Middle East Research Journal of Engineering and Technology
ISSN **2789-7737 (**Print) & Open Access
Frequency: Bi-Monthly
DOI: 10.36348/merjet.2022.v02i01.001

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office.kspublisher@gmail.com

Critical Security & Privacy Issue in Blockchain Technology Intended to Industry 4.0

Devasis Pradhan[1*], Arun Agarwal[2], Hla Myo Tun[3], Zaw Min Naing[4], Thandar Oo[3]

[1]Assistant Professor, Department of Electronics & Communication Engineering, Acharya Institute of Technology, Dr. Sarvepalli Radha Krishnan Road, Bengaluru- 560107, India

[2]Assistant Professor, Department of Electronics & Communication Engineering, ITER, Siksha 'O' Anusandhan Deemed to be University, Jagmara, Bhubaneswar -751030, India

[3]Faculty of Electrical and Computer Engineering, Yangon Technological University, Yangon, Myanmar

4Department of Research and Innovation, Ministry of Science and Technology, Yangon, Myanmar

ABSTRACT: Block-chain is getting famous and one of the most widely recognized subjects can be thought of it has additionally changed the ways of life of many individuals in specific fields, in view of the effect on organizations and joins. Blockchain guarantees more dependable and fitting assets and it is exceptionally vital to remember that security and protection have a few deterrents as any innovation in this fields. The range of blockchain applications is extremely reached out into various regions in banking, wellbeing, car, the Internet of Things (IoT) and so forth. Numerous concentrates on focus on utilizing the block-chain information model in various executions. Motivated from these facts, in this paper, we present a systematic review of various blockchain- based solutions and their applicability in various Industry 4.0-based applications. In this paper, we attempt to portray block-chain innovation by talking about its model of information security and protection point of view with various agreement calculations, as well as issues and open doors in blockchains.

Keywords: Blockchain technology, security issues, privacy issues, IoT.

REVIEW PAPER

***Corresponding Author:**
Devasis Pradhan
Assistant Professor, Department of Electronics & Communication Engineering, Acharya Institute of Technology.

How to cite this paper:
Devasis Pradhan *et al.;* "Critical Security & Privacy Issue in Blockchain Technology Intended to Industry 4.0". Middle East Res J. Eng. Technol, 2022 Jan-Feb 2(1): 1-7.

Article History:
| Submit: 10.12.2021 |
| Accepted: 22.01.2022 |
| Published: 28.02.2022 |

1. INTRODUCTION

Over the course of the last years, the web has noticed the commencement of various base up, critical applications that settle issues in an obliging and dispersed method. A portion of these public and non-benefit frameworks have become notable and broad. One inquiry that is climbing with amazing recurrence is connected with cryptographic money bitcoin as well as the innovation source behind it called Blockchain. Albeit the examination interest endeavors to isolate blockchain from Bitcoin, the historical backdrop of the two together is worth to be known. Bitcoin was concocted in the year 2008 by Satoshi Nakamoto and the code was delivered as open source in 2009 [1-5].

With the wide prominence of the Internet and related advances, different Industry 4.0-based applications have been involved across the globe in which sensors and actuators sense, register, and impart the information for modern robotization. As in Industry 4.0-based applications, information between various areas streams utilizing an open channel. Such applications manage information in enormous volumes and thus, it is important to consider issues, for example, information heterogeneity, information respectability, and information overt repetitiveness alongside security and protection concerns. Also, various applications require datasets from various areas in various organizations. In this manner, it is additionally expected to normalize the information design so it very well may be utilized by various Industry 4.0-based applications [6-8].

