WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Block-Chain-Based IoT Gateway Security Mechanism for Efficient Network Establishment:

Rohit Karosiya, Prof. Unmukh Datta

Computer Science, Maharana Pratap Colllege of Technology

DOI : https://doi.org/10.55248/gengpi.6.0425.1592

ABSTRACT –

The best information security characteristics are necessary sensors and wireless sensor networks connected to the IoT. A thorough analysis of IoT security concerns is provided. Recent years have uses in industry, smart homes, smart cities, and more. First, an overview of the Internet seen an enormous number of security problems and threats looking for weaknesses that may be used to take advantage of any network. Security concerns have emerged as a major issue that necessitates prompt and ongoing attention against the backdrop of the Internet of Things' recent, fast expanding technological innovation. Given that security and privacy show an persistent problems, so finding and analyzing vulnerabilities is a crucial network procedure. In order to stop malevolent attempts and network incursion, this thesis offers block chain-based security analysis of data produced by IoT devices. A vast array of diverse sensing devices, topologies, and protocols can be found network.

I. INTRODUCTION

The Internet of Things is one of the fastest-growing technological paradigms, with a vast number of devices that generate, process, and exchange vast amounts of data. IoT devices within the network can therefore be the target of various threats and intrusions. The limited power becomes a difficult problem for security and privacy because many lightweight IoT devices have low energy capacities that are used by their core functions and application processing . Low-powered IoT devices and networks cannot use the conventional security techniques and protocols for sensing, processing, and communication.

II. LITERATURE REVIEW

Internet of Things Security Survey :

Le et al. [139] suggested a simple method for safe devices that uses an observer or attestor from a blockchain-based Internet of Things network to approve new blocks. The IoT devices can process and validate utilizing Bloom filters without requiring complicated computations. Their experimental simulation demonstrates that low-power devices may accomplish blockchain security.

Prada-Delgado et al. [140] presented a novel anti-counterfeiting method for Internet of Things devices that takes advantage of special features of embedded memory chips to extract encrypted private data that is part of a blockchain block for trustworthy and dependable identity verification of IoT devices. They used a Texas Instruments microcontroller to measure and analyze the performance under various operating situations. When compared to unprocessed answers, the experimental results demonstrate the distinctive feature of performance across a wide temperature range with a noise reduction in the physical unclonable function (PUF) responses of up to 90%.

Using the ring signature technique and proxy re-encryption, Gong et al. [143] introduced a blockchain-based privacy protection architecture for the Internet of Things. Within this framework, authorized users share this dispersed data, and a blockchain-based distributed storage system relieves the operational strain of a traditional centralized IoT network. In order to protect data privacy, the proxy re-encryption technique was developed to safely share data between service providers and authorized users.

The proxy node acts as an intermediary while sending cipher text data, making it hard to determine the source address and link of the data sharing individual. A ring signature technique is used to effectively protect the sender's data address information and stop intermediary nodes from deceiving the transaction parties by preventing them from accessing the address information.

The "IEEE P1931.1 ROOF Standard," which has possibilities for the Internet of Things, all function as fully autonomous systems that don't require human interaction or context awareness. All of these significant interactions are represented by the Real-Time Onsite Operations Facilitation (ROOF).

A "Secure Method of Exchanging Resources in Heterogeneous Internet of Things (SMER)" was put up by Zhang et al. [147]. The SMER system offers facilities for the efficient, profitable, secure, and effective interchange of resources for IoT devices. This study established a model based on the operational process of SMER and elaborated on the structure and functional technique of the SMER system.

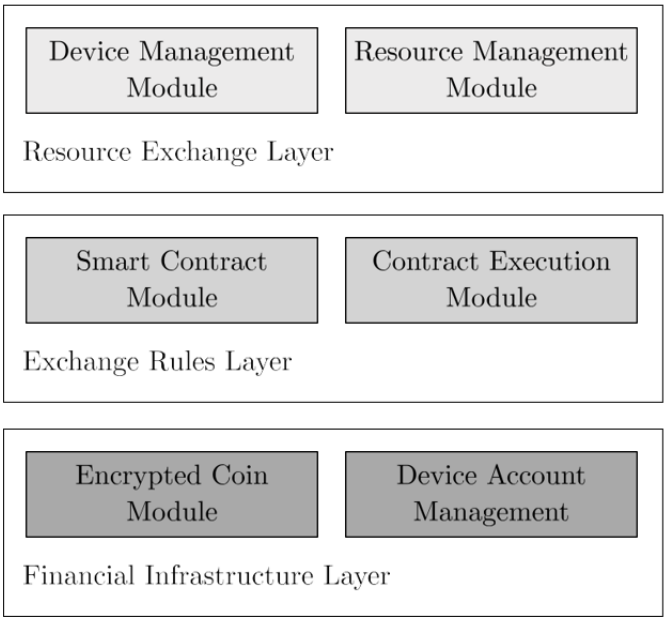

Figure 1 : The Layered Architecture of the SMER System

Lastly, device account management and an encrypted currency module are offered by the financial infrastructure layer. It is also in charge of creating and managing accounts for every IoT device and oversees resource exchange concerns. Additionally, this layer is in charge of transaction, transfer, and account security records.

