IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Review On Security Challenges In Iot And Wireless Sensor Networks

Mrs.C.Mahesh Sathya[1], Dr.R.Ramkumar[2]

Ph.D Research scholar [1], Principal [2]

[1]Department of Computer Science,[1]Sasurie College of Arts & Science, Tirupur. Tamil Nadu, India.

Abstract: Internet of Things (IoT) and Wireless Sensor Networks (WSNs), modern technology has advanced tremendously, enabling unparalleled connectivity and data collection across a variety of disciplines. This paper explores the critical issues of data confidentiality, integrity, authentication, authorization, and network availability. Emphasizing the need for robust encryption, strong authentication protocols, and resilient network designs, it highlights the importance of physical security and industry-wide standards. Addressing these multifaceted challenges is essential to safeguard data and ensure the reliable operation of IoT and WSNs, thereby fully leveraging their potential in various sectors.

***Keywords*:IoTSecurity,WirelessSensorNetworks,DataConfidentiality,Authentication,Networkresilience**

I. INTRODUCTION

IoT (Internet of Things) refers to the network of interconnected devices, ranging from commonplace household objects to highly advanced industrial gear, that exchange data and communicate with each other in order to optimize processes, boost productivity, and increase quality of life. As a component of the Internet of things, WSNs are made up of spatially dispersed sensors that track environmental or physical parameters like pressure, humidity, and temperature and send the information they gather to a central hub. While these technologies offer numerous benefits, they also introduce significant security challenges that must be addressed to ensure their safe and reliable operation.

The proliferation of IoT and WSNs has exponentially increased the attack surface for potential cyber threats. The diversity and sheer number of connected devices present unique security vulnerabilities. Many IoT devices are designed with minimal security features due to constraints like cost, size, and power consumption. Consequently, these devices often lack robust encryption, authentication, and access control mechanisms, making them attractive targets for cyber attackers. Unauthorized access, data breaches, and even the manipulation of vital systems can result from inadequate security. One of the primary security challenges in IoT and WSNs is ensuring data confidentiality. Sensitive information transmitted between devices, such as personal data, health records, or financial transactions, must be protected from eavesdropping and interception. Traditional encryption methods, while effective, may not be suitable for resource-constrained IoT devices. Lightweight encryption protocols and advanced cryptographic techniques are necessary to provide adequate security without compromising performance.

Another significant concern is data integrity. Ensuring that the data collected by IoT devices and sensors remains accurate and unaltered during transmission is crucial. Tampering with data can lead to erroneous decisions and actions, particularly in critical applications like healthcare, industrial automation,

and smart grids. Secure communication protocols and robust authentication mechanisms are essential to verify the authenticity and integrity of data. It is also crucial to address the issue of device authorization and authentication. IoT devices must be able to reliably identify and authenticate each other to prevent unauthorized access. Implementing strong authentication protocols, such as public key infrastructure (PKI) and mutual authentication can mitigate the risk of unauthorized devices joining the network. Furthermore, establishing granular access

controls ensures that devices only have access to the necessary data and resources, minimizing the potential impact of a security breach.

Network availability and resilience are critical for the continuous operation of IoT and WSNs. Denial-of-service (DoS) attacks, which aim to disrupt the availability of network services, pose a significant threat. These attacks can overwhelm network resources, rendering the IoT system inoperative. Implementing intrusion detection and prevention systems, along with redundancy and failover mechanisms, can enhance network resilience and maintain service availability. Additionally, the physical security of IoT devices and sensors cannot be overlooked. These devices are often deployed in unattended or remote locations, making them susceptible to physical tampering, theft, or destruction. Ensuring physical security through tamper-resistant hardware, secure enclosures, and regular monitoring is essential to prevent unauthorized physical access.

