International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 08, August 2022)

Blockchain Technology for Secure Electronic Health Records in the Healthcare Sector

Shiva Tiwari[1], Prof. Saurabh Sharma[2], Prof. Vishal Paranjape[3], Prof. Saurabh Kapoor[4]
[1,2,3,4]*Global Nature Care Sangathan Group of Institutions, Jabalpur (M.P), India*

Abstract— **Access, data processing, monitoring, and healthcare are all areas where global health systems are changing significantly. By 2020, it's anticipated that linked and data-capturing equipment will have produced around 2314 exabytes of health care data[1]. Cybercriminals work very hard to get access to medical information. The cybersecurity market is predicted to reach $27.1 billion in 2026 as a result of this challenge[2]. A centralised repository for data collection in clinical trials will be aided by blockchain technology. This article proposes a safe approach utilising blockchain to guarantee the security of digital medical records (EHR). Databases, the Internet of Things, sensors, and other computing resources are all part of the architecture. In comparison to the conventional healthcare system, the security and privacy of EHR will be improved by this framework for security.**

Keywords—**EHR, IoT, Blockchain, Cybersecurity**

I. INTRODUCTION

Today across the world, health care industry is undergoing through enormous transformations are taking place in health care. In addition, demographic, economic, social and technological changes are forcing us to reconsider everything about the health care industry. The delivery methods, resource allocation, funding models, scientific innovation, the physician's role are also changing as a result of the transformations. Health care is not only becoming increasingly connected, but data are also becoming increasingly big and complex. The healthcare industry is a data-intensive sector [3] that produces, distributes, sorts and accesses massive data every second. The global health data produced in 2013 are 153 exabytes and by 2020, it is expected to be around 2314 exabytes [4]. Any industry has recently begun to create products for the healthcare industry using the new information and communication technology [4]. Many powerful on-chip connectivity architectures and topologies were built [5, 6] as part of the Internet of Things (IoT)[7,8]. This is also essential in order to shield EHRs from numerous health systems. Patient data is often straightforward but sometimes it's difficult to manage unstructured patient data. This data is generated from various stakeholders and can be accessed or manipulated for efficient use by various stakeholders.

A system may also be built to evaluate and identify health anomalies and to report to healthcare units. This method would then adjust the entire situation in order to make the health system much simpler and more convenient. The EHR includes vast volumes and a wide range of clinical notes, records of patients, laboratory reports, findings fromimaging exams and other studies.

Recently, IoT has shown an important function in patient diagnostics and monitoring. The key benefits this technology is in monitoring of patient condition continuously all the time, which is often difficult to accomplish in the conventional approach. Furthermore, remote accessibility and ongoing theoretical side have demonstrated a variety of options for quicker diagnosis and improved healthcare. Secure and scalable data sharing in the health care sector is critical for the diagnosis and decision- making process [9][10][11][12][13].

The exchange of data is mandatory so that healthcare professionals can transfer records of patient in a way that is secure and acceptable. The data is usually sent either via a "store-and-forward" device or through clinical monitoring in real time. Data security, reliability and privacy are also the most important features to carry out the program due to critical importance of patient records. The implementation of blockchain technology, revolutionary technology recently assumed full regulation of access, transaction and storage.The blockchain can be defined as follows:

Definition – *"*The blockchain framework can be defined as software solutions that simplifies the development and deployment of blockchain applications with little customization [14]".

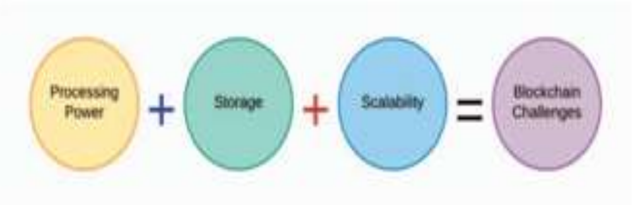

Figure 1: Blockchain computational complexity [14]

The key challenges of any blockchain framework are computing capacity, storage and scalability as shown in Figure 1. The main challenge in EHR is the development of a confidentiality and security scheme, so that many interested parties can access the data. A blockchain platform is also highly appropriate to protect the data of the patient from unauthorized access or use.