2. BLOCKCHAIN TECHNOLOGY

Blockchain is a digitized, decentralized, and public record of all cryptographic money exchanges. These exchanges are recorded in sequential request, making a difference member to monitor computerized money exchanges without focal recordkeeping [17, 3, 22]. A conveyed information base is one of the vital highlights of blockchain [11]. This sort of data set exists in many duplicates across different PC frameworks shaping a distributed organization, signifying that no singular, unified data set or server exists [18]. All things

considered, a blockchain data set across the decentralized organization of PCs exists. Each PC in the organization is known as a hub in the organization and each hub in the organization gets a copy duplicate of the blockchain that naturally gets downloaded. Exchanges are carefully endorsed with public key cryptography that utilizes two keys, which contains a public and a confidential key. These two keys are numerically connected with each other. Inferable from the intricacy of math utilized, it is remarkably difficult to figure these keys, making it harder for the exchanges to be broken. The public key is utilized to sign and scramble a message to be sent and the assigned beneficiary can decode the message utilizing their confidential key. To keep up with the blockchain data set as a "Overall Ledger" information regarding all new exchanges is engendered to all hubs [9-12].

3. Basic Elements of Blockchain 4.0

The level of consistent mix of Industry 4.0-based applications. It utilizes the brilliant agreement which takes out the requirement for paper-based agreements and manages inside the organization by its agreement.

a. Smart Contracts (SC): It is a convention that permits the presentation of exchanges without an outsider that makes exchanges irreversible and detectable.
b. Tokenization: It is quite possibly of the main thing that should be remembered for the blockchain. It works with the advanced portrayal of merchandise, administrations, and privileges with the assistance of tokens. It permits the trading of values also, trust for various clients without including the focal authority.
c. Information security: Security consistence is a significant and fundamental necessity of blockchain innovation with a lawful perspective.
d. Decentralized information capacity: It is an essential necessity of the appropriated framework.
e. Agreement: Transactions ought to possibly be refreshed when every one of the confirmed clients in the organization consents to something very similar.
f. Composed Blocks: It is expected for the savvy contract and for high velocity installment in deals. Thus, information arranging of the various kinds of blocks including its time, agreement calculation, number of exchange per obstructs, and its substance information types.
g. Sharding: It is expected for the division of content over subsets of hubs as it were, that not every one of the hubs need to convey all handling load or any weight.
h. Access privileges the board: Encryption-based private also, public key cryptography and dispersed data sets with client, ID is expected to appoint and make due access freedoms.
i. Standard information arranging: In the blockchain framework, it is additionally expected to normalize the information designs with regard to Application Programming Interfaces (API). Every association in the blockchain network requirements to utilize similar information arrangement or APIs to convey in the same organization.
j. Updation: The requirement for information updation in the circulated record is generally significant for records. In a shared network, information should be organized and deliberately refreshed for every hub that executes inside the organization.
k. Anonymity: Using a haphazardly made address, any client might draw in with the blockchain without uncovering their genuine personality. Be that as it may, the exchange history is freely accessible to all clients. While the bitcoin blockchain can't guarantee security inferable from its characteristic limitations, other blockchain conventions vow to give the greatest degree of secrecy.

4. Security Issue of Blockchain 4.0

Security in blockchain can be characterized as the insurance of exchange data and information in a block (whatever type of information) against interior and fringe, malignant, and unexpected dangers. Ordinarily, this assurance includes location of danger, avoidance of danger, and proper reaction to danger utilizing security arrangements, instruments, and IT administrations [13-15].

a. Guard in entrance. This is a methodology which utilizes various restorative measures to safeguard the information. It follows the rule that safeguarding information in various layers is more effective rather than a solitary security layer.
b. Least Privilege: In this system, admittance to information is decreased to the most minimal level conceivable to build up a raised degree of safety.
c. Oversee weaknesses. In this system, we check for weaknesses and oversee them by recognizing, confirming, altering, and fixing.
d. Oversee risks. In this methodology, we process the dangers in a climate by recognizing, surveying, and controlling dangers.
e. Oversee patches. In this methodology, we fix the defective part like code, application, working framework, firmware, and so on by obtaining, testing, and introducing patches.