Issues with privacy in IoT systems : Future global networks of "things" present privacy and security issues. Availability, confidentiality, and integrity become critical when data is transferred between IoT devices. In order to prevent device corruption and its impact on the network, additional responsibility is required due to the intelligence and autonomy of these devices. There are various process-based and cryptographic methods available to guarantee and provide availability, secrecy, and integrity. However, in addition to these services, IoT systems must emphasize how these solutions are implemented.Optimized and carried out. Therefore, it is essential to examine the IoT platform as a whole using basic security concepts that can help security researchers and advocates better understand the key characteristics that a secure IoT solution has to have.

IoT physical components are susceptible to availability, confidentiality, and integrity attacks since security is a major concern for large networks. Using cryptographic features is the "first line of defense.". While message authentication codes guarantee both integrity and authenticity, encryption schemes safeguard confidentiality. Attack models requiring physical access to the nodes were addressed by earlier WSN implementations. After WSNs were made available to the Internet, the threat model evolved because attackers could now access WSNs everywhere, where sensor nodes were most at risk from limited processing power.

Survey of Block chain : Block chain is having a profoundly transformative effect on the production of technology and knowledge in the knowledge society, not just in this production, but also in the reorganization of the economy and society to generate commodities and services. The new industrial revolution has been discussed extensively the economy, and society. In the short term, it is anticipated that these developments will change how goods and services are produced. Under such circumstances, a new industrial revolution is on the horizon, one that is in line with artificial intelligence and ES (expert systems). This will change the way that things are produced, from mass production to customized production, and have an unprecedented effect by gradually changing how people are grouped in society for this purpose, which will lead to a decentralized economy.

The primary contribution of this study is the development of an expert system that can design any drawing without the need for an existing one. Better yet, it is based on a decentralized system like the block chain. The block chain will support the safety and integrity of the data against any human errors or hacker attacks, and this kind of expert system can be helpful in any industry transformation process.

Drawings are the foundation of the evolving industry since they contain all the necessary information (know-how, bill of materials, supplies, assembly indications, technological signals, etc.) to complete the task, hence developing a designer expert system can propel the sector into an industrial revolution. In this instance, the expert system's primary task is creating installation plans for sensors in smart homes.

III. METHODOLOGY

Problem Statement : The following security flaws exist in contemporary IoT network-based infrastructures:

- **System for Centralized Intrusion Detection :** The centralized security measures used by contemporary IoT-based systems to stop intrusion detection systems function well in many homogeneous networks but poorly in most heterogeneous ones.
- **Peer-to-peer communication that is not trusted :** Peer-to-peer transactions and interactions are followed by a variety of device-to-device and machine-to-machine connections; this has become a difficult problem. To get around this restriction, a decentralized security mechanism is necessary.
- **Unsecured Gateway Protection :**

The provision of gateway security has always been an essential duty for any infrastructure.

- **Ineffective Mechanism for Fault Tolerance :** All network infrastructures must be able to self-recover from partial failures because even one system failure could result in a total system failure.

Shortage of research:

According to the expert review, at present there are many research works related

- also made a huge contribution in today's time, so there is a lot of lack of research work here, there is a good amount of research work available here, there is a huge shortage of research work here right now.
- Evaluating the performance of any employee in the corporate sector comes under wireless sensor networking and it is also used in Internet of Things applications, so here also a lot of research work is present in today's time, but the research work has not been done properly here yet and there are lot of flaws here.
- there is a great opportunity to do research work in this field.
- A particular model can be prepared to improve the management schemes related to any ashram or trust, but here also there is a lack of research work.
- Creating an efficiency enhancement model using the Internet of Things which has the security of goals and planned research for the proposed study :

- **System for Decentralized Intrusion Detection :** Better virus protection and intrusion prevention mechanisms are offered by blockchain-based security solutions in Internet of Things networks.
- **Establishing Trust in Peer-to-Peer Interactions Trusted Peer-to-Peer Communication :** Communication with untrustworthy devices is made possible by the Blockchain-based peer-to-peer distributed IoT network, which is effective, reliable, and secure.

