Defense Strategy Security Mechanism for Sensor Networks

Rakesh Nayak[1](✉), Jitesh Shinde[2], Praveen Gupta[5], Satyabrata Dash[3], Umashankar Ghugar[1], and Lokendra Singh[4]

[1] Department of CSE, OP Jindal University, Raigarh, India
nayakrakesh8@gmail.com, ughugar@gmail.com
[2] Department of Electronics Engineering (VLSI Design and Technology), CSMSS Chh Shahu College of Engineering, Chh. Sambhajinagar (Aurangabad), Maharashtra, India
[3] Department of Computer Science and Engineering GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, India
[4] Department of Electronics and Communication Engineering, Graphic Era (Deemed to be University), Dehradun, Uttrakhand, India
[5] Department of Computer Science and Engineering, Jaipur National University, Jaipur, India

Abstract. This paper examines the safety measures used in sensing unit networks, focusing on their effectiveness in securing critical applications from threats like unapproved access, information violations, and meddling. It assesses the current state of these devices, identifies their weaknesses and strengths, and identifies obstacles such as source restrictions, scalability, and ease of access to risks. The paper emphasizes the importance of cooperation and data sharing among countries in reinforcing protection technique safety devices. The review concludes with a call to action, emphasizing the need for continuous research, innovation, and policy frameworks to address the evolving security landscape and protect critical infrastructure.

Keywords: Sensor Network · Security Mechanism · Vulnerabilities · Intrusion Detection

1 Introduction

In the quickly progressing landscape of sensing unit networks, the requirement for durable protection approach protection devices has come to be significantly vital. As sensing unit networks continue to multiply throughout different domain names consisting of healthcare, commercial automation, ecological surveillance, as well as clever facilities, making certain the honesty along with discretion of the information transferred as well as refined by these networks is of utmost significance. This write-up looks into the essential function of protection method safety and security systems in sensing unit networks as well as the importance of applying durable procedures to safeguard delicate information [1].

P. Pareek et al. (Eds.): IC4S 2024, LNICST 597, pp. 47–60, 2025.
https://doi.org/10.1007/978-3-031-77075-3_5

The Expansion of Sensor Networks: Sensor networks have ended up being global in modern-day technical communities, making it possible for the collection, handling, as well as transmission of information from varied atmospheres. In the context of healthcare sensing unit networks play a crucial duty in helping with remote person tracking, tracking vital indicators and also taking care of clinical devices. These networks are likewise essential to commercial automation, where they allow real-time tracking of equipment and also ecological problems. Additionally in clever framework applications, sensing unit networks add to the reliable administration of sources as well as the execution of anticipating upkeep methods. The Vulnerabilities of Sensor Networks: Despite their many advantages sensing unit networks are vulnerable to numerous protection dangers as well as susceptibilities. The dispersed nature of sensing unit nodes coupled with source constraints makes these networks naturally susceptible to strikes such as eavesdropping, information meddling plus denial-of-service (DoS) strikes. Additionally, the release of sensing unit networks in remote or aggressive settings heightens their direct exposure to physical tampering [2]. To mitigate the essential susceptibilities of sensing unit networks, the application of durable protection technique safety and security devices is vital. These systems incorporate a range of techniques plus modern technologies targeted at shielding the stability, privacy, as well as accessibility of information within sensing unit networks. Security methods protected interaction procedures together with gain access to control devices are basic elements of protection technique protection systems, making certain that information sent as well as saved within sensing unit networks continues to be shielded from unapproved gain access to together with meddling [3].

Finally, the combination of protection method protection devices in sensing unit networks especially in the context of health care plus various other crucial domain names, is essential for protecting delicate information and also making certain the smooth procedure of adjoined gadgets. By leveraging modern technologies such as haze computer together with side tools, companies can enhance their protection method safety devices therefore improving functional effectiveness and also reducing safety and security dangers. As sensing unit networks remain to progress plus increase the positive application of durable safety actions will certainly be crucial in cultivating a safe and also resistant technical ecological community. Altogether, the imperious requirement for protection method protection devices in sensing unit networks, especially in health care atmospheres, highlights the criticality of protecting delicate information and also making sure the smooth procedure of adjoined gadgets. With the combination of haze computer, side gadgets, and also durable protection actions companies can enhance their protection method protection systems therefore improving functional effectiveness and also reducing protection threats [4].

1.1 Contribution of the Paper

- To explore the different strategies of the defence mechanism.
- To know the security technique of Sensor Networks.
- To discuss the several challenges of the defense mechanism.

1.2 Organization of the Paper

The paper has been organized into five sections. The first section, it represents the defense mechanism and its application and security system. The second section represents the related work and the third section represents the implementations of defense strategy security mechanisms. In section four, it represents the challenges and issues and finally, section five represents the conclusion and future works.

2 Related Work

Sensing unit networks are susceptible to numerous safety and security hazards along with susceptibilities that can jeopardize stability and privacy, coupled with the accessibility of the information they accumulate as well as transmit. Comprehending these susceptibilities is important for executing efficient protection methods safety and security systems. In this area, we will certainly perform an extensive evaluation of the dangers dealt with by sensing unit networks. Figure 1 shows types of security vulnerabilities.

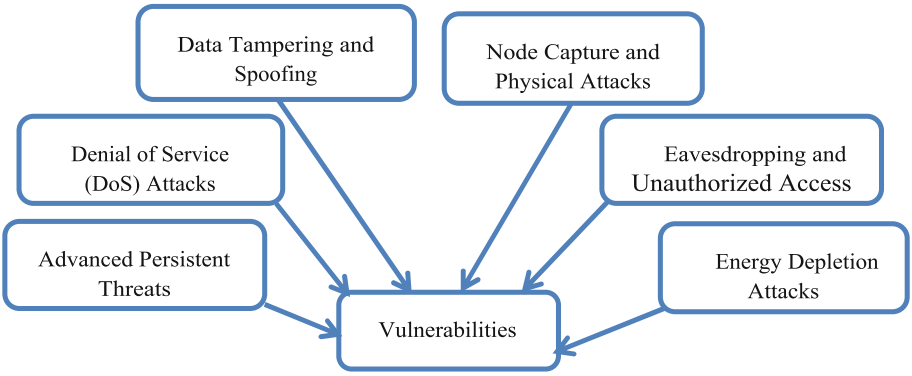

Fig. 1. Exploring the Vulnerabilities

- Advanced Persistent Threats (APTs): APTs are long-lasting targeted strikes that intend to obtain unapproved accessibility to sensing unit networks. These strikes can make use of susceptibilities in network procedures, software application or equipment parts enabling assailants to penetrate the network and also endanger its safety and security.
- Denial of Service (DoS) Attacks: DoS strikes intend to interfere with the regular performance of a sensing unit network by frustrating it with a high quantity of harmful website traffic. These strikes can provide the network less competent, triggering a loss of information as well as impacting the network's capability to do its desired features.
- Information Tampering and Spoofing: Attackers might try to adjust or customize the information sent by sensing unit nodes bring about imprecise or incorrect info. This can have serious repercussions in important applications such as healthcare or ecological surveillance.

- Node Capture and Physical Attacks: Sensor nodes are commonly released in remote or aggressive atmospheres making them susceptible to physical strikes. Assaulters might literally change with or record sensing unit nodes obtaining unapproved accessibility to delicate information or interrupting the network's procedure.
- Eavesdropping and Unauthorized Access: Sensor networks transfer information wirelessly making them at risk to eavesdropping [3] strikes. Assaulters might obstruct as well as evaluate the transferred information endangering the personal privacy and also privacy of the network.
- Energy Depletion Attacks: Sensor nodes have actually restricted power sources and also opponents might manipulate this susceptibility by releasing power deficiency strikes. These strikes intend to drain pipes the power of sensing unit nodes quickly making them inefficient along with interfering with the network's procedure.