5. Privacy Issue of Blockchain 4.0

Protection is the capacity of a solitary individual or a gathering to separate themselves or information, consequently, articulating their thoughts insightfully. Security in blockchain implies having the option to perform exchanges without spilling distinguishing proof data. Simultaneously, security permits a client to stay consistent by insightfully disclosing themselves without displaying their action to the whole organization [16, 17, 19].

a. **Adaptability**: Blockchain gives the adaptability to store all types of information. The protection viewpoint in blockchain differs for individual and hierarchical information. In spite of the fact that protection rules are pertinent for individual information, more tough security rules apply to delicate and hierarchical information [18].
b. **Capacity dissemination**. The hubs in the organization that stores total duplicates of the blockchain are called full hubs. The full hubs in blend with the add just trait of blockchain lead to information overt repetitiveness. This overt repetitiveness of information upholds two critical highlights of blockchain innovation including straightforwardness and evidence. The similarity of the application with information minimization chooses the degree of straightforwardness and undeniable nature of that organization for an application [19].
c. **Annex as it were**. It is difficult to change the information of past blocks in the blockchain undetected. The affix just component of blockchain in specific cases doesn't reduce to one side to revision of clients, particularly in the event that information is recorded inaccurately. Exceptional consideration should be given while doling out privileges to information subjects in blockchain innovation.[20]
d. **Confidential versus public blockchain**. The availability of blockchain is momentous from the point of view of security. At a high level, the confined information on a block can be encoded for contingent access by approved clients as each hub in the blockchain keeps a duplicate of the whole blockchain.
e. **Non-permissioned versus permissioned sorts of blockchain**. With public or nonpermissive blockchain applications, all clients on a basic level are allowed to add information. Allowing the rebuilding of believed arbiters impacts the appropriation of command over the organization [21].

6. OPEN CHALLENGES

6.1 Deployment in Smart Cities

The future of the blockchain can be chosen by its security, heartiness, savvy contract, information base innovation, security tokens, and changing administrative climate. Nonetheless, to accomplish the objectives, the plan and execution of the blockchain need to give outrageous dependability, security, also, versatility which depend on significant innovations, for example, shared record, agreement, provenance, permanence, and savvy contract. Figure 2. depict potential component of smart city where blockchain can play a important role [22-23].

a. **Usage of Land/Property**: Conventional enlistment of land or property is a very time consuming and expensive cycle. The blockchain innovation can take out the obstacles related with this traditional process by making a computerized course of mechanized property enlistment. This arrangement expands the straightforwardness and trust inside the framework and works on the economy. The fresher advancement of savvy urban areas joins the blockchain based innovation for various cycles like land and property library, getting endorsements, producing assessment reports what's more, recording the authentications [24].
b. **Transport and Logistics**: The transportation business is exceptionally famous these days to offer routine types of assistance to countless clients. Offering fundamental types of assistance to the clients is very exorbitant. The association of outsiders in offering types of assistance may lead to the break of protection of clients' very own information too as an expansion in the expense of benefiting administrations. A decentralized blockchain organization can deal with this multitude of issues successfully.
c. **Education Sector:** In this day and age, schooling foundations either private or public, try not to give the specific records to the public authority. That is why the public authority can't check or help for proficiency targets. With the incorporation of blockchain innovation, instructive records can be made accessible by means of a computerized assent system. This arrangement makes the data repetitive furthermore, the equivalent can be coordinated with the public authority populace library so it can deal with all the proficiency focuses in the nation's populace [25].
d. **Identification:** In the ongoing time, online administrations need clients or clients to give individual distinguishing proof data prior to benefiting of the administrations. This large number of information is put away without the information of the proprietors and can be gotten to by outsiders. When decentralized blockchain innovation is utilized to carry out internet based administrations, computerized ids are made for all clients. These ids alongside computerized watermarking strategies are utilized while executing client exchanges. This is the manner by which clients' information can be put away, kept up with, and controlled in the permissioned network approaching privileges just with the person clients [21, 23].