The dynamic and heterogeneous nature of IoT and WSNs further complicates security management. The integration of devices from different manufacturers, each with varying security standards and protocols, creates interoperability challenges. Establishing industry-wide security standards and frameworks can facilitate better integration and enhance overall security. The security challenges in IoT and WSNs are multifaceted and require a comprehensive approach that encompasses robust encryption, authentication, access control, and physical security measures. As the adoption of these technologies continues to grow, addressing these challenges is imperative to safeguard data, ensure reliable operation, and fully realize the potential benefits of IoT and WSNs in various sectors.

II. LITERATURE REVIEW

1. A. Viswanathan (2017) et.al proposed Security Challenges in the Integration of IoT with WSN for Smart Grid Applications. The Internet of Things (IoT) is a burgeoning technology paradigm with applications spanning Smart Grids, Smart Homes, and Communication Networks, among others. Wireless Sensor Networks (WSNs) play a pivotal role in applications such as landslide detection, waste management, and water quality monitoring in rivers and lakes. Smart Grids represent a critical application area for WSNs, addressing issues of power grid reliability and energy scarcity. The primary challenge in traditional power grids lies in their unreliability and the lack of user awareness regarding energy availability and usage limits, leading to increased energy costs and perceptions of unaffordability. IoT-enabled Smart Grid solutions aim to transform existing grids into reliable and cost-efficient systems by leveraging WSNs. This paper explores the integration of IoT into Smart Grids and the associated security challenges. Additionally, it introduces a solar energy harvester for a Smart City Framework, where buildings equipped with solar energy systems can share energy based on decisions made by a central control station. This approach proposes a cost-effective Smart Grid model using distributed renewable energy generators to meet local power demands effectively.

2. N. b. H. Kasah (2020) et.al proposed Investigation on 6LoWPAN Data Security for Internet of Things. Low-power wireless network technology is a critical characteristic in communication systems essential for the Internet of Things (IoT). Among the communication protocols crucial for IoT applications is the 6LoWPAN standard, facilitating efficient transfer of IPv6 packets within a well-defined IEEE 802.15.4 link-layer framework. Despite its development, 6LoWPAN faces challenges such as security threats and trust issues. Securing the network is paramount, with data security being a major concern in these communications. Researchers are actively working on analyzing the architecture and network features to enhance 6LoWPAN communication security. The technology's vulnerabilities expose it to various network attacks, necessitating investigation into security solutions and the presentation of safety requirements for 6LoWPAN..

3. H. Garg (2019) et.al proposed Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware. The Internet of Things (IoT) is a highly disruptive technology that has grown exponentially, influencing and transforming various industries with its vast capabilities. This paper discusses the role of REST API in IoT systems, highlighting how IoT technology facilitates comprehensive data recording and analytics. It emphasizes the importance of middleware in connecting IoT devices with the cloud, noting that the emergence of IoT applications in the cloud has introduced new security and privacy threats. The paper proposes a secure IoT system design aimed at preventing network infiltration by attackers and securing data in transit from IoT devices to the cloud. It details how Representational State Transfer (REST) API securely exposes connected devices to cloud applications and users. In this proposed model, middleware serves to expose device data through REST, abstracting technical details and acting as an interface for users to interact with sensor data effectively.

4. M. A. Saleem (2021) et.al proposed Security Analysis on A Secure Three-Factor User Authentication Protocol with Forward Secrecy for Wireless Medical Sensor Network Systems. The Internet of Things (IoT) enables various devices and objects to connect to the internet, facilitating data transmission through emerging technologies, thereby realizing the vision of intelligent identification. Wireless Sensor Networks (WSNs), a fundamental component of IoT, find application in diverse fields such as smart transportation and healthcare. With the rapid development of WSNs and Wireless Medical Sensor Networks (WMSNs), ensuring data security, including preventing secret data leakage, has become a significant concern for researchers. Despite numerous authentication protocols proposed for WMSNs, many suffer from serious security flaws. Recently, Li et al. (IEEE Syst. J., vol. 14, no. 1, pp. 39–50, Mar. 2020) introduced a three-factor user authentication protocol for WMSNs, claiming it provides user anonymity and prevents sensor node impersonation attacks. This work provides a thorough security study of the protocol proposed by Li et al. It is found that the protocol is not secure against impersonation attempts by sensor nodes and does not provide user anonymity as advertised. Finally, we suggest appropriate remedies to address the identified deficiencies in Li et al.'s protocol.