A. Stolen Data Business in Healthcare

This is true because privacy and protection are important for EHRs. But what if the information were stolen? This motive for fraud remains uncertain, considering that the stolen health data are lower costs than any financial data. Cyber criminals expend a great deal of time, money and energy on the manipulation and monetization of EHRs [15]. Till now, medicinal and biomedical knowledgebase has been one of the most powerful evidence in rivalry for consumer data against cyber criminals [15]. The healthcare system is currently unprepared for data protection. However, several organizations including the FDA have released the latest recommendations and data protection requirements for medical devices to introduce stringent safety protocols before the release of products.

B. Market Analysis of Cybersecurity

In 2018, the total cybersecurity healthcare market was around US$ 7.66 billion [2]. In the healthcare sector, cybersecurity growth is expected to cross USD 27.10 billion by 2026[2]. This involves robbing EHRs, medical equipment and hospital infrastructure and ransomware attacks. In recent years, almost 66% have registered a ransomware attack, while 45% have encountered data attacks leading to destruction.

In cybersecurity, the ransomware industry dominated with the highest portion of 37.7% [2]. In 2017, Pattern Micro blocked almost 1 trillion ransomware attacks [16]. The Federal Investigative Bureau has warned healthcare industry that hackers have key goals [16]. A health stakeholder study found that 16 percent foresee a blockchain approach in the immediate future, while 56 percent plan to use a blockchain approach by 2020[3].

After the presentation in Section I, we have discussed the state-of-the-art in healthcare systems in Section II. The Section III addresses the proposed framework and its elements. Finally, section IV presents the conclusion.

II. Related Work

A blockchain-based architecture framework was proposed by S. Amofa et al. [17] to secure the control of sharing the patients' personal health-related data by various healthcare service providers.

By creating a method for regulating data, the framework that is being given enables minimal risk to data. The author asserts that the health care provider may guarantee more robust data management security utilising the framework provided than is possible with the current system.

A blockchain and the decentralised Interplanetary File System (IPFS) based on a unique EHRs sharing framework on a mobile cloud platform were proposed by Dinh C. Nguyen [18] et al. The project at hand creates a safe access control system.

Mechanism for patients and healthcare service providers to share EHRs. Authors demonstrated a working prototype that integrates an Amazon cloud computing mobile app with the Ethereum blockchain in a real-world data exchange scenario. The outcome demonstrates that the concept offers a practical and successful approach for dependable and trustworthy data transmission on mobile clouds by protecting sensitive patient health-related data from various dangers.

A secure HER system called MedBloc, introduced by Jack Huang et al. [19], allows patients and healthcare service providers to communicate and access health-related records while maintaining patient privacy. The MedBloc stores patterns of patient health-related data and allows patients to regularly update this data. The access control method imposed by the framework MedBloc is based on smart contracts and employs an encryption mechanism.

According to Ayesha Shahnaz et al. [20], the usage of blockchain technology can successfully revolutionise the EHRs system and offer many solutions for this problem. By adhering to the granular access rules for users of the proposed framework, the authors offered a blockchain-based framework for the healthcare sector for EHR that provides secure and effective storage of patient-related electronic health information. The methodology that is being presented also focuses on the scalability problems that blockchain technology faces. The structure suggested in this study offers an integrated, secure, and scalable blockchain-based solution in addition to a secure EHRs system.

By utilising the special characteristics of Blockchain, Theodouli et al. [21] have suggested an architecture that facilitates the safe sharing that permits the stakeholders. The proposed design encourages the legitimacy of data access, which increases device security. The consensus concept is used in this system to provide an effective and interoperable transactional framework. To improve cooperation among nodes across third-level blockchain networks, the system is designed on a tripartite structure at various levels, including the blockchain framework, application middleware, and smart contracts.