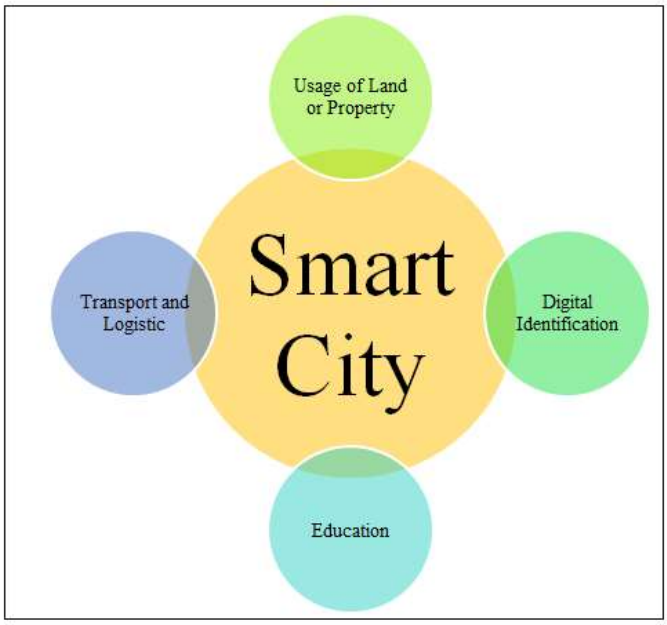

Figure 2: Component of Smart City

6.2 Implementation to Smart Healthcare

Basic Component of healthcare is shown in Figure 3.

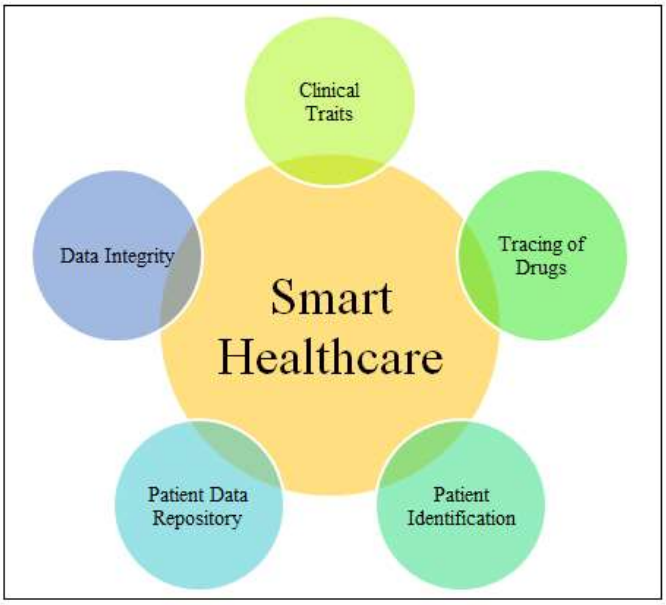

Figure 3: Basic Component of Smart Healthcare

a. **Data Integrity**: Patients' wellbeing data, electronic wellbeing records, information gathered from IoT, and it are kept up with to screen frameworks by the clinical offices. Here, the fundamental objective is to get the data and its sharing procedures, approve healthcare offices and its elements to affirm the right information and guarantee the legitimate administrations. The blockchain is more valuable in such situations as a result of its capacity to give information respectability [18-19].

b. **Patient Identification:** Consistently the volume of medical care related information increments furthermore, frequently while managing medical services information, records get crisscrossed or copied. Likewise, unique electronic wellbeing records frameworks have their own information configuration and informational collection to enter and execute the information, which raises a requirement for a normalized information design. Because of the utilization of blockchain innovation, the information are cryptographically hashed in the record [17-19].

c. **Patient Data Repository**: The patients' information security and makes the information PHI got, however the patients need to give their clinical information to outsiders like drug

specialists, forcing the need of safeguarding the information. With the utilization of the blockchain, a hash for every patient's wellbeing data in blocks contains the patient guide made.