By evaluating these risks and susceptibilities, companies can create durable protection methods to alleviate the dangers and also safeguard their sensing unit networks. In adhering to areas, we will certainly check out different protection techniques safety and security devices that can be executed to improve the safety and security of sensing unit networks.

2.1 Defense Mechanisms

To guarantee the protection of sensing unit networks it is essential to carry out durable protection systems that can secure against different hazards plus susceptibilities. In this area, we will certainly carry out a detailed testimonial of protection methods for sensing unit networks. Figure 2 shows defense mechanisms with network monitoring, intrusion detection systems, cryptographic techniques, key management, physical security, and secure data aggregation.

- Intrusion Detection Systems (IDS): IDSs are vital parts of protection devices in sensing unit networks. They keep track of network web traffic and also find any kind of dubious or harmful tasks. IDSs can recognize unapproved gain access to efforts, and information meddling together with various other safety violations, enabling prompt action together with mitigation [5].
- Cryptographic Techniques: Cryptography plays a critical function in protecting sensing unit networks. File encryption formulas can be made use of to shield the privacy as well as stability of information sent in between sensing unit nodes and also the control station. Verification devices such as electronic trademarks, can confirm the identification of sensing unit nodes together with make certain the credibility of the information.
- Key Management: Effective secret administration is necessary for preserving the protection of sensing unit networks. Trick circulation procedures as well as crucial contract systems allow safe and secure interaction in between sensing unit nodes and also the control station. Trick disobedience and also upgrade systems make sure that jeopardized or out-of-date secrets do not endanger the network's protection.
- Physical-Layer Security: Physical-layer safety and security systems intend to shield sensing unit networks from physical assaults together with sleuthing. Strategies

Fig. 2. Defense Mechanisms

such as safe signal handling, disturbance discovery and also physical-layer security can improve the safety and security of sensing unit networks by protecting against unapproved accessibility and also information interception.

- Secure Data Aggregation: Data gathering is an essential procedure in sensing unit networks, as well as safeguarding this procedure is essential. Safeguard information gathering techniques make sure that accumulated information is precise plus trustworthy also despite jeopardized or destructive nodes. Strategies such as fully homomorphic security and also safeguard transmitting procedures can be used to attain safe information gathering.
- Network Monitoring and Management: Continuous tracking, as well as monitoring of sensing unit networks, are crucial for finding and also reducing safety risks. Network managers can use network surveillance devices and also strategies to recognize abnormalities, spot strikes plus reply immediately to safety occurrences. By applying a mix of these protection devices companies can boost the safety and security of their sensing unit networks plus safeguard versus a variety of dangers. It is essential to frequently upgrade and also adjust these protection methods to deal with arising hazards together with susceptibilities in sensing unit networks.

2.2 Intrusion Detection Systems

Intrusion Detection Systems (IDS) play a crucial function in protecting sensing unit networks from unapproved gain access to along with prospective protection violations. IDSs check network web traffic and also find any type of questionable or harmful tasks, permitting prompt feedback coupled with mitigation.

By implementing IDSs in sensor networks, organizations can achieve the following benefits:

- Threat Detection: IDSs continually keep an eye on network website traffic coupled with examine it for indicators of unapproved gain access to or dubious habits. They can find different kinds of breaches, such as unapproved gain access to efforts, information meddling along with network scanning.
- Early Warning System: IDSs supply a very early caution system by signaling network managers or safety and security workers when prospective safety and security dangers are identified. This makes it possible for the experience examination and also reaction to alleviate the effect of the violation.
- Real-time Monitoring: IDSs provide real-time surveillance of network web traffic allowing companies to have an extensive sight of the network's safety and security position. This aids in recognizing continuous strikes together with taking instant activity to avoid additional damages.
- Incident Response: IDSs produce notifies plus logs that can be made use of for occurrence feedback and also forensic evaluation. These logs offer beneficial info regarding the nature of the breach, the concession systems, along with the prospective effect on the network.
- Network Segmentation: IDSs can be utilized to sector the network right into various safety and security areas permitting granular surveillance plus control. This aids in consisting of the effect of an invasion plus stopping side motion within the network.
- Compliance and Auditing: IDSs play a vital function in conference regulative conformity needs. They offer the essential tracking as well as discovery abilities to show that suitable safety procedures remain in location to safeguard the sensing unit network.

It is very important to keep in mind that IDSs must be consistently upgraded with the most recent hazard knowledge and also trademarks to successfully identify as well as alleviate arising dangers. In addition, companies need to have a distinct occurrence action strategy in position to resolve any type of safety occurrences discovered by the IDS. By executing invasion discovery systems, companies can boost the protection of their sensing unit networks and also guard versus unapproved gain access to plus prospective protection infractions.

2.3 Cryptographic Techniques

Cryptographic methods play an essential duty in improving information personal privacy as well as honesty in sensing unit networks. These methods make certain that delicate information sent plus saved in sensing unit networks continues to be protected along with shielded from unapproved accessibility or meddling. Right here are some cryptographic strategies frequently made use of to boost information personal privacy as well as stability in sensing unit networks. Figure 3 shows some cryptographic techniques used as security mechanism [6].

- Encryption: Encryption [5] is the procedure of transforming simple text information right into cipher text making use of an encryption formula as well as a secret secret. In sensing unit networks file encryption is made use of to secure information discretion by making certain that just licensed events can access as well as understand the secured information. File encryption stops eavesdropping as well as unapproved information interception.

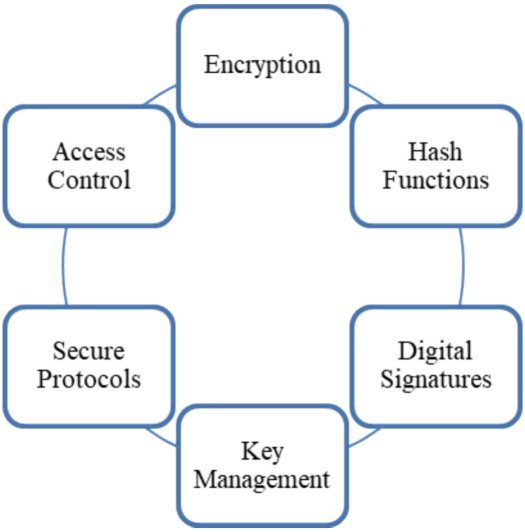

Fig. 3. Cryptographic Techniques

- Hash Functions: Hash features are mathematical formulas that produce a fixed size hash worth or message absorb from input information. In sensing unit networks hash features are made use of to confirm information honesty. By determining the hash worth of the information at the resource as well as contrasting it with the obtained information's hash worth any kind of adjustments or meddling can be found.
- Digital Signatures: Digital signature [7] offer information honesty and also verification in sensing unit networks. An electronic trademark is developed utilizing the sender's exclusive secret as well as can be validated utilizing the sender's public trick. By affixing an electronic trademark to the information, the receiver can confirm the information's credibility as well as stability making certain that it has actually not been damaged throughout transmission.
- Key Management: Key management is critical for guaranteeing the safety of cryptographic strategies in sensing unit networks. It entails producing, dispersing as well as safely saving file encryption secrets. Secret administration procedures and also formulas are made use of to develop safe interaction networks coupled with shield the privacy as well as honesty of the secrets themselves.
- Secure Protocols: Secure methods, such as Transport Layer Security (TLS) or Secure Shell (SSH), can be executed in sensing unit networks to supply protected interaction networks. These methods make certain the privacy as well as honesty of information traded in between sensing unit nodes as well as various other network entities.
- Access Control: Access control devices such as accessibility control check lists (ACLs) or role-based gain access to control [8] (RBAC) can be used to limit accessibility to delicate information in sensing unit networks. By imposing accessibility control plans, just licensed entities can access plus control the information lowering the threat of unapproved information adjustments.

By using these cryptographic strategies sensing unit networks can boost information personal privacy together with stability, securing delicate details from unapproved gain access to meddling and also interception. It is essential to thoroughly create as well as execute these methods based upon the particular needs as well as restrictions of the sensing unit network setting.

2.4 Key Management for Secure Communication

Key management monitoring is an essential facet of making certain safe and secure interactions coupled with verification in sensing unit networks. It includes the generation, circulation, as well as safe storage space of file encryption tricks made use of in cryptographic strategies to safeguard information privacy coupled with stability. Fig. 4. Shows some key management techniques used for secure communication. Right here are some essential monitoring strategies generally utilized in sensing unit networks:

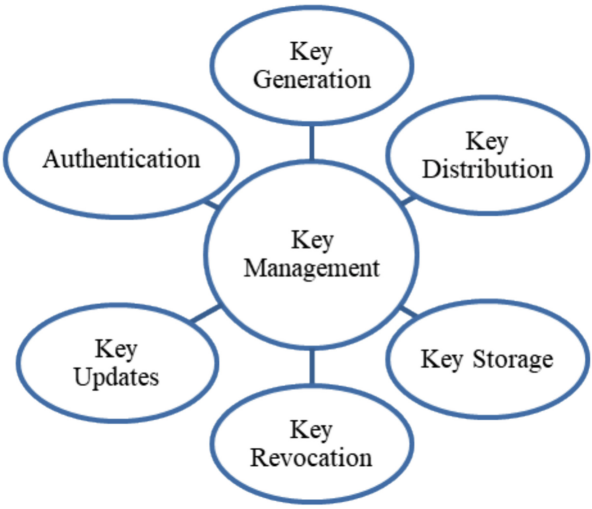

Fig. 4. Key Management

- Key Generation: Key generation includes producing cryptographic secrets that are made use of for file encryption, translation together with verification functions. In sensing unit networks, secrets can be produced making use of different techniques such as arbitrary number generators or secret obtained formulas. It is necessary to utilize solid as well as uncertain secrets to guarantee the protection of the network.
- Key Distribution: Key circulation is the procedure of safely sharing cryptographic secrets amongst sensing unit nodes. In a sensing unit network where nodes might have restricted sources as well as interaction abilities effective essential circulation devices are important. Strategies such as pre-distribution, in proportion secret facility, or public essential facilities (PKI) can be utilized for vital circulation.

- Key Storage: secure storage space of cryptographic secrets is crucial to avoid unapproved gain access to. In sensing unit networks where nodes might be literally easily accessible to assaulters safeguarding the secrets from burglary or meddling is essential. Safe secret storage space devices such as, such as hardware security modules (HSMs) or protected aspects, can be utilized to save secrets safely.
- Key Revocation: Key invalidation is the procedure of making nullified or shed secrets to stop unapproved gain access to. In sensing unit networks, where nodes might be susceptible to physical assaults or endangered by harmful entities, vital revocation systems are essential. Strategies such as certification suspension listings (CRLs) or on-line certification condition method (OCSP) can be utilized for vital revocation.
- Key Updates: Regular crucial updates are very important to preserve the safety and security of the sensing unit network. By regularly transforming cryptographic secrets the danger of vital concession or unapproved accessibility can be minimized. Secret upgrade devices need to be meticulously made to guarantee smooth shifts and also minimal interruption to the network's procedure.
- Authentication: Authentication [9] is the procedure of validating the identification of interacting entities in a sensing unit network. It makes sure that just licensed nodes can access the network and also connect safely. Verification devices such as electronic trademarks or challenge-response procedures, can be made use of to validate sensing unit nodes as well as develop safe interaction networks.

By applying durable crucial monitoring methods, sensing unit networks can guarantee protected interaction and also verification. These strategies assist in securing delicate information, stop unapproved accessibility along with preserve the stability of the network. It is necessary to think about the particular needs plus restrictions of the sensing unit network setting when making as well as carrying out crucial monitoring devices.

2.5 Energy-Efficient Security Solutions

In sensor section networks stabilizing protection demands with source restrictions is essential to guarantee reliable and reliable procedure. Energy-efficient security [10] options goal to give appropriate protection steps while decreasing the influence on minimal sources such as power, refining capacities as well as memory. Below are some strategies as well as strategies for accomplishing energy-efficient protection in sensing unit networks. Figure 5 shows different energy efficient security solutions.

- Lightweight Cryptography: Traditional cryptographic formulas can be resource-intensive as well as might not be ideal for resource-constrained sensing unit nodes. Lightweight cryptography concentrates on establishing effective cryptographic formulas particularly made for low-power tools. These formulas intend to supply an equilibrium in between protection as well as source use making it possible for energy-efficient safety and security remedies in sensing unit networks.
- Secure Data Aggregation: Data gathering is a usual procedure in sensing unit networks where numerous sensing unit nodes accumulate and also integrate information before transferring it to the base terminal. Safe information gathering methods intend to ensure the honesty and also privacy of accumulated information while decreasing

Fig. 5. Energy-Efficient Security Solutions

source use. Methods such as homomorphic file encryption, safe multiparty calculation and also information blend formulas can be utilized to accomplish energy-efficient safe information gathering.

- Trust-Based Routing: Trust-aware transmitting procedures think about the trustworthiness of sensing unit nodes when forwarding information in the network. By developing trust fund connections plus reviewing the integrity of nodes energy-efficient transmitting choices can be made while making sure of protected interaction. Trust-based transmitting methods can aid in alleviating strikes as well as save sources by preventing harmful or endangered nodes.
- Key Management Optimization: Key management [6] plays a vital function in safeguarding interaction in sensing unit networks. Maximizing crucial administration procedures, such as vital generation, circulation, storage space, withdrawal as well as updates can dramatically lower source intake. Strategies such as vital predistribution, essential sharing plus effective essential upgrade systems can be utilized to accomplish energy-efficient essential administration.
- Intrusion Detection and Prevention: Intrusion detection plus avoidance systems (IDPS) can aid determine and also alleviate safety and security dangers in sensing unit networks. Energy-efficient IDPS methods concentrate on decreasing source use while efficiently identifying, and also stopping assaults. This can be attained with light-weight breach discovery formulas, dispersed discovery devices, coupled with flexible surveillance techniques.
- Energy-Aware Security Protocols: Energy-aware safety and security methods aim to enhance safety and security procedures based upon the offered power sources in sensing unit nodes. These methods dynamically change safety and security specifications and also procedures to maintain power while keeping an appropriate degree

of safety. Methods such as flexible security careful information verification, plus energy-efficient vital exchange can be used to attain energy-aware safety and security procedures.

By applying these energy-efficient safety and security remedies, sensing unit networks can strike an equilibrium in between safety demands as well as source restrictions. These methods aid make certain the privacy, honesty, and also schedule of information while decreasing the effect on restricted sources. It is essential to think about the particular demands as well as restraints of the sensing unit network atmosphere when developing, as well as carrying out energy-efficient safety and security options.

3 Implementations of Defense Strategy Security Mechanisms

While the search results page supplied do not straight consist of study of real-world applications of protection approach safety and security devices in sensing unit networks I can give you with a basic summary of some remarkable examples on strategies in this field.

- TinySec: TinySec [11] is a well-known protection structure made especially for cordless sensing unit networks. It gives light-weight safety systems such as security, verification, plus honesty monitoring. TinySec intends to stabilize safety and security demands with the minimal sources of sensing unit nodes making it ideal for energy-constrained atmospheres.
- SPINS: SPINS [12] (Security Protocols for Sensor Networks) is a collection of protection methods established for sensing unit networks. It consists of methods for safe interaction, time synchronization, together with essential monitoring. SPINS concentrates on accomp g safeguarding tasks while offering safety solutions such as privacy, stability along with verification.
- LEAP: LEAP [13] (Localized Encryption and Authentication Protocol) is a crucial administration method developed for sensing unit networks. It intends to decrease the power usage connected with essential circulation and also storage space. LEAP utilizes a power structure crucial circulation system, where nodes closer to the base terminal have extra keying product minimizing the interaction expenses as well as power usage.
- Secure Data Aggregation in WSN [14]: Several research study researches have actually focused on protected information-gathering methods in sensing unit networks. For instance some techniques utilize homomorphic security to allow safe gathering without exposing specific information worths. Others utilize safe and secure multiparty calculation methods to do gathering while protecting personal privacy and also honesty.
- Trust-Based Routing Protocols: Trust-based routing protocol [15] have actually been recommended to boost safety and security in sensing unit networks. These procedures take into consideration the dependability of nodes when making transmitting choices, staying clear of possibly endangered or destructive nodes. Trust-based transmitting can assist save sources by decreasing the transmission of information with untrusted nodes.

While these instances supply a summary of some protection approach safety and security devices in sensing unit networks, it is very important to keep in mind that real world applications might differ relying on the certain application, network design, as well as source restrictions. Study plus real-world applications can offer useful understandings right into the useful difficulties as well as efficiency of these devices in various circumstances.

4 Challenges Issues

Sensor networks deal with a number of obstacles together with challenges when it involves guaranteeing their safety and security [16, 17]. Below are some vital obstacles as well as possible future instructions for progressing the safety of sensing unit networks:

- Resource Constraints: Sensor nodes commonly have actually restricted sources in regards to handling power, memory, as well as power. This positions a difficulty for executing durable safety and security systems that can run effectively within these restraints. Future instructions can focus on creating light-weight safety procedures together with formulas that decrease source intake while still offering appropriate defense.
- Key Management: Key management [6] is essential for making certain safe and secure interaction as well as information honesty in sensing unit networks. Nevertheless dispersing as well as upgrading secrets in a large-scale network can be testing. Future instructions might entail discovering unique secret administration plans that are scalable, energy-efficient, and also immune to assaults such as node capture or concession.
- Secure Data Aggregation: Data gathering is a basic procedure in sensing unit networks where several sensing unit nodes incorporate their information to lower repeating and also save power. Nevertheless, collecting information safely while maintaining personal privacy as well as stability is an intricate job. Future instructions can entail establishing innovative strategies such as safe and secure multiparty calculation or homomorphic security to allow safe and privacy-preserving information gathering.
- Trust and Authentication: Establishing count on and also confirming nodes in a sensing unit network is important for avoiding unapproved accessibility as well as making sure the stability of the network. Future instructions might entail discovering trust-based directing procedures, online reputation systems or aberration discovery strategies to boost the integrity of sensing unit nodes together with spot harmful actions.
- Secure Localization: Localization is necessary for numerous applications in sensing unit networks yet it can be prone to strikes such as spoofing or meddling. Future instructions might concentrate on establishing safe and secure localization methods that can spot as well as alleviate these strikes making sure the precision as well as dependability of area details.
- Privacy Preservation: Sensor networks typically gather delicate information as well as maintaining the personal privacy of people or companies entailed is of utmost significance. Future instructions might entail discovering privacy enhancing innovations such as differential personal privacy safe and secure information privacy or safe

information sharing methods to secure delicate info while still making it possible for valuable evaluation together with decision-making.

- Intrusion Detection and Response: Detecting coupled with reacting to intrusions or assaults in real-time is important for keeping the safety and security of sensing unit networks. Future instructions might include creating reliable together with reliable invasion discovery systems customized to the special attributes of sensing unit networks, such as minimal sources as well as vibrant network topologies.

In general, progressing the safety and security of sensing unit networks calls for attending to these obstacles as well as checking out ingenious remedies that strike a balance in between safety needs as well as source restrictions. Future research study instructions must concentrate on establishing useful, scalable and also energy efficient safety and security systems that can be properly set up in real-world sensing unit network implementations.