In hospitals and nursing schools, Sivagami et al. [22] have talked about systems that remotely monitor and record patient, staff, and biomedical equipment. The suggested architecture encourages the employment of monolithic network-based RFID, WSN, and Smart Wearables Managed Application Protocol systems. The distribution of patients and smart environmental sensing will be accomplished through the low-power network for the personal area. But the security concern raised by the suggested method is not addressed in this article.

Collaboration between IoT healthcare networks has been suggested by Budida et al. [3] for patient monitoring. The main focus of the suggested architecture is the creation of data from intelligent, energy-efficient biosensors, transmission to microcontrollers, and storage on MYSQL database servers. These primary data and diagnostic information must be tracked, gathered, processed, and recorded using effective solutions for medical professionals and patients everywhere.

The authors of the suggested method, however, did not investigate any security features.

Another healthcare system concept based on the blockchain network paradigm has been put forth by Wang et al. [23] to enhance diagnosis quality and accuracy using artificial systems. In order to deliver a treatment offered by the patient in line with the model, the growing Artificial Health System (AHS) has the ability to create and grasp the complimentary system between real physicians and computer-simulated ones.

An affordable approach for a health sensor network was put up by Raj et al. [24]. The programme includes a new technique for application, online video sharing, messaging, automatic and prescriptions, as well as encrypted messages, medical devices, and remote centres. However, the secure communication mechanism is not discussed by the authors in their study. Regarding the usage of blockchains to store EHR and other medical data, Zainab Alhadhrami et al. [24] explored the topic.

A common and linked jargon system and model for classification in computer education and IBM Cloud Computing for crucial patient safety monitoring have been proposed by Neloy et al. [26]. The Logistic Regression, Naive Bayes, K-NN, and Tree Classification are the four fundamental predictors used in the Machine Learning (ML) architecture for the prediction of patient disorders.

A blockchain-enabled system for the management of medical transactions made with the use of sensors and other connected devices was introduced by Dey et al. [27]. The proposed framework avoids problems associated with the traditional IoT approach, such as high-cost server equipment and single points of failure.

III. Proposed Framework

This suggested framework is built on wearable medical device collecting, blockchain technology, Internet of Things, and data archiving. The safe healthcare system can be built utilising blockchain technology, as demonstrated in Figure 2. The patient's attached sensors can gather information from the body and send it immediately to the cloud or, if the patient is in the hospital, via mobile phones. The communication channel receives the encrypted data, which is then transferred to the blockchain by the cloud [28][29][30][31].

Although intended for patient records, EHRs also have use in the pharmaceutical, medical imaging, and insurance industries. Before being stored on the blockchain network, this data is processed by an EHR both locally and in the cloud. The peer nodes in this network process data in the blockchain network and communicate data across wireless communication channels [15]. We will go over a number of the proposed framework's components in the part after that.

1) A means of communication

EHR cloud and LPWAN gateway provide substantial processing power to support stakeholder decision-making. The communication channel's primary goal is to deliver data more quickly to the communication network so that the IoT device's functionality can be verified [14]. The local nodes that are responsible for storing the data sent via the data recording devices may be deployed [14].

The records acquired from the logger are encrypted to maintain system confidentiality. A certifying agency can help with the distribution of the keys. The complete node can use the local node to solve the LPWAN challenge or conduct a PoW transaction [28][14][31].

2) Cloud technology Infrastructue

The healthcare system, professionals, clinics, and patients all rely on cloud computing (CC) to get data that is linked to the blockchain network. Virtualization, encryption, decryption, and online services are the main uses for CC systems [14]. The management and storage of various keys within the cloud infrastructure is handled by key management software. Cloud-based sharing is currently secured via public key infrastructure enabled signatures.

3) Creation of a blockchain

This is accurate since sensor devices have very limited computer power and cannot exploit blockchain functionalities. As depicted in Figure 2[14], the data acquired from the IoT/LPWAN gateway was transmitted to a blockchain network.