d. **Clinical Traits**: In blockchain innovation, information adjustment is unthinkable with the SHA256 calculation that makes the remarkable hash values which are connected together into a chain. The medical services industry necessities to keep up with and share the data connected with clinical preliminaries safely which can be imparted to approved gatherings, for example, research supports or then again administrative councils. With the blockchains, the information can be overseen or followed with assent inside numerous locales, protocols, and frameworks [17-20].

e. **Tracing of Drugs:** At present, the primary obstacle in pharmacology is drug falsifying. By a study of wellbeing specialists, it has been seen that around 10 to 30 percent of the medications in non-industrial nations are copies. The unfriendly impact of this is the deficiency of business and inappropriate use of phony medications which can prompt serious harm to an individual's wellbeing. The utilization of the blockchain network across the medication offices can recognize cheats from the street pharmacist [17-19].

6.3 Implementation of IIoT

IoT environments rely on the brought together organization in which every one of the gadgets are associated in a client-server model through handled correspondence. It utilizes the cloud server to verify and recognize gadgets. With the expansion in the quantity of gadgets utilized in IoT every year, it turns into an extremely tricky and testing task for makers or specialist co-ops to keep up with these gadgets on a day to day basis. A unified data set has a limited registering power and capacity limit. There is consistently an enormous number of hubs to interface with the server which is a tedious errand. It is additionally hard to track down broken hubs in this construction. A large portion of the IoT gadgets associate with the brought together data set and cloud network which builds the expense and computational necessities [21-23, 25-28]. In the circulated blockchain innovation, hubs have least availability yet, the organization remains solid and safe. The basic components of Industrial Internet of Things(IIoT) is shown in Figure 4.

These days, to procure a benefit, different organizations store, use, and offer clients' information to outsiders without the assent of the clients. Such activities compromise the security of clients' information. Blockchain innovation utilizes a disseminated data set structure that stores information in encoded structure and subsequently diminishes the gamble of information taking and break of security. In the ongoing time, sensor gadgets utilized in IoT applications are little in size and have restricted processing and stockpiling limit. Thus, such gadgets are helpless against physical goes after like pantomime or satirizing. The blockchain innovation utilizes savvy agreements and agreement systems which support the appropriate character confirmation of the IoT [22-24].

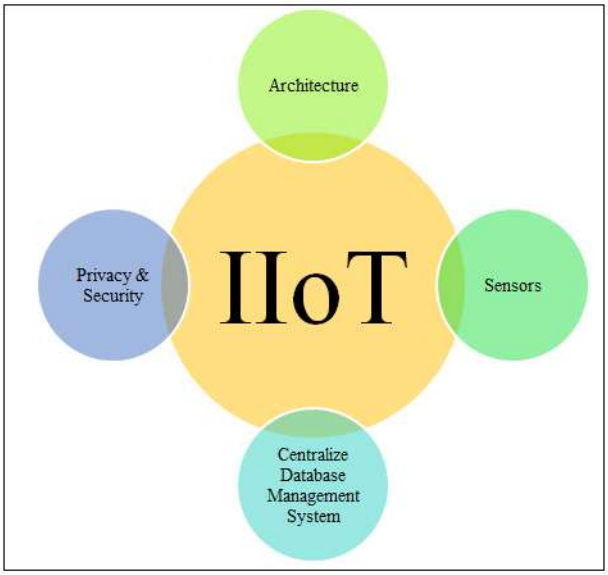

Figure 4: Component of Industrial Internet of Things (IIoT)

6.4 Implementation in Smart Agriculture

In agribusiness, all the data with respect to food varieties, ranchers, also, merchant purchaser data is extremely obsolete and not accessible to all clients. Thus, handling the data is undeniably challenging also, lead market investigation. With the use of a blockchain network, every one of the members approach of all records and exchanges in a dependable and secure way. A few times limited scope ranchers are not getting the entirety market access in agribusiness. In this manner,

the ranchers split the difference with greater expenses with restricted admittance to the market. With the the assistance of circulated record innovation of blockchain network, every one of the information are accessible and simple admittance to each market on the organization, which helps every one of the ranchers to interfaces with the market and furthermore to fabricate trust. Figure 5 depicts the basic elements of Agriculture field [23-25].