5 Conclusion and Future Works

Sensing unit networks are progressively being made use of as an important part in protection method protection devices. Nonetheless, obstacles continue in attending to these networks. One such obstacle is the requirement for durable safety and security steps. To get over these obstacles, it is essential to improve partnership plus details sharing welcome arising modern technologies as well as fads, take on a detailed technique, and concentrate on maritime safety and security teamwork coupled with deal with restrictions and also obstacles. This includes developing systems for sharing info coupled with coordinating initiatives to improve the safety and security of sensing unit networks. By remaining upgraded on technical breakthroughs as well as integrating them right into protection methods, sensing unit networks can much better get used to progressing hazards as well as guarantee durable protection. Furthermore, resolving constraints as well as obstacles in existing protection techniques such as security strategies, breach discovery systems verification procedures, and also vital monitoring techniques, can assist boost the general safety position of sensing unit networks. By carrying out these procedures, sensing unit networks can efficiently minimize hazards in an increasingly linked along with digitized globe.

References

1. Wang, M., Lu, Y., Qin, J.: A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Comput. Secur. 88 (2020)
2. Karakaya, A., Akleylek, S.: A survey on security threats and authentication approaches in wireless sensor networks. In: 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–4. Antalya, Turkey (2018)
3. Zou, Y,, Wang, G.: Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. IEEE Trans. Indust. Inform. **12**(2), 780–787 (2016)
4. Nayak, R., Nanda, A.K., Awasthi, L.K.: Multiple private keys with NTRU cryptosystem. Int. J. Res. Comput. Commun. Technol. **4**(3), 250–255 (2015)

5. Altulaihan, E., Almaiah, M.A., Aljughaiman, A.: Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions. Electronics (2022)
6. Amara, S.A., Gopala Gupta, L.G., Syam Prasad, G.: A review on defense strategy security mechanism for sensor network. Smart Sensor Networks Using AI for Industry (2021)
7. Nayak, R., Pradhan, J., Sastry, C.V.: NTRU digital signature scheme - a matrix approach. Int. J. Adv. Res. Comput. Sci. **II**(I), ISSN 0976 – 5697 (2011)
8. Alturi, V., Ferraiolo, D.: Role-based access control. In: van Tilborg, H.C.A., Jajodia, S. (eds.) Encyclopedia of Cryptography and Security. Springer (2011)
9. Yousefpoor, M.S., Barati, H.: Dynamic key management algorithms in wireless sensor networks: a survey. Comput. Commun. **134**, 52–69 (2019)
10. Nanda, A.K., Nayak, R., Awasthi, L.K.: NTRU with gaussian integer matrix. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(2), 359–365 (2015)
11. Gautam, A.K., Kumar, R.: A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Appl. Sci. **3**, 50 (2021)
12. Gudivada, R.B., Hansdah, R.C.: Energy efficient secure communication in wireless sensor networks. In: IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), pp. 311–319. Krakow, Poland (2018)
13. Karlof, C., Sastry, N., Wagner, D.A.: TinySec: a link layer security architecture for wireless sensor networks. In: ACM International Conference on Embedded Networked Sensor Systems (2004)
14. Ullah, F., Mehmood, T., Masood, H., Muhammad, I.: SPINS: security protocols for sensor networks. In: 009 International Conference on Machine Learning and Computing, IPCSIT vol. 3. IACSIT Press, Singapore (2011)
15. Raut, A.R., Bele, S.B., Totade, S.K.: Leap protocol in wireless sensor network. IJRECE **6**(3) (2018)
16. Othman, S., Ben, T.A., Youssef, H., Alzaid, H.: Secure data aggregation in wireless sensor networks. In: 2013 12th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), pp. 55–58. Ajaccio, France (2018)
17. Jawhar, I., Mohammed, F., Jaroodi, J.A., Mohamed, N.: TRAS: A trust-based routing protocol for ad hoc and sensor networks. In: IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), p. 382387. New York, NY, USA (2016)