This is one technique to communicate using a blockchain node and an IoT-based healthcare infrastructure without the need for storage or compute. The IoT module receives data from sensors and tracking devices that are positioned on patients' bodies or in the monitoring area. As seen in Figure 2 [14], the data obtained through the communication channel is sent to the blockchain network. This is one approach to communicate without the need for processing or storage. In this work, we suggest employing a chain of encrypted keys in combination with a blockchain without key signatures to enable secure transmission over a healthcare system [14]. Patient-generated data from wearable systems is sent and stored in the cloud [14].

The external blockchain network was created with the intention of managing the data generated during a patient visit. The necessary information would then be applied to the consensus chain or to the decision made in advance by all blockchain stakeholders on an algorithm like "Proof of Stake."

The medical expert requires quick and secure access to the information in order to enhance care and explain the patient's status. The blockchain network processes data produced by connected devices [14]. All of the problems, including programme effectiveness, security, and data confidentiality, are resolved by the suggested solution.

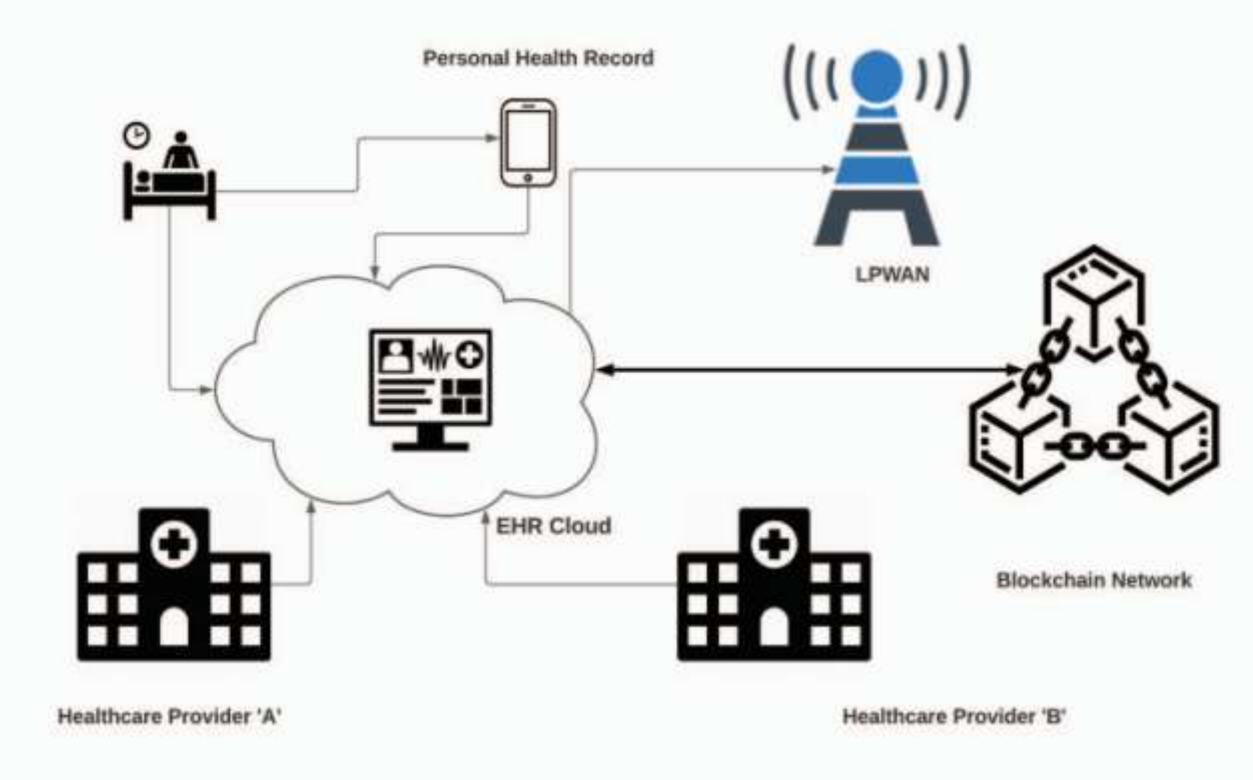

Figure 2. Proposed Blockchain framework for healthcare

IV. Conclusion And Future Work

Smart cities, transportation networks, energy systems, the healthcare industry, and other modern sectors of digital growth all depend heavily on the Internet of Things, RFID, and other technologies [32–34]. EHR security was examined in light of recent developments in blockchain technology in the healthcare industry.

This work also offers a foundation for the health care system's connection with LPWAN gateways and blockchain systems. Healthcare data is secure and reliable thanks to the proposed solution. However, there are unresolved issues that demand further research. For instance, cross-border health care information sharing involves actions involving multiple jurisdictions, which could reduce the benefits of blockchain.

Protocols, standardisation, and multijurisdictional health and data-protection measures will be difficult to recall in the future. Exploring the capacity of blockchain to store, process, and analyse large volumes of data in a reasonable amount of time will be another crucial topic of future research.

The simulation models, the consensus procedure, and their performance assessment are all part of the future work.

REFERENCES

[1] Matej Mikulic,Projected growth in global healthcare data volume2020, Statista, 2019

[2] Healthcare Cybersecurity Market To Reach USD 27.10 Billion By2026, Reports And Data, 2019

[3] Budida, D.A.M. and Mangrulkar, R.S., 2017, March. Design and implementation of smart HealthCare system using IoT. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017 InternationalConference on (pp. 1-7). IEEE.

[4] Mohammad Rashid Ansari, Abdul Quaiyum Ansari, Mohammad Ayoub Khan, Design and Evaluation of Binary-Tree Based Scalable 2D and 3D Network-on-Chip Architecture, Smart Science, Vol. 5, Number 4, pp 194-198, 2017, Taylor & Francis, https://doi.org/10.1080/23080477.2017.1383078

[5] Abdul Quaiyum Ansari, Mohammad Rashid Ansari, Mohammad Ayoub Khan, Modified quadrant-based routing algorithm for 3D Torus Network-on-Chip architecture, Perspectives in Science, Volume 8, 2016, Pages 718-721, https://doi.org/10.1016/j.pisc.2016.06.069.

[6] A. Q. Ansari, M. R. Ansari and M. A. Khan, "Performance evaluation of various parameters of Network-on-Chip (NoC) for different topologies," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-4, doi: 10.1109/INDICON.2015.7443762.

[7] M. A. Khan, M. T. Quasim, F. Algarni and A. Alharthi, "Internet of Things: On the Opportunities, Applications and Open Challenges in Saudi Arabia," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), Al Madinah Al Munawwarah, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/AECT47998.2020.9194213.

[8] M. Tabrez Quasim, F. Algarni, A. Abd Elhamid Radwan and G. M. M. Alshmrani, "A Blockchain based Secured Healthcare Framework," 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 386- 391, doi: 10.1109/ComPE49325.2020.9200024.

[9] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020. DOI: 10.1109/ACCESS.2020.2980739

[10] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," The 33rd International Convention MIPRO, Opatija, 2010, pp. 344-349.

[11] M. A. Khan and F. Algarni, "A Healthcare Monitoring System for the Diagnosis of Heart Disease in the IoMT Cloud Environment Using MSSO-ANFIS," in *IEEE Access*, vol. 8, pp. 122259-122269, 2020, doi: 10.1109/ACCESS.2020.3006424.