- **Effective Gateway Security System :** For effective network setup, the blockchain implementation offers a reliable IoT gateway security mechanism.
- **Fault Tolerance System Based on Blockchain Technology :** A fault-tolerant system design in IoT networks is facilitated by the Blockchain-based validation method, ensuring the system remains operational even in the event of a fault occurring.

IV. EXPERIMENT AND RESULT

A Block-chain-based IoT gateway security mechanism for efficient network establishment :

Security Concerns with IoT Gateways :

An essential part of a smart home is the home gateway, which communicates with external networks and shares and exchanges data across multiple heterogeneous protocols. Multiple heterogeneous networks can be coupled with IoT networks, and there should be a gateway with several interfaces. The gateway security system protects all of the appliances and smart home components in addition to itself. As a result, gateway security is a crucial component of smart home systems. As shown in Figure 1, the IoT-based smart home has the following security problems.

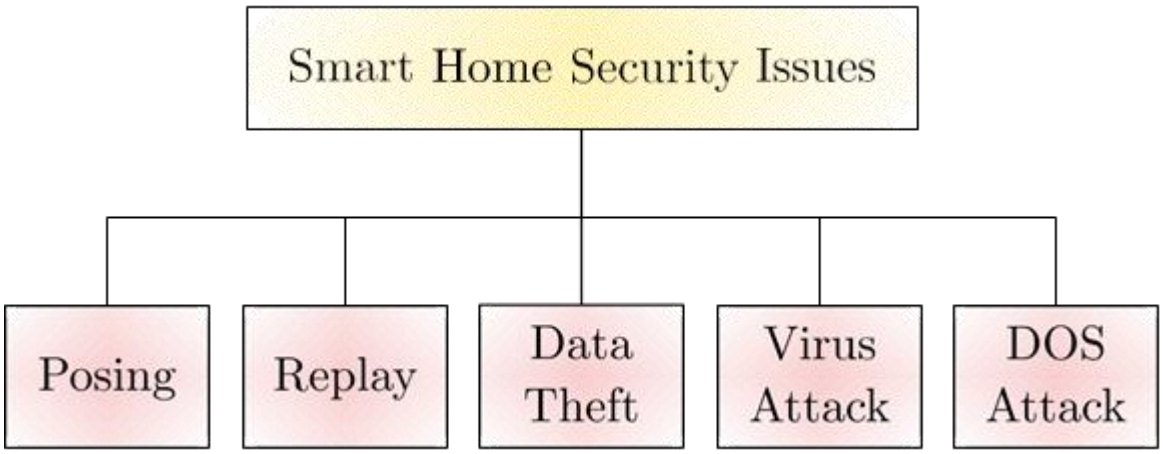

Figure 1 : Smart Home Security Issues

- **Posing :** An attacker or intruder can pretend to be a home gateway to send fictitious data to the terminal host by providing control commands, or he can pretend to be an end host to the smart home gateway.
- **Replay :** Replay attacks come in two varieties: home gateway replay and terminal host replay.
- **Data Theft :** Data packets and information can be intercepted by tapping the line between the smart home gateway and the terminal host.
- **DOS Attacks :** The "denial-of-service (DOS)" assault prevents other users from accessing the network and disrupts it.

of a traditional centralized Internet of Things network, and this dispersed data is shared by authorized users. In order to protect data privacy, the proxy re-encryption technique was developed to safely share data between service providers and authorized users. The proxy node acts as an intermediary while sending cipher text data, making it hard to determine the source address and link of the data sharing individual. A ring signature technique is used to effectively safeguard sender data address information and stop intermediary nodes from deceiving the transaction parties by preventing them from accessing the address information.

Proposed System Model : As IoT-based research continues to grow, it has impacted people's modern lifestyles and offered a wide range of applications in business, medicine, education, industry, and many other fields. Because there are so many different IoT applications, the an increasingly important aspect of the Internet of Things network is order to guarantee and validate the system's regular operations. These days, block chain technology offers exceptional network and database security solutions. Figure 2 shows the suggested block chain-based IoT gateway security system for effective network setup.

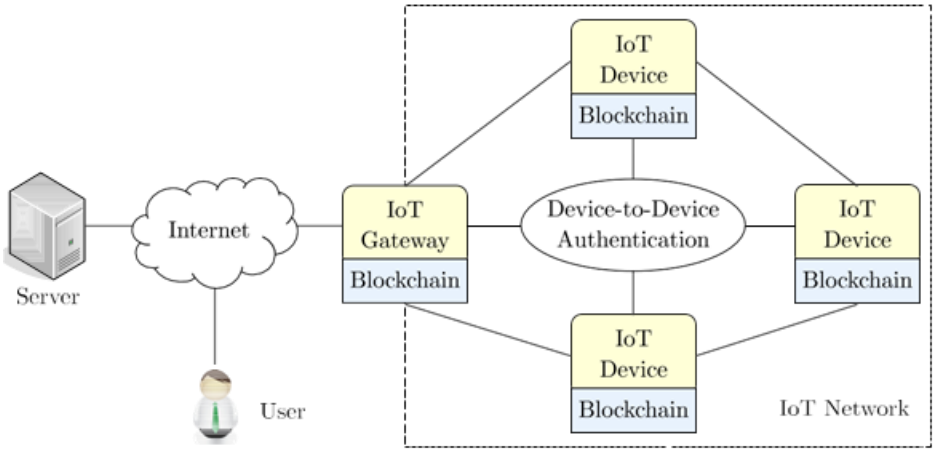

Figure 2 :Internet of Things Gateway Security

Deploying all edge computing IoT devices is crucial after creating and implementing the Block chain-based gateway and network. The following steps can be used to describe the suggested process:

- The local sample IoT devices are first regarded as independent synchronous devices.
- A probability distribution model is created using the Gaussian model to resemble a normal distribution, and the maximum probability value for the targeted function distribution is obtained by modifying every location and node degree in the local network.

Equation 1 displays the distribution function for this process:

$$f(x,\mu,\sigma) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{1}{2}(x-\mu)^2\sigma^{-2}}$$

……(1)

Where denotes the mean value, which describes the center of the probability distribution; variance, which denotes the degree of data density of an IoT device, is represented by 2. The distribution is more decentralized if this value is higher.

and it is the more centralized if the value is less. Equation 2 displays the entire sum of the corresponding possibilities or probabilities:

$$P(x_i,\mu,\sigma) = \sum_{j-1}^{K} \alpha_j \times f(x_i,\mu_j,\sigma_j)$$

……(2)

where j denotes each component's weight and must satisfy Equation 3.

$$\sum_{j-1}^{K} \alpha_j = 1, \quad 0 \le \alpha_j \le 1, \forall_j \in [1,K]$$

……..(3)

Based on these formulas, it may guarantee that, under the maximum probability distribution, the desired workload of every device in the network that the gateway's processor covers will be insufficient to support its improved operation.

Result Analysis :

The simulation results of the suggested blockchain-based gateway security solution are shown in this section. The data transmission of nodes from nodes of other networks is necessary in this proposed network, and a gateway records every transaction into

distributed ledger system built on the blockchain. Hit rate, system hit rate, and average response time are regarded as the key analytical parameters for results evaluation. Figure 2 shows the corresponding hit ratio comparison between centralized networks and blockchain integrated gateway-based networks, taking into account the different storage sizes of IoT devices.

The Comparison of Hit Rate between Centralized and Blockchain

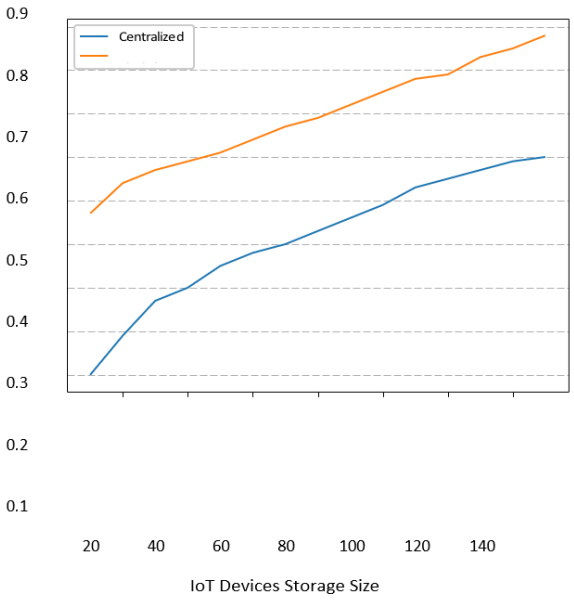

Figure 3 The Hit Rate Comparison between Block chain-Integrated Gateway-based Networks and Centralized Networks.

Figure 3 shows both a block chain-integrated gateway-based network and a centralized network. Figure 4 shows the average response time comparison between a block chain integrated gateway-based network and a centralized network. The hit rate and integrated system hit rate both rise as the storage capacity of IoT devices grows. A block chain-based IoT gateway system exhibits a greater one-shot hit rate than a centralized IoT network, as seen in the results from Figures 3 and 4. Additionally, as shown in Figure 3, the average response time of a block chain-enabled gateway network is less than that of a centralized system, indicating that the decentralized IoT network is not only safe but also because it reacts much more quickly than a centralized IoT network when IoT device storage capacity increases.

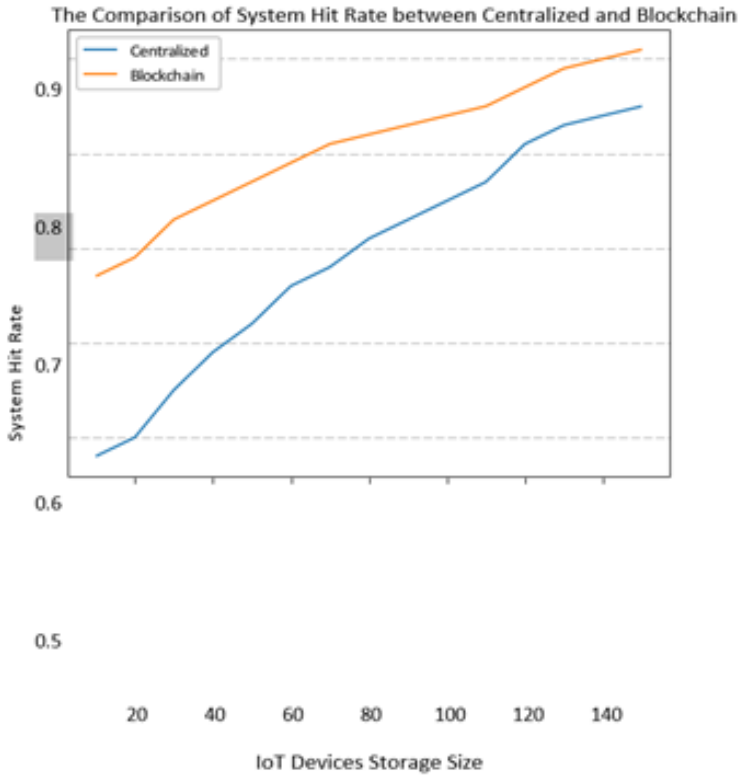

Fig 4 The System Heat Rate Comparison Between Block-chain Integrated Gateway-Based Networks and Centralized Networks

V.CONCLUSION & FUTURE WORK

Conclusion :

Since IoT-based applications are becoming more and more prevalent due to the never-ending advancement of current technology, and because there are innumerable IoT devices connected to heterogeneous networks, privacy and security concerns have grown to be major concerns worry and difficulty for technicians, researchers, and pertinent specialists. IoT device networks with gateways are examined, and centralized and block chain-based distributed systems are simulated and optimized based on hit rate, average response time, and the network's overall system hit rate. It is evident from of gateways and Internet of Things application space, gateway security and device analysis are crucial. It also promotes the expansion of the IoT network and permits numerous estimations for the future work of IoT-based computation and security analysis.

Future Work :

Over the past few years, a small number of leading companies have been testing simple use cases that will be implemented sometime in the upcoming year. However, hardly nobody is now utilizing IoT block chain solutions, and numerous future block chain initiatives in e.g. The supply chain industry will only track its goods using the "block chain" portion of IoT block chain; data entry will still be done by hand. Right now, an embedded wallet for the Internet of Things—basically, a "Ledger Nano" for machines—seems like a potential answer. Almost any device could connect to any DLT in this fashion, and since it isn't an IoT gateway, it keeps the advantages of block chain security while significantly lowering the burden on IoT devices due to its lack of full node functionality. If we want a completely scalable infrastructure for an autonomous, machine-driven economy in the ensuing decades, this might be one approach.

The Internet of a few decades ago is still analogous to block chain today. The modern Internet is very different from what it was in the past, and block chain technology is no exception. To put it simply, block chain can bring about a completely new level of to the Internet by establishing new guidelines for peer-to-peer communication and data transparency. The use cases of block chain (and IoT) that we see today, in my opinion, will resemble the extremely slow Internet that existed when it first became available to the public in the 1990s in a few decades. In the upcoming years, devices will be able to transport not only data but also money, creating new marketplaces worth trillions of dollars.

Reference

[1] E. Troubleyn, I. Moerman, and P. Demeester, "Qos challenges in wireless sensor networked robotics," *WirelessPersonalCommunications*, vol. 70, no. 3, pp. 1059–1075, Jun 2013. doi: https://doi.org/10.1007/s11277-013-1103-2

[2] A. Sharif, V. Potdar, and E. Chang, "Wireless multimedia sensor network technology:A survey," in*20097thIEEEInternationalConferenceonIndustrialInformatics*,June2009,pp. 606–613.doi:https://doi.org/10.1109/ INDIN.2009. 5195872

[3] C.Li,H.Zhang,B.Hao,andJ.Li,"Asurveyonroutingprotocolsforlarge- scale wireless sensor networks," *Sensors*, vol. 11, no. 4, pp. 3498–3526, 2011. doi: https://doi.org/10.3390/s110403498

[4] D. Midi, S. Sultana, and E. Bertino, "A system for response and prevention of security incidentsinwirelesssensornetworks,"*ACMTrans.Sen.Netw.*,vol.13,no.1,pp.1:1–1:38, Dec.2016.doi:http://doi.acm.org/10.1145/2996195

[5] M.DiFrancesco,S.K.Das,andG.Anastasi,"Datacollectioninwirelesssensornetworkswith mobile elements:A survey,"*ACM Trans. Sen. Netw.*, vol. 8, no. 1, pp. 7:1–7:31, Aug. 2011. doi:http://doi.acm.org/10.1145/1993042.1993049

[6] C. Liu, D. Fang, X. Liu, D. Xu, X. Chen, C.-J. M. Liang, B. Liu, and Z. Tang, "Low-cost and robustgeographicopportunisticroutinginastriptopologywirelessnetwork,"*ACMTrans. Sen. Netw.*,vol.15,no.2,pp.24:1–24:27,Mar.2019.doi:http://doi.acm.org/10.1145/3309701

[7] S. Tullimas, T. Nguyen, R. Edgecomb, and S.-c. Cheung, "Multimedia streaming using multipletcpconnections,"*ACMTrans.MultimediaComput.Commun.Appl.*,vol.4,no.2,pp.12:1–12:20,May2008.doi :http://doi.acm.org/10.1145/1352012.1352016

[8] S.Yoon,C.Veerarittiphan,andM.L.Sichitiu,"Tiny-sync:Tighttimesynchronization for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 3, no. 2, Jun. 2007. doi: http://doi.acm.org/10.1145/1240226.1240228

[9] M. Xu, W. Xu, T. Han, and Z. Lin, "Energy-efficient time synchronization in wireless sensor networks via temperature-aware compensation," *ACM Trans. Sen. Netw.*, vol. 12, no. 2, pp. 12:1–12:29,Apr.2016.doi:http://doi.acm.org/10.1145/2876508

[10] E.Popovici,M.Magno,andS.Marinkovic,"Powermanagementtechniquesforwirelesssensor networks:Areview,"*5thIEEEInternationalWorkshoponAdvancesinSensorsandInterfaces (IWASI)*, vol. 47, no. 6, pp. 194–198, Jun. 2013.

[11] Y. Gui, Z.-g. Tao, C.-j. Wang, and X. Xie, "Study on remote monitoring system for landslide hazard based on wireless sensor network and its application," *Journal of Coal Science and Engineering (China)*, vol. 17, no. 4, pp. 464–468, 2011. Y.Wang,W.Chu,S.Fields,C.Heinemann,andZ.Reiter,"Detectionofintelligentintruders inwirelesssensornetworks,"*FutureInternet*,vol.8,no.1,p.2,2016.

12 R. Yueqing and X. Lixin, "A study on topological characteristics of wireless sensor network basedoncomplexnetwork," in*2010InternationalConferenceonComputerApplicationand System Modeling (ICCASM 2010)*, vol. 15.IEEE, Oct 2010, pp. V15–486–V15–489.

13 R.S.BishtandS.K.Budhani,"Performanceanalysisofhierarchicalandnonhierarchicalrouting techniquesinwirelesssensornetworks," in*Soft ComputingTechniques forEngineering and Technology (ICSCTET), 2014 International Conference on*.IEEE, Aug 2014, pp. 1–8.

14 L. Liu, H. Ma, and X. Zhang, "Analysis for localization-oriented coverage in camera sensor networks,"in*ProceedingsofWirelessCommunications&NetworkingConference*.NewYork, USA: IEEE, Mar. 2008, pp. 2579–2584.

15 A. A. Ahmed, H. Shi, and Y. Shang, "A survey on network protocols for wireless sensor net-works,"in*InformationTechnology:ResearchandEducation,2003.Proceedings.ITRE2003. InternationalConferenceon*,Aug2003,pp.301–305.

16 P.DeshpandeandM.S.Madankar,"Techniquesimprovingthroughputofwirelesssensornetwork:Asurvey,"in*Circuit,PowerandComputingTechnologies(ICCPCT),2015International Conference on*.IEEE, March 2015, pp. 1–5.

17 B.Li,H.Li,W.Wang,Q.Yin,andH.Liu,"Performanceanalysisandoptimizationforenergy-efficientcooperativetransmissioninrandomwirelesssensornetwork,"*IEEETransactionson Wireless Communications*, vol. 12, no. 9, pp. 4647 – 4657, 2013.

18 L.Brisolara,P.R.Ferreira,andL.S.Indrusiak,"Applicationmodelingforperformanceevalu- ation on event-triggered wireless sensor networks,"*DesignAutomationforEmbeddedSystems*,pp.1–19,2016.

19 S.K.Chong,M.M.Gaber,S.Krishnaswamy,andS.W.Loke,"Energyconservationinwireless sensor networks: arule-basedapproach, "*KnowledgeandInformationSystems*,vol. 28,no. 3,pp.579–614,2011.

20 J.AiandA.A.Abouzeid,"Coveragebydirectionalsensorsinrandomlydeployedwirelesssensor networks," *Journal of Combinatorial Optimization*, vol. 11, no. 1, pp. 21–41, 2006.

21 D. Eid, A. Yousef, and A. Elrashidi, "Ecg signal transmissions performance over wearable wirelesssensornetworks," *ProcediaComputerScience*,vol.65,pp.412–421,2015.

22 A.S.K.Mammu,U.Hernandez-Jayo,N.Sainz,andI.delaIglesia,"Cross-layercluster-based energy-efficientprotocolforwirelesssensornetworks," *Sensors*,vol.15,no.4,p.8314,2015.

23 N. M. Boers, P. Gburzyński, I. Nikolaidis, and W. Olesiński, "Developing wireless sensor network applicationsinavirtualenvironment," *TelecommunicationSystems*,vol.45,no.2,pp.165–176, 2010.

24 C.MaandY.Yang,"Battery-awareroutingforstreamingdatatransmissionsinwirelesssensornetworks,"in*2ndInternationalConferenceon BroadbandNetworks,2005*. IEEE,Oct2005, pp.464–473 Vol. 1.

25 .S.Emami,"Batterylifetimeofcoincelloperatedwirelesssensornetworks,"in*2014IEEE11thConsumerCommunicationsandNetworking Conference (CCNC)*,Jan2014,pp.7–10.

26. ——, "Parallel battery configuration for coin cell operated wireless sensor networks," in *2013 IEEE24thAnnualInternationalSymposiumonPersonal,Indoor,andMobileRadioCommu- nications (PIMRC)*, Sept 2013, pp. 2317–2320.

27. T. Qiuling, L. Ye, Q. Yongming, and W. Huan, "Joint scaling of battery discharge and modu-lationschemeinwirelesssensornetworks,"in*ComputerScienceandEducation(ICCSE),2010 5th International Conference on*,Aug2010,pp.1689–1693.

28. R. Anane, K. Raoof, M. B. Zid, and R. Bouallegue, "Optimal modulation scheme for energy efficient wireless sensor networks,"in *Wireless Communications, Networking and Mobile Com- puting (WiCOM 2014), 10th International Conference on*.IEEE, Sept 2014, pp. 500–513.

29. G. Joshi, S. Jardosh, and P. P. Ranjan, "Bounds on dynamic modulation scaling for wireless sensornetworks," in*WirelessCommunicationandSensorNetworks,2007.WCSN'07.Third International Conference on*.IEEE, Dec 2007, pp. 13–16.

30. Y. Chen, J. Cheng, H. Yang, and B. Liu, "Research on a wireless sensor network's modulation basedonultrawidebandsignals,"in*2010InternationalConferenceonComputer,Mechatronics, Control and Electronic Engineering*, vol. 5.IEEE, Aug 2010, pp. 1–4.

31. A. Mota,L. B. Oliveira,F. F. Rocha,R. Riserio,A. A. F. Loureiro,C. J. N. Coelho,H. C. Wong,andE.Nakamura,"Wisenep:Anetworkprocessorforwirelesssensornetworks,"in*11th IEEESymposiumonComputersandCommunications(ISCC'06)*,June2006,pp.8–14.

32. Y. Xu, L. Liu, P. Shen, T. Lv, and X. Li, "Processor design considerations for wireless sensor network,"in*20056thInternationalConferenceonASIC*,vol.1.IEEE,Oct2005,pp.212–214.

33. L.Liu,P.Shen,T.Lv,andX.Li,"Lowpowerprocessordesignforwirelesssensornetworkapplications,"in*Proceedings.2005InternationalConferenceo nWirelessCommunications,Net- workingandMobileComputing,2005.*,vol.2.IEEE,Sept2005,pp.921–924.

34. C. Gu, G. U. Caidong, and F. Ling, "Calculation and simulation of transient optimal voltage outputpointinwirelesssensornetworks," *TheJournalofSupercomputing*,vol.72,no.7,pp. 2767–2781, 2016.

35. E. Yoon and K.-S. Yun, "Development of a wireless environmental sensor system and mems- based rf circuit components," in *The 13th International Conference on Solid-State Sensors, ActuatorsandMicrosystems,2005.DigestofTechnicalPapers.TRANSDUCERS'05.*,vol.2. IEEE, June 2005, pp. 1981–1985 Vol. 2.

36. Y.Cho,Y.Kim,andN.Chang,"Pvs:passivevoltagescalingforwirelesssensornetworks,"in*LowPowerElectronicsandDesign(ISLPED),2007ACM/IE EEInternationalSymposiumon*,Aug2007,pp.135–140.

37. L.B.Hörmann,P.M.Glatz,C.Steger,andR.Weiss,"Evaluationofcomponentawaredynamicvoltagescalingformobiledevicesandwirelesssensornetw orks,"in*WorldofWireless,Mobile andMultimediaNetworks(WoWMoM),2011IEEEInternationalSymposiumona*,June2011,pp.1–9.

38. T. Le and M. W. Mutka, "A lightweight block validation method for resource-constrained IoT devicesinblockchain-basedapplications,"in*2019IEEE20thInternationalSymposiumon"A WorldofWireless,MobileandMultimediaNetworks"(WoWMoM)*, June 2019, pp. 1–9. doi: https://doi.org/10.1109/WoWMoM.2019.8792979

39. M. Ángel Prada-Delgado,I. Baturone,G. Dittmann,J. Jelitto,and A. Kind,"PUF-derived IoT identities in a zero-knowledge protocol for blockchain," *Internet of Things*, p. 100057, 2019.doi:https://doi.org/10.1016/j.iot.2019.100057

40. I.Baturone,M.A.PradaDelgado,andS.Eiroa,"Improvedgenerationofidentifiers,secretkeys,andrandomnumbersfromsrams,"*IEEETransactionsonI nformationForensicsandSecurity*,vol.10,no.12,pp.2653–2668,Dec2015.doi:https://doi.org/10.1109/TIFS.2015.2471279

41. S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework forsecuretransactionsinIoT,"*IEEEInternetofThingsJournal*,vol.6,no.3,pp.4650–4659,June2019.doi: https://doi.org/10.1109/ JIOT.2018.2874095

42. J. Gong, Y. Mei, F. Xiang, H. Hong, Y. Sun, and Z. Sun, "A data privacy protection schemefor internet of things based on blockchain," *TransactionsonEmergingTelecommunications Technologies*,vol.n/a,no.n/a,p.e4010.doi:https://doi.org/10.1002/ett.4010

43. A.Meloni,S.Madanapalli,S.K.Divakaran,S.F.Browdy,A.Paranthaman,A.Jasti, N. Krishna, and D. Kumar, "Exploiting the IoT potential of blockchain in the IEEE P1931.1 ROOFStandard," *IEEECommunicationsStandardsMagazine*,vol.2,no.3,pp.38–44,Sept 2018.doi:https://doi.org/10.1109/MCOMSTD.2018.1800019

44. N. Kathayayani, J. K. Murthy, and V. N. Naik, "Hyperledger fabric blockchain for data securityinIoTdevices,"*InternationalJournalofRecentTechnologyandEngineering(IJRTE)*, vol. 9, no. 1, pp. 2571–2577, May 2020. doi:https://doi.org/10.35940/ijrte.A3040.059120

45. M. S. Hossain, S. Waheed, Z. Rahman, S. A. Shezan, and M. M. Hossain, "Blockchain for the securityofinternetofthings:Asmarthomeusecaseusingethereum," *InternationalJournal ofRecentTechnologyandEngineering(IJRTE)*,vol.8, no.5, pp.4701–4608, Jan2020.doi: https://doi.org/10.35940/ijrte.E6861.018520

46. Y. Zhang, Y. Han, and J. Wen, "SMER: a secure method of exchanging resources in heterogeneousinternetofthings,"*FrontiersofComputerScience*,vol.13,no.6,pp.1198–1209, Dec2019.doi:https://doi.org/10.1007/s11704-018-6524-3

47. Y.A.Qadri,R.Ali,A.Musaddiq,F.Al-Turjman,D.W.Kim,andS.W.Kim,"Thelimitationsinthestate-of-the-artcounter-measuresagainstthesecuritythreatsinH-IoT," *ClusterComputing*,Jan2020.doi:https://doi.org/10.1007/s10586-019-03036-7

Book –

48. https://pg.its.edu.in/sites/default/files/KCA043%20Internet%20of%20things%20-IoT%20by%20Raj%20Kamal%20Text%20Book.pdf

49. https://aitskadapa.ac.in/ebooks/CSE/IOT/Internet%20of%20Things_%20Architectures,%20Protocols%20and%20Standards%20(%20PDFDrive%20).pdf

50. https://mrcet.com/downloads/digital_notes/EEE/IoT%20&%20Applications%20Digital%20Notes.pdf