5. R. Mahmoud (2015) et.al proposed Internet of things (IoT) security: Current status, challenges and prospective measures. The paper provides a comprehensive survey and analysis of the current state and concerns regarding Internet of Things (IoT) security. IoT aims to connect anything, anywhere, and anyone, typically structured into three layers: Perception, Network, and Application. Security principles must be applied across these layers to achieve a secure IoT framework. Addressing and resolving security issues are crucial for ensuring the future development of IoT. Researchers have developed various countermeasures to tackle specific security concerns at different IoT layers and devices. An overview of security concepts, technological difficulties, suggested solutions, and potential future paths to improve IoT security are provided in this study.

6. M. Azarmehr (2017) et.al proposed secure authentication and access mechanism for IoT wireless sensors. Security remains the primary challenge in designing and implementing interconnected objects on today's ubiquitous Internet network infrastructure. To address these concerns, numerous security solutions have been proposed for IoT-enabled devices. In this paper, an integrated method for access control and authentication in wireless sensor nodes of Internet of Things networks is presented. The method offers robust protection against known attacks such as energy depletion and Man-In-The-Middle attacks by ensuring that only authorized devices can access the network, thus mitigating the risks of unauthorized access and data breaches. By integrating these mechanisms, the approach not only enhances the security posture of IoT networks but also contributes to their reliability and operational integrity. The effectiveness of this method is demonstrated through its ability to defend against common security threats, providing a viable solution for securing IoT environments amidst the growing threat landscape.

7. Z. Hamici (2018) et.al proposed Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways. The integration of wireless sensor networks into the Internet of Things (IoT) has ushered in a new generation of sensor nodes that connect directly to remote servers for the processing of signals and making decisions. This shift from local node processing is made possible by decoupling the node hardware from the processing capabilities, enabled through network virtualization implementations. However, this virtualization, which introduces new services executed remotely, also brings significant security challenges due to the continuous exchange of data between sensor nodes and remote servers. We suggest a novel genetic algorithm for data security that uses strong security architecture and a one-time key

for single block enciphering, as opposed to block chaining or weak stream enciphering, in order to overcome these difficulties. High resilience to cryptanalysis is provided by this algorithm architecture, which produces changeable (stealthy) keys and data with statistical behaviors similar to white noise. The method blends gene fusion and horizontal gene transfer, drawing inspiration from the way antibiotic resistance spreads among bacteria. A stealthy-key feature is also added to the encryption by a Salt that is taken from the hash value of the data block. The approach exhibits an avalanche effect in practice, averaging 98% for a 16x16 byte block of encrypted sensor data with a single bit flipped in the data.

8. R. Johari (2020) et.al proposed START: Smart Stick based on TLC Algorithm in IoT Network for Visually Challenged Persons. A smart stick designed for visually challenged individuals addresses the challenges they face while navigating unknown terrain and crossing roads. The stick utilizes the Traffic Light Crossing (TLC) Algorithm for guidance, incorporating a Global Positioning System (GPS) for navigation.

It features obstacle detection via ultrasonic sensors, traffic light color detection using a color sensor, and a buzzer-based alert system. Additionally, it includes GSM (Global System for Mobile) technology for message alerts and location sharing, all managed by the ATmega328P microcontroller. Future plans include integrating voice recognition and GPS guiding systems to further enhance its functionality and usability for visually impaired users.

9. S. Mishra (2020) et.al proposed A Critical Analysis of Attack Detection Schemes in IoT and Open Challenges. The Internet of Things (IoT) encompasses a vast array of Internet-connected devices that profoundly impact our daily lives across various domains. Security and privