International Journal of Computer Sciences and Engineering
Vol.11, Special Issue.1, pp.243-248, November 2023
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

Research Paper

A Comprehensive Study of Various Challenges and Constraints in Wireless Sensor Networks (WSNs)

Sucheta Panda[1*], Sushree Bibhuprada B. Priyadarshini[2]

[1]Computer Science and Engineering, SOA University, Bhubaneswar, India
[2]Information and Technology, SOA University, Bhubaneswar, India

**Corresponding Author: suchetapanda10@gmail.com*

Abstract: Numerous applications are possible for Wireless Sensor Networks (WSNs). However, there are a number of implementations where the sensor data is useless and may lead to an false analysis of the provided information, especially if the coordinates information is unknown. Because of this, localization is crucial to many WSN operations. The problems and difficulties preventing the position of the sensor nodes in WSNs are thoroughly examined in this research. The fundamental concept behind a sensor network is to disperse tiny sensing devices which is capable of detecting changes in incidents or parameters and interacting with other devices over a defined geographic area for a variety of objectives, such as target tracking, vigilance, and environmental tracking. It is profitable to be utilized in great abundance in the future by integrating sensor technologies with computing power and wireless connectivity. A variety of security risks are also brought on by the use of wireless communication technology. In this essay, issues and difficulties with wireless sensor networks are surveyed.

Keywords: Wireless Sensor Network, Localization, Sensor node, Network, Sensing devices, Environment monitoring

1. Introduction

While sensor networks have a lot in common with other distributed systems, they also have their own set of challenges and limits. The design of a WSN is influenced by these constraints, resulting in protocols and algorithms that differ from those used in other distributed systems. In this section, the most significant design restrictions for a WSN are discussed. The creation of inexpensive, low-power, multipurpose tiny devices for use in distant sensing applications has been made possible by recent advancements in the area of electronics and wireless communication. Combining these elements has increased the possibility of using a sensor network made up of a lot of intelligent sensors, allowing for the gathering, processing, examining, and dispersing of useful information gathered in various situations. These sensor nodes are employed to keep an eye out for activity in the environment and transmit the sensory data to the Base station (BS) , also known as the sink [1].

An extensive network of sensor nodes that can sense, analyse data, and communicate together makes up a sensor network. Figure 1. depicts the architecture of WSN.

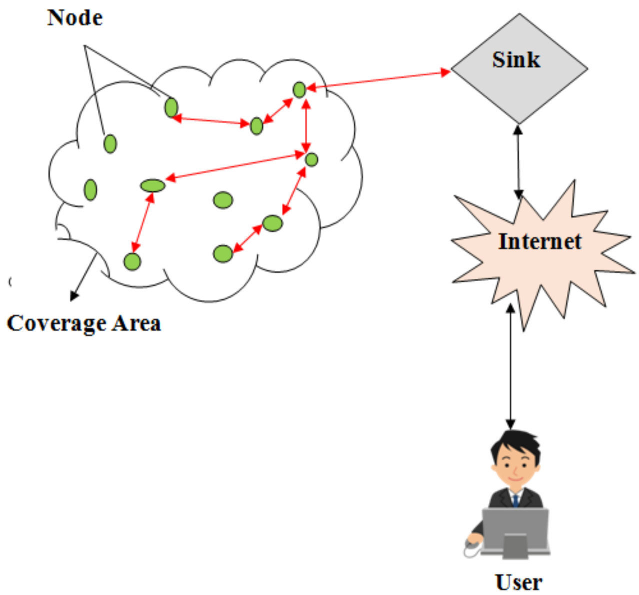

Figure 1. An overview of WSN Architecture

2. Related Work on Various Type of Constraints

2.1 Design Constraints

When compared to traditional computing systems, which are always improving, wireless sensor design's primary goal is for creating smaller, less expensive, and more efficient devices. Sensor nodes have processing and storage speeds that are comparable to those of decades-old computer systems because they must run specialized programmes with little energy consumption. Since they must have a small form factor and use little energy, many desirable components, including GPS receivers, cannot be used. At several levels, these constraints and requirements affect how software is designed. For instance, operating systems must effectively manage resources and have tiny memory footprints. The development of compact and effective operating systems is made simpler by the absence of sophisticated hardware characteristics (such as support for parallel executions) [1-5]. Different protocols and algorithms utilized in a WSN are designed taking into account the hardware limitations of a sensor. The memory of a sensor might not be able to store routing tables, for instance, which have entries for every probable network destination. The memory of a sensor node having a limited capacity to store data is an alternative (such as a list of neighbors). While it is possible to employ in-network processing to minimize duplicate data. More processing power and storage may be needed for some sensor aggregation and fusion activities than can be provided by inexpensive sensor nodes. As a result, various OS, middleware, and network protocol designs and solutions need to be created to operate effectively on hardware with constrained resources. Figure. 2 shows the constraints of WSN in detail.

2.2 Security

Sensitive data is collected by many wireless sensor networks. Sensor nodes are more vulnerable to hostile intrusions and attacks when they operate remotely and unmanaged. Furthermore, wireless connections make eavesdropping on sensor transmissions simpler for an opponent. For instance, a DoS attack, which seeks to stop a sensor network from functioning properly, is the challenging issues. A jammer attack, which interferes with sensor communications by using powerful wireless broadcasts, is one method that can be used to do this. Depending on how the sensor network is being used, the repercussions may be severe. There are a variety of distributed systems strategies and techniques that can prevent assaults or lessen their impact, but many of them have high computation, communication, and storage demands that resource-constrained sensor nodes cannot fulfill. In order to generate and distribute keys, authenticate nodes, and maintain secrecy in sensor networks, specific methods must be used [6-13].

2.3. Decentralized Management

Many WSNs are too large and resource-constrained to use centralized algorithms to carry out network management activities like topology maintenance or routing (for example, at the Base station(BS)). Instead of having access to global data, to produce judgements that are localized, sensor nodes must collaborate with their neighbours. Therefore, while the outcomes of these distributed (or decentralized) algorithms won't be flawless, they might be more energy-efficient than centrally located ones. As an example, consider routing for both centralized and decentralized strategies. A BS can gather data from all sensor nodes, select the best paths (for instance, in terms of energy usage), and communicate the nodes' paths to one another. Instead, a decentralized strategy enables each node to pick its own course based on sparse local data(for instance a list of neighbors and their distance from the base station) Administrative costs are significantly reduced, notwithstanding the possibility that this decentralized technique will produce less-than-ideal routes[1, 13-17].

2.4. Ad Hoc deployment

Individual sensor node placements don't always need to be designed and engineered for wireless sensor network applications. This is crucial for networks built in isolated or challenging-to-access locations. When sensors are dropped over the appropriate areas, such as during war or disaster assessment [18-36]. It's possible that many of the sensor nodes won't survive and won't ever be able to start performing their detection tasks. In contrast, the remaining nodes must individually complete a range of setup and configuration tasks, including as connecting to other adjacent sensor nodes, picking their placements, and beginning their sensing duties. Depending on this knowledge, sensor nodes' production and transmission of different kinds and quantities of information on behalf of other nodes may differ. The quantity and kind of the information that a node generates and transmits, for instance, may depend on its location and the number and identities of its neighbours.

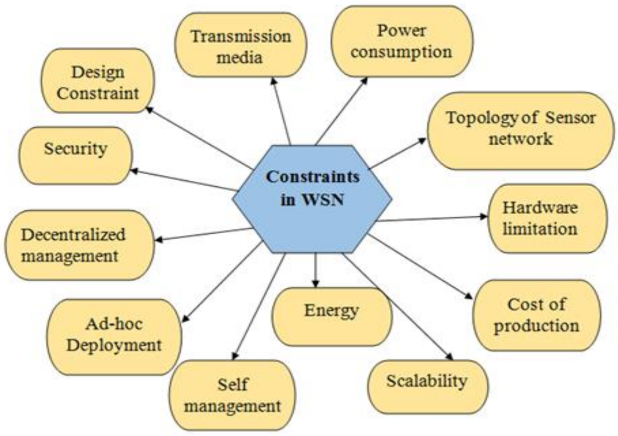

Figure 2. Types of Constraints in WSN

2.5. Self-Management

Many sensor network applications lack infrastructure support and maintenance and repair choices and are made to operate in severe environments and remote locales. As a result, sensor nodes must be able to self-manage. A node needs to be able to configure itself, run, interact with other nodes, and adapt on its own to failures, environmental changes, and changes in ambient stimuli in order to be considered self-managing.

2.6. Energy

The constrained energy budgets of the sensor nodes are the primary restriction on the construction of sensor networks. They typically run on batteries, which must be changed out or replenished (for instance, using solar power) when they run low. Some nodes will be destroyed if their energy supply runs out because neither option is adequate for them. The energy consumption strategy is significantly impacted by whether the battery can be recharged. Non-rechargeable batteries should be able to power a sensor node until the mission timer expires or a new battery can be installed. Therefore, for a WSN, energy efficiency is frequently the first and biggest design problem. The architecture of sensor nodes and networks as a whole are impacted by this requirement. According to Sinha and Chandrakasan (2000), the two main causes of energy consumption in CMOS-based processors are switching energy and leakage energy.

$$E_{CPU} = E_{switch} + E_{leakage} = C_{total}V_{dd}^2 + V_{dd}I_{leak}\Delta t$$

Where C_{total} is the amount of capacitance that was switched overall during the computation,

$V_{dd} = Supply\ voltage$

$I_{leak} = Leakage\ current$

$t = computation\ period$

Even if the energy transition is ongoing to account for the majority of processor energy consumption, leakage energy is predicted to overtake switching energy in the future (De and Borkar 1999). Leakage energy control techniques include two examples: software-based solutions like Dynamic Voltage Scaling and gradual shutdown of idle components (DVS). Accessing the wireless channel for sensor nodes is the responsibility of the MAC layer. All of these approaches have downsides, such as energy costs, collision-related delays, and recovery-related delays, as well as the potential need for sensor nodes to continuously monitor the medium to ensure that no transmissions are lost.

The demand for energy efficiency has an impact on everything from small memory footprints to efficient task switching, middleware, security measures, and even the programmes themselves. To combine many sensor inputs or remove extraneous sensor data, In-network processing, for instance, is often used. Due to the trade-off between computing (processing sensor data) and transmission (sending processed data rather than raw data), it is possible to reduce energy. The following are the specific design issues in WSNs, according to Matin and Islam [22].

2.7. Scalability

SNs can range in size from a handful to several hundreds of nodes. The deployment density can also be changed appropriately. The high-resolution data collecting technique may cause the node density to increase to the point where each node has a large number of neighbours within its transmission range. These degrees of scalability and performance preservation should be supported by the protocols employed in SNs.

2.8 Cost of Production

Only if the specific SNs could be created at an affordable price could sensor networks potentially compete with conventional information gathering techniques, as different deployment models view SNs as disposable devices. An NS should have a target price that is as low as is practical.

2.9 Hardware Limitations

Each NS must include a power source component, processing component, transmission component, and sensor component for detection. The nodes may have a large number of internal sensors or other components, such as a localization setup, that at some point aid in location-aware routing. Despite this, each extra feature has a price and expands the node's size and rate of power consumption. Therefore, the cost and power requirements must always be compared to the added capability.

3.Research Methodology

3.1 Research queries

1. It is necessary to develop new network protocols that take into account the essential features of wireless communication. More research is required to:
2. Measure and evaluate how wireless communication theoretical features are manifested in today's and tomorrow's sensing and communication equipment.
3. Create innovative network protocols that take into consideration the communication challenges of real-world contexts.
4. Individual solutions are tested on real platforms in real-world scenarios, and unique solutions are synthesized into a whole protocol stack for the entire system for a genuine application.

3.2 Source of Information

- Science Direct ()
- ACM Digital Library ()
- Google Scholar ()
- IEEE Xplore ()

3.3 Research Keywords

The following table 1 shows the keyword and synonyms and Figure 3 shows the way of doing research for this paper.

Table 1: Synonyms and search terms

Keywords	Synonyms
WSN	Wireless Sensor Network
WSN Protocols	Wireless Sensor Network protocols
SNS	Sensor network services
Survey	Issues and reviews

3.4 Research selection

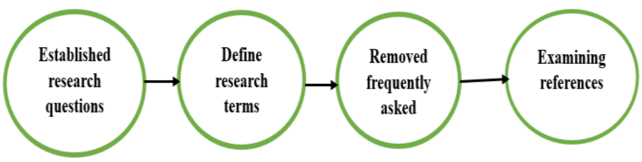

Figure 3. Methodology of research

4. Theoretical Discussion

Although WSNs have made progress in a number of areas, they still have resource constraints in terms of their ability to communicate, store data, process data, and store data. Among the aforementioned restrictions, energy resource management is of paramount importance, as seen by the abundance of algorithms, techniques, and protocols developed for energy conservation since the network's beginnings according to reports [23].

4.1 The Media of Transmission

Most of the time, nodes interact and communicate via radio on the well-known ISM bands. While infrared communication has the advantages of being reliable and interference-free, other sensor networks use optical or infrared communication.

Table 2: Types of WSN with challenges

Categories	Number of Nodes	Disposition	Cost	Challenges
Terrestrial WSN(TWSN)	Inexpensive nodes from hundreds to thousands	Ad-hoc or Pre planned Manner	Less costly	Grid, optimum, placement of Three dimensional models in preplanned TWSN are challenging to implement
Underground WSN (UgWSN)	Few number of nodes than TWSN	Setting up in mines or caves	Greater cost than TWSN	It is challenging to deploy and gather data.
Mobile WSN(MoWSN)	Positioned in large numbers	Movement, self-configuration, and physical environment sensing capabilities	High Cost	Effective coverage of the sensing region, localization, self-configuration, deployment
Multimedia WSN(MuWSN)	A number of inexpensive sensor nodes with cameras and microphones	Scheduled deployment to guarantee adequate coverage Retrieval and compression of data are made simple by effective deployment	High Cost	High energy and bandwidth demands Cross-layer design, QOS provisioning, and compression strategies

4.2 The Consumption of Power

As was already said, a lack of power supplies was the main cause of most WNS problems. The power source's size is constrained by the node's size (battery). As a result, when designing the software and hardware, issues of efficient energy usage must be properly taken into account. The amount of energy required for radio transmission, for instance, may decrease as a result of data compression, but processing, calculation, and/or filtering still require additional energy. Sensor networks provide a powerful combination of dispersed sensing, processing, and communication, according to Puccinelli and Haenggi [24]. Due to their special characteristics, they bring up a world of opportunities but also present a number of challenges, most notably the stringent energy limitations that sensor networks are prone to. While infrared communication has the advantages of being dependable and interference-free, other sensor networks rely on optical or infrared transmission. Many HWD platforms have been developed in order to assess the large ideas and concepts generated by various researchers and to successfully develop applications that suit all fields of study, notably those in science and technology [25].

There are a variety of programming methods that have been proposed, with an emphasis on low-level systems, to build and implement WSNs. According to BenSaleh et al. [26], who assert that using the model-driven engineering (MDE) technique is proving to be a particularly favourable option, these HLB methodologies would be highly valuable in easing the design and deployment of WSNs as well as minimising some of the problems.

5. Results and Discussion

This article presents several research problems and difficulties related to WSNs that the researchers have encountered. Despite their many difficulties, sensor networks have a wide range of applications that entice researchers to learn more about them. An Investigations into WSN have shown that it is a diverse field. It requires scalable architecture from hardware engineers to assure high quality of service and energy-efficient protocols and algorithms from software programmers to make them workable and practicable. One of the key concerns is energy conservation, and diverse study topics ultimately come down to trying to limit it at all costs. In order to make Wireless Sensor Network a reality, the research community should take a comprehensive strategy and work together. These initiatives are worthwhile because WSNs have the potential to benefit humanity as a whole and to enable pervasive computing in the future.

Wireless sensor networks have gotten increasingly sophisticated as a result of aspects such as node implementation, protection, and authenticity. This research adds to showcasing wireless sensor network applications, attacks, and challenges. Much research has gone into the development of systems and technologies that work with WSN to improve the quality of that specific region. This research focuses on the many locations where the WSN is used. WSN is being used to improve efficiency in the military, agriculture, and hospitals, among other places. This article outlines many WSN attacks and problems.

6. Conclusion and future scope

Small nodes that have the ability to sense, assess, and interact wirelessly make up Wireless Sensor Networks (WSNs). Numerous routing, power management, and information dissemination protocols have been created especially for WSNs where energy consciousness is a crucial architecture consideration. As a relatively new area of study, there is a lot of effort being done to address numerous outstanding problems in wireless sensor networks. Wireless sensor networks have several limitations that need to be fixed since some fundamental hardware issues, particularly those relating to energy supply and miniaturisation, have not yet been fully resolved. The current research makes an effort to give a thorough and in-depth analysis of the problems and challenges associated with the localization of the sensor nodes in WSNs. As more and more sensor networks are deployed, and as the applications become more and more diverse, cooperative localization research will continue to expand. According to the WSN application spectrum, there is a wide range of research opportunities because different applications require different protocols and resources, such as those used in building automation, wearable technology, medical management, mechanical, automobile, oil and gas, retail, agriculture and defence. Self-Management, Decentralised Management, Fault-Tolerance, and Scalability are the most important specific difficulties and limitations that have an impact on the architecture of a WSN, according to our article. We provide a few areas of study related to wireless sensor networks at the conclusion of this essay. In order to prevent these variables from negatively affecting WSN networks in the future, they are given in this study along with potential remedies. There are some security solutions also available:

- 802.15.4
- Zigbee
- Bluetooth
- Tiny Sec
- Mini Sec
- Spin
- AM Secure
- Sizzle

Conflict of Interest
The authors declare no conflict of interest.

Funding source
This research received no external funding.

Authors' contribution
All the authors have equal contribution in drafting the manuscript.

Acknowledgements
The authors are really very appreciative to the Siksha 'O' Anusandhan University for affording the support to make this investigation successful.

References

[1]. Marcelloni, F., & Vecchio, M. "Exploiting Multi–Objective Evolutionary Algorithms for Designing Energy–Efficient Solutions to Data Compression and Node Localization in Wireless Sensor Networks". In Evolutionary Based Solutions for Green Computing, Springer, Berlin Heidelberg, pp. 227-255,2013.
[2]. Tiwari P, Saxena VP, Mishra RG, Bhavsar D, "Wireless sensor networks: Introduction, advantages, applications and research challenges", HCTL Open International Journal of Technology Innovations and Research.,vol.14, pp.1-11,2015.
[3]. Di, Ma, and ErMeng Joo. "A survey of machine learning in wireless sensor networks from networking and application perspectives." In Information, Communications & Signal Processing, 6th International Conference on. IEEE, pp. 1-5, 2007.
[4]. Akyildiz, Ian F., et al. "A survey on sensor networks." IEEE communications magazine, Vol. **40**, Issue **8**, pp.102-114,2002.
[5]. B. Charan Patel, G. R Sinha and Naveen Goel, "Introduction to sensors", Advances in Modern Sensors, IOP publishing, pp. 1-21, 2020.
[6]. S. Manish Kumar; Amin, Syed Intekhab; Imam, Syed Akhtar; Sachan, Vibhav Kumar; Choudhary, Amit "A Survey of Wireless Sensor Network and its types", International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) ,IEEE, Noida, pp. 326–330,2018.
[7]. A. Abdelhakim , B. Bouhorma, M. B. Mohamed, "New Technique of Wireless Sensor Networks Localization based on Energy Consumption", International Journal of Computer Applications (0975 – 8887), Volume 9, Issue 12, pp.25-28 , 2010. doi:10.5120/1436-1935.
[8]. R. Ahmad, R. Wajirali, T. Abu-Ain," Machine Learning For Wireless Sensor Networks Security: An Overview Of Challenges And Issues", Vol 22, Issue 13, pp.1-35 ,2022, https://doi.org/10.3390/s22134730.
[9]. Bouaziz, M., & Rachedi, A. (2016). A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. Computer Communications, Vol 74, pp. 3–15. doi:10.1016/j.comcom.2014.10.004
[10]. Wood AD,L.Fang,R.Stoleru,"Context-aware wireless sensor networks for assisted living and residential monitoring", IEEE Network, Vol 22,Issue 4,pp. 26-33,2008.
[11]. Ahmad Abed ,Alhameed Alkhatib, Gurvinder Singh Baicher,"Wireless Sensor Network Architecture", International Conference on Computer Networks and Communication Systems(CNCS 2012),IPCSIT IACSIT Press, Singapore, pp. 1-6,2011.
[12]. Buratti C, Conti A, Dardari D, Verdone R. "An overview on wireless sensor networks technology and evolution". Sensors, Vol. 9, Issue 9, pp. 6869-6896, 2009, https://doi.org/10.3390/s90906869.
[13]. L., Liu, Q., Shao, J., & Cheng, Y. "Distributed Localization in Wireless Sensor Networks Under Denial-of-Service Attacks". IEEE Control Systems Letters. Vol. 5, Issue 2, pp. 493-498, 2021, doi: 10.1109/lcsys.2020.3003789.
[14]. K. Sharma, M K Ghose. Wireless Sensor Networks: "An Overview on its Security Threats". IJCA Special Issue on "Mobile Ad-hoc Networks ,pp. 42-45, 2010, doi:10.5120/1008-44.
[15]. Newsome, J., E. Shi, D. Song, and A. Perrig. "The Sybil Attack in Sensor Networks: Analysis and Defenses." In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, India, pp. 1259-1268,2004.
[16]. Douceur, J. "The Sybil Attack." In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge Massachusetts, USA, Springer LNCS, pp. 251-260,2002.
[17]. Michael Healy, Thomas Newe, Elfed Lewis Optical Fibre Sensors Research Centre, "Security for Wireless Sensor Networks: A Review", SAS 2009 IEEE Sensors Applications Symposium New Orleans, pp. 1-7 , 2009.
[18]. Hassan Ali, Abdullah Al Mamun, Sultan Anwar, "All Possible Security Concern and Solutions of WSN: A Comprehensive Study", Vol.6, Issue 4, pp. 64-74, 2015.
[19]. Al-Sakib Khan Pathan , Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Vol. 1, pp. 1043-1048,2006.
[20]. Anitha S.Sastry, Shazia Sulthana and Dr.S Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer", International Journal of Advanced Networking and Applications, Vol. 04 ,Issue 04, pp. 1657-1661, 2013.
[21]. D.L., Nguyen, T.K., Nguyen, T.V., Nguyen, T.N., Massacci, F. and Phung, P.H., "A convolutional transformation network for malware classification". 6th NAFOSTED conference on information and computer science (NICS) ,IEEE, pp. 234-239,2019.
[22]. Deng, J., R. Han, and S. Mishra. "Counter measures against Traffic Analysis in Wireless Sensor Networks." Security and Privacy for Emerging Areas in Communications Networks, IEEEExplore,pp.1-13,2005,doi:10.1109/securecomm.2005.16.
[23]. Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks Journal, Vol.1, Issue 2-3, pp. 293-315, 2003, doi:10.1016/s1570-8705(03)00008-8.
[24]. Yan Sun, Zhu Han, and K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks," IEEE

Communications Magazine, Vol 46, Issue 2, pp.112-119, 2008,doi: 10.1109/mcom.2008.4473092.