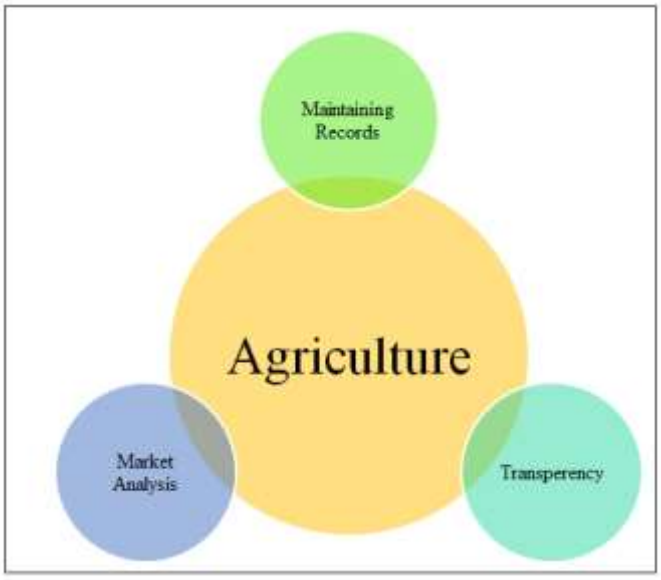

Figure 5: Elements of Agribusiness

6.5 Energy Management

In the present situation, we don't have a savvy network like framework, and the utilization of the typical foundations makes the outsider go-between issues like VAT cheats, security issues, significant expense, and fossil fuel byproducts which can lead the climate to an exceptionally more regrettable condition. With the utilization of blockchain innovation, the improvement of the brilliant lattice energy framework is conceivable through which each client can get emanation stipend measures for the secure environment [25, 26].

7. Conclusion

Various sorts of examination on blockchain security and protection have been led, notwithstanding, a total investigation of blockchain security stays lacking. We intended to show a methodical delineation of blockchain security weaknesses by looking at noticeable blockchain frameworks and giving a full depiction of the related genuine attacks. All through this section, we've discussed blockchain's security and protection highlights and their different applications and difficulties. The section has focused on the most significant blockchain security and privacy issues.

Reference

1. S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Tech. Bitcoin.Org., 2008.
2. P. Noizat, ‘‘Blockchain electronic vote,’’ in Handbook of Digital Currency, D. L. K. Chuen et al., Eds. San Diego, CA, USA: Academic, 2015, ch. 22, pp. 453–461.
3. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, ‘‘A survey on privacy protection in blockchain system,’’ J. Netw. Comput. Appl., vol. 126, pp. 45–58, Jan. 2019.
4. G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, ‘‘Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions,’’ Comput. Ind., vol. 109, pp. 83–99, Aug. 2019.
5. V. J. Morkunas, J. Paschen, and E. Boon, ‘‘How blockchain technologies impact your business model,’’ Bus. Horizons, vol. 62, no. 3, pp. 295–306, May 2019.
6. Y. Lu, ‘‘The blockchain: State-of-the-art and research challenges,’’ J. Ind. Inf. Integr., vol. 15, pp. 80–90, Sep. 2019.
7. H. F. Atlam and G. B. Wills, ‘‘Technical aspects of blockchain and IoT,’’ Adv. Comput., vol. 115, pp. 1–39, Mar. 2019, doi: 10.1016/bs.adcom.2018.10.006.
8. X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, ‘‘Survey on blockchain for Internet of Things,’’ Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.
9. M. Muzammal, Q. Qu, and B. Nasrulin, ‘‘Renovating blockchain with distributed databases: An open source system,’’ Future Gener. Comput. Syst., vol. 90, pp. 105–117, Jan. 2019.
10. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, ‘‘A review on consensus algorithm of blockchain,’’ in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC), Oct. 2017, pp. 2567–2572.

11. U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, ‘‘A survey on decentralized consensus mechanisms for cyber physical systems,’’ IEEE Access, vol. 8, pp. 54371–54401, 2020.
12. S. Hirsh, S. Alman, V. Lemieux, and E. T. Meyer, ‘‘Blockchain: One emerging technology—So many applications,’’ Proc. Assoc. Inf. Sci. Technol., vol. 55, no. 1, pp. 691–693, 2018.
13. M. H. Onik, M. H. Miraz, and C.-S. Kim, ‘‘A recruitment and human resource management technique using blockchain technology for industry 4.0,’’ in Proc. Smart Cities Symp., Apr. 2018, pp. 1–6
14. Pradhan D, Priyanka KC. RF-Energy harvesting (RF-EH) for sustainable ultra dense green network (SUDGN) in 5G green communication. Saudi Journal of Engineering and Technology (SJEAT). 2020;5(6):258-64.
15. Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, ‘‘A decentralizing attribute-based signature for healthcare blockchain,’’ in Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN), Jul. 2018, pp. 1–9.
16. P. Fraga-Lamas and T. M. Fernandez-Carames, ‘‘A review on blockchain technologies for an advanced and cyber-resilient automotive industry,’’ IEEE Access, vol. 7, pp. 17578–17598, 2019.
17. Pradhan D, Priyanka KC. A comprehensive study of renewable energy management for 5G green communications: Energy saving techniques and its optimization. Journal of Seybold Report ISSN NO. 2020;1533:921
18. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ‘‘MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,’’ IEEE Access, vol. 5, pp. 14757–14767, 2017.
19. N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, ‘‘Towards using blockchain technology for eHealth data access management,’’ in Proc. 4th Int. Conf. Adv. Biomed. Eng. (ICABME), Oct. 2017, pp. 1–4.
20. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ‘‘Integrating blockchain for data sharing and collaboration in mobile healthcare applications,’’ in Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Oct. 2017, pp. 1–5.
21. Pradhan D, Sahu PK, Dash A, Tun HM. Sustainability of 5G green network toward D2D communication with RF-energy techniques. In2021 International Conference on Intelligent Technologies (CONIT) 2021 Jun 25 (pp. 1-10). IEEE..
22. Kalukhe Siddhesh Vikas Susmita. (2021). Portable Firewall for Data Security toward Secured Communication. East African Scholars J Eng Comput Sci, 4(4), 41-45.
23. Srivastava, Shivika, et al. “IoT Based Human Guided Smart Shopping Cart System for Shopping Center.” Saudi Journal of Engineering and Technology, June 2020. Scholars Middle East Publishers, https://doi.org/10.36348/sjet.2020.v05i06.004.
24. Devasis Pradhan, A Dash (2020) 'An Overview of Beam Forming Techniques Toward the High Data Rate Accessible for 5G Networks', International Journal of Electrical, Electronics and Data Communication, ISSN(p): 2320-2084, ISSN(e): 2321-2950 , 8(12), pp. 1-5
25. Pradhan D, Priyanka KC. GREEN-Cloud Computing (G-CC) Data Center and Its Architecture toward Efficient Usage of Energy. InFuture Trends in 5G and 6G 2021 Dec 30 (pp. 163-182). CRC Press.
26. Pradhan D. 5G-Green Wireless Network for Communication with Efficient Utilization of Power and Cognitiveness. In International Conference on Mobile Computing and Sustainable Informatics 2020 Jan 23 (pp. 325-335). Springer, Cham.
27. Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, ‘‘Introducing blockchains for healthcare,’’ in Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA), Nov. 2017, pp. 1–4
28. S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, ‘‘BlocHIE: A blockchain-based platform for healthcare information exchange,’’ in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun. 2018, pp. 49–56.