[12] M. A. Khan, "An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier," in IEEE Access, vol. 8, pp. 34717-34727, 2020. DOI: 10.1109/ACCESS.2020.2974687

[13] M. T. Quasim, M. A. Khan, M. Abdullah, M. Meraj, S. P. Singh and P. Johri, "Internet of Things for Smart Healthcare: A Hardware Perspective," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 2019, pp. 1-5. DOI: 10.1109/ICOICE48418.2019.9035175

[14] Quasim M.T., Khan M.A., Algarni F., Alharthy A., Alshmrani G.M.M. (2020) Blockchain Frameworks. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, DOI: https://doi.org/10.1007/978-3- 030-38677-1

[15] Christiaan Beek, et. al., Health Warning: Cyberattacks are targeting the health care industry https://www.mcafee.com/enterprise/en- us/assets/reports/rp-health-warning.pdf

[16] The threat landscape, Healthcare Cyber Security,URL: https://www.trendmicro.com/en_ie/business/capabilities/solutions - for/healthcare.html, 2019

[17] S. Amofa et al., "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-6, doi: 10.1109/HealthCom.2018.8531160.

[18] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[19] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads and Y. Tu, "MedBloc: A Blockchain-Based Secure EHR System for Sharing and Accessing Medical Data," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 594-601, doi: 10.1109/TrustCom/BigDataSE.2019.00085.

[20] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[21] Theodouli, et. al., On the design of a Blockchain-based system to facilitate Healthcare Data Sharing. In 2018 17th IEEE International Conference On Trust, Security And Privacy , pp. 1374-1379

[22] Sivagami, S., Revathy, D. and Nithyabharathi, L., 2016. Smart Health Care System Implemented Using IoT. International Journal of Contemporary Research in Computer Science and Technology, 2(3).

[23] Wang, S., et. al, Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. IEEE Transactions on Computational Social Systems, 2018, (99), pp.1-9.

[24] Raj, C., et. al, HEMAN: Health monitoring and nous: An IoT based e- health care system for remote telemedicine. In WiSPNET, 2017 International Conference on (pp. 21152119). IEEE.

[25] Alhadhrami, Z. et. al, Introducing blockchains for healthcare. In Electrical and Computing Technologies and Applications (ICECTA), 2017 International Conference on (pp. 1-4). IEEE.

[26] A. A. Neloy, et. al, "Machine Learning based Health Prediction System using IBM Cloud as PaaS,"3rd International Conference on Trends in Electronics and Informatics,India, 2019, pp. 444-450.

[27] Dey, T. et. al, HealthSense: A medical use case of Internet of Things and blockchain. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 486-491). IEEE

[28] Mohammad Ayoub Khan, et. al, Decentralised IoT, Decenetralised IoT: A Blockchain perspective, Springer, Studies in BigData, 2020, DOI:https://doi.org/10.1007/978-3-030-38677-1

[29] K. A. Abuhasel and M. A. Khan, "A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing," in IEEE Access, vol. 8, pp. 117354-117364, 2020, doi: 10.1109/ACCESS.2020.3004711

[30] Khan, MA, Abuhasel, KA. Advanced metameric dimension framework for heterogeneous industrial Internet of things. Computational Intelligence. 2020; 1–21. https://doi.org/10.1111/coin.12378

[31] A.Q Ansari, M. A. Khan, Fundamentals of Industrial Informatics and Communication Technologies, In Handbook of Research on Industrial Informatics and Manufacturing Intelligence: Innovations and Solutions, IGI Global, 2012,DOI: 10.4018/978-1-4666-0294-6.ch001

[32] Tyagi S., Ansari A.Q., Khan M.A. (2011) Extending Temporal and Event Based Data Modeling for RFID Databases. In: Nagamalai D., Renault E., Dhanuskodi M. (eds) Advances in Parallel Distributed Computing. PDCTA 2011. Communications in Computer and Information Science, vol 203. Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-24037-9_43

[33] Khan, M.A and S. Ojha, "Virtual Route Tracking in ZigBee (IEEE 802.15.4) enabled RFID interrogator mesh network," 2008 International Symposium on Information Technology, Kuala Lumpur,2008, pp. 1-7, doi: 10.1109/ITSIM.2008.4631904.

[34] S. Tyagi, A. Q. Ansari and M. A. Khan, "Dynamic threshold based sliding-window filtering technique for RFID data," 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, 2010,pp. 115-120, doi: 10.1109/IADCC.2010.5423025.