[25]. Puccinelli D, Haenggi M. “Wireless sensor networks: Applications and challenges of ubiquitous sensing”, IEEE Circuits and Systems Magazine. Vol 5, Issue 6, pp.19-29,2005.

[26]. V. Thiruppathy Kesavan and S. Radhakrishnan, “Secret Key Cryptography Based Security Approach for Wireless Sensor Networks”, International Conference on Recent Advances in Computing and Software Systems, IEEE, pp. 185-191,2012.

[27]. K. Sharma, M.K. Ghose, D. Kumar, R. P. Kumar Singh, V.K Pandey. “A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks”. In IJAST, Vol. 7, pp. 31-44, 2010.

[28]. Hamid, M. A., Rashid, M-O., and Hong, C. S., “Routing Security in Sensor Network: Hello Flood Attack and Defense”, IEEE ICNEWS ,Vol 2, pp. 2-4,2006.

[29]. Nath MP, Priyadarshini SB, Mishra D, “A comprehensive study on security in IoT and resolving security threats using machine learning (ML)”, In Advances in Intelligent Computing and Communication, Proceedings of ICAC ,pp. 545-553,2021

[30]. Priyadarshini SB, Bagjadab AB, Mishra BK, ”Digital signature and its pivotal role in affording security services”, In Handbook of e-Business Security,1st edition, Auerbach Publications,India,pp.365-384,2018,ISBN:9780429468254.

[31]. Priyadarshini SB, Bagjadab AB, Mishra BK. “Security in distributed operating system: A comprehensive study”, Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies,Wiley-Scrivener publisher, pp. 221-30, 2019, ISBN: 9781119488057.

[32]. Priyadarshini SB.,”A Comprehensive Study of Security in Electronic Commerce Frameworks in the Modern Era of Technology”, In Artificial Intelligence and Cybersecurity,1st edition, CRC press, India, pp. 121-140, 2022, ISBN9781003097518.

[33]. Dasmohapatra S, Priyadarshini SB,” A Comprehensive Study on SQL Injection Attacks, Their Mode, Detection and Prevention”,In Proceedings of Second Doctoral Symposium on Computational Intelligence: DoSCI ,pp. 617-632,2022.

AUTHORS PROFILE

Sucheta Panda earned B. Tech., M. Tech., from BPUT, Odisha in 2014 and Utkal University, Bhubaneswar in 2017 respectively. Sucheta is pursuing PhD in Computer Science and Engineering. Few review papers based on Cryptography and Wireless sensor network have also been published. Basically my research domain focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Data Mining, IoT and Wireless Sensor Network. I have 4 years of teaching experience and 1 year of research experience.

Sushree Bibhuprada B. Priyadarshini earned her B. Tech. from BPUT, Orissa in 2011, M. Tech. from S’O’A University in 2013, BBSR and Ph. D. from VSSUT, Burla, Odisha in 2018. She was the branch topper in her M. Tech. and Dr. Priyadarshini is employed as an Assistant Professor in the ITER Department of Computer Science from SOA’ University, Bhubaneswar since 2018.She is a member of IEEE CSTA, IEEE, IAENG, SDIWC, IJERT, IEDRC. She has published more than 50 research papers in renowned international journals incorporating Thomson Reuters, SCI, Web of Science and various conferences including IEEE. Her main research profile emphasizes on Wireless Sensor Network.