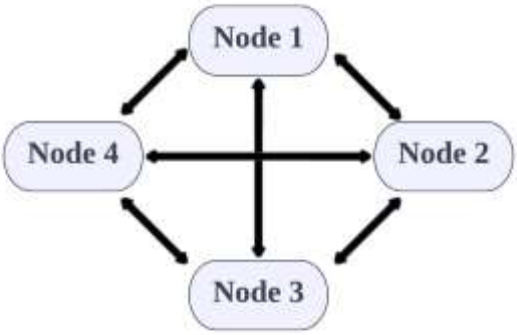

Fig. 3. Peer to Peer model Representation

As shown in Fig. 3, it uses a “peer-to-peer model” to enable communication between two network users without the use of an intermediary or third party. It uses a peer-to-peer protocol, which denotes that every member of the network has an exact copy of every transaction, allowing for consensus method sanctioning. Over the entire procedure, there are no delays or extra costs. To undertake any network activity, approval from each and every registered node in the network is required. If the database or central ledger in a centralized network is targeted by hackers, the entire system is damaged. A decentralized network, on the other hand, eliminates this problem because there is no one point of storage.

E. Transparency in Blockchain

Although a user's personal information is kept private on the blockchain, it is essentially an open source technology, allowing individuals on the network to change the code as they see fit, till the majority of the network's members agree. Because the blockchain network has hundreds of thousands of users, it is not likely that someone can make changes without being recognized.

F. Blockchain implementation of EHRs

Blockchain is already used by many hospitals and clinics to securely store their patients' health information. A personal health information may be developed, tested, and then added to blockchain network, giving them complete guarantee that the information can’t be changed. These personalised medical data will be encrypted and kept on the blockchain network employing a “private key”, safeguarding the patient's privacy and limiting access of medical information to just authorized users when it matters most.

G. System Design and Architecture

Transactions, Assets, and Participants are the three main components of the blockchain network. EHR system is comprised of three main actors in this blockchain-based implementation:

- Patients
- Doctors
- Laboratories
- Admins

Being a participant in the EHR system, patients have a big part to play. These individuals are the proprietors of the blockchain-produced and-stored health records. People have the option to amend their personal data. Individuals are able to control who gets access to their papers as a consequence. Patients restrict access to their data by any unapproved healthcare professional or third party.

Doctors are the healthcare professionals who will diagnose patients and obtain medical information from them. If a patient has verified them as their authorised physician and given them permission to write into their record, they are exclusively in charge of updating material in their records that is health-related.

It is the responsibility of laboratories to conduct tests, provide test findings, and update this data in the health records of patients who gave them authorization to write into their records.

The admin is in responsible of setting up the blockchain network, carrying out numerous network contracts, producing the key, and managing transaction data encryption and decryption.

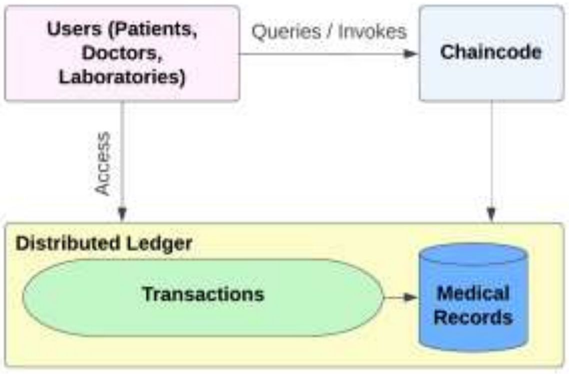

Fig. 4. Blockchain EHR system architecture

Fig. 4 shows the system architecture. In this system, the network's asset is medical records. A patient who is a part of the network is the owner of each medical record. A transaction results in a change in the asset's value. Updates include prescription adjustments, test results, document updates unless the patient is given a new diagnosis, and so forth.

Transactions are operations that are primarily performed on network assets. Examples include creating a medical record, granting clinician or lab access, updating the participant's information, adding a participant to the network, and removing access from those entities. A few of these transactions can only be carried out if the two participating nodes have a relationship. For instance, the doctor who has to access a patient's clinical information, the patient's identification needs to be included within the directory that contains the doctor's patients. Basically, the individual whose health information needs viewing has to be one of the patients of doctor who requests access to those information. The authorisation rules are likewise set forth by this system. These guidelines specify which participants have entry to which resources and in what ways. Controlling accessibility to every system resource is aided by this. Some records can only be changed or seen by authorised users.

The transactions taking place in the system are:

- **CreateMedicalRecord -** This transaction produces network records. It includes information such as labs, list of permitted patients, owner, and recordID. It includes areas for storing patient medical information such as allergies, date of consultation, last consultation with which doctor, medical history, any dangerous behaviors, and so on. It is possible to identify a particular record in a collection using the record ID that was established, which is specific to that record.
- **GrantAccess –** For the change in records, the medical professional must have access to the record. The medical record may only be accessed, read, and written to by the authorized doctor. To grant this access, this transaction is utilised.
- **GrantAccessToLab -** If the labs wish to change the record, they must also have access to it.
- **RevokeAccess -** After the necessity of accessing a record has been met, the clinician's access to the particular record is revoked. The record cannot be reviewed or altered by the clinician anymore.
- **RevokeAccessFromLab -** Once the task is completed, access to the labs is likewise removed.
- **AddParticipant -** A new node is introduced to the system by running this transaction.
- **UpdateParticipant -** This happens whenever the participant's node's data is altered.
- **UpdateAsset -** This happens when the information in the health records are changed.

IV. SYSTEM IMPLEMENTATION

We utilised the Composer tool and the blockchain-based Hyperledger Fabric architecture to create this system.

A. Hyperledger Fabric

It is a Hyperledger project and an implementation of the blockchain technology created by the Linux Foundation. This framework is utilised because it enables plug-and-play compatibility for elements like consensus and membership services. It enables smart contracts, sometimes referred to as "chaincode," which make up the system's logic, to be hosted using container technology [19].

B. Hyperledger Composer

It is a set of open source tools for creating a “blockchain-based business network”. It assists developers and company owners in the creation of many smart contracts and blockchain apps for the purpose of solving various business difficulties.

C. Steps taken to build this blockchain-based EHR network

- **Data collection:** Patient's personal information and health information including allergies, dangerous habits, lab results, medicines, and data created by the doctor's clinical diagnosis.
- **Wallet allocation:** This is a space reserved for the deployment of our blockchain network. That is where all transactions are kept track of.
- **Setting up a blockchain network using Composer and Hyperledger Fabric:** We develop our business network and deploy our blockchain network on composer playground after wallet allocation.
- **Development of various nodes in the system:** The node designs for various participants are included into a model of our system in our blockchain network, including patients, doctors, and labs.
- **Creating Medical Records:** Furthermore, we provide a framework for storing health data held by patients.
- **Transaction creation:** We design the necessary transactions following the requirement, such as authorising or disabling access from medical professionals and specifying the approved medical professionals.
- **Node addition to the system:** With the provided sample data, an instance of the Medical record node, Lab node, Clinician node, and Patient node owned by a patient was generated. Before being joined to the network, nodes are confirmed by other nodes already registered there, and a public identification is created.
- **Definition of various user permissions:** This section outlines the system resources a given participant may access. Access to certain medical record data is restricted to individuals with specified rights.
- **Transaction execution:** Different transactions are completed fulfilling needs of the user, and The saved collection of records can also be used to retrieve records as needed. An updated health record is made after the execution.

The flowchart of the whole process is given in Fig. 5.

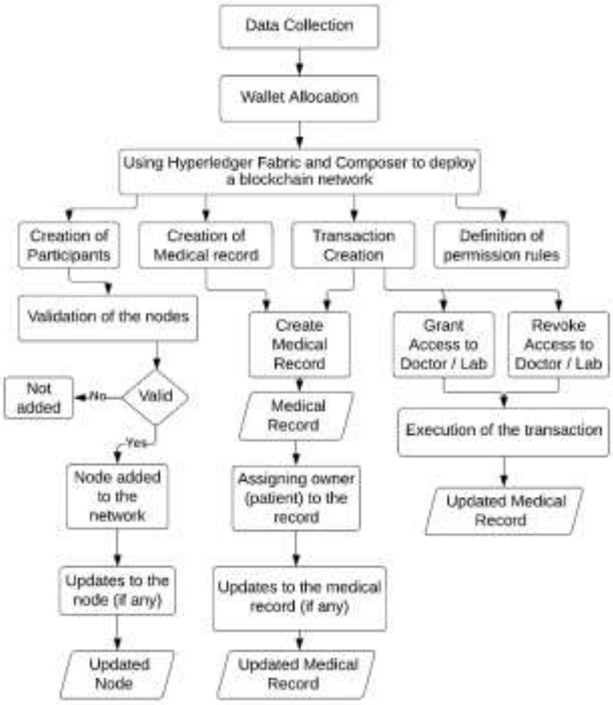
Data Collection
Wallet Allocation
Using Hyperledger Fabric and Composer to deploy a blockchain network
Creation of Participants
Creation of Medical record
Transaction Creation
Definition of permission rules
Validation of the nodes
Create Medical Record
Grant Access to Doctor / Lab
Revoke Access to Doctor / Lab
Not added
No
Valid
Yes
Medical Record
Execution of the transaction
Node added to the network
Assigning owner (patient) to the record
Updated Medical Record
Updates to the node (if any)
Updates to the medical record (if any)
Updated Node
Updated Medical Record

Fig. 5. Flowchart of the implementation

V. Conclusion and Future Scope

We were successful in developing the core network functions and establishing a blockchain-based EHR network. By employing the key components of blockchain, we were able to protect patient privacy and secure EHRs, which was the core aim of our study. In our opinion, blockchain technology is an innovative approach for creating EHRs that holds the means to support medical study and advancement in the near future.

The concept and execution may to eventually be increased by including other smart contracts to handle sophisticated EHR system operations. Billing, transportation, and other areas can be connected to the network to create a whole system for managing healthcare. To enhance its interactivity, you might connect it with a web application. By including pharmacists as an additional user in the system, EHRs may be valuable for tracking drug sales.

References

[1] Liu, S., Wang, H., Gao, B., & Deng, Z. (2022). Doctors' provision of online health consultation service and patient review valence: evidence from a quasi-experiment. *Information & Management*, *59*(5), 103360.

[2] Raghupathi, W., Raghupathi, V., & Saharia, A. (2023). Analyzing Health Data Breaches: A Visual Analytics Approach. *AppliedMath*, *3*(1), 175-199.

[3] Crameri, K. A., Maher, L., Van Dam, P., & Prior, S. (2022). Personal electronic healthcare records: What influences consumers to engage with their clinical data online? A literature review. *Health Information Management Journal*, *51*(1), 3-12.

[4] Evans, R. S. (2016). Electronic health records: then, now, and in the future. *Yearbook of medical informatics*, *25*(S 01), S48-S61.

[5] Wu, Z., Xuan, S., Xie, J., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Computers in biology and medicine*, *147*, 105726.

[6] Rasool, R. U., Ahmad, H. F., Rafique, W., Qayyum, A., & Qadir, J. (2022). Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *Journal of Network and Computer Applications*, 103332.

[7] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*, 1-8.

[8] Zhang, J., Xue, N., & Huang, X. (2016). A secure system for pervasive social network-based healthcare. *Ieee Access*, *4*, 9239-9250.

[9] Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access*, *5*, 14757-14767.

[10] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-5). IEEE.

[11] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a blockchain-based platform for healthcare information exchange. In *2018 ieee international conference on smart computing (smartcomp)* (pp. 49-56). IEEE.

[12] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-based data preservation system for medical data. *Journal of medical systems*, *42*, 1-13.

[13] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, *42*, 1-11.

[14] Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, *42*(8), 152.

[15] Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE access*, *6*, 11676-11686.

[16] Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039.

[17] Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: research and applications*, *3*(2), 100067.

[18] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1545-1550). Ieee.

[19] Sato, T., Shimosawa, T., Kondo, Y., & Nishijima, N. (2023). Toward Fully-Decentralized System With Hyperledger Fabric. *IEICE Communications Express*

[20] NVR Goluguri, Infectious diseases of Rice plants classified using a deep learning-powered Least Squares Support Vector Machine Model ,Indian Journal of Computer Science and Engineering (IJCSE) 13 (5), 1640-1659

[21] L. Vanitha, R. Kavitha, M. Panneerselvam, and G. M. Valantina, "A Novel Deep Learning Method for the Identification and Categorization of Footpath Defects based on Thermography," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1401-1408, doi: 10.1109/ICOSEC54921.2022.9951904.

[22] Muppalaneni, N.B.,. (2021). A Secure Smart Shopping Cart Using RFID Tag in IoT. In: Shakya, S., Balas, V.E., Haoxiang, W., Baig, Z. (eds) Proceedings of International Conference on Sustainable Expert Systems. Lecture Notes in Networks and Systems, vol 176. Springer, Singapore. https://doi.org/10.1007/978-981-33-4355-9_52.

[23] Shaik, A.A.., Muppalaneni, N.B. (2019). A Computational Approach to Predict Diabetic Retinopathy Through Data Analytics. In: Internet of Things and Personalized Healthcare Systems. SpringerBriefs in Applied Sciences and Technology(). Springer, Singapore. https://doi.org/10.1007/978-981-13-0866-6_10.

Arun Kumar, J.R.,Anusuya, R.Ramkumar Prabhu, M.Auto Encoders and Decoders Techniques of Convolutional Neural Network Approach for Image Denoising In Deep Learning,Journal of Pharmaceutical Negative Resultsthis link is disabled, 2022, 13(4), pp. 1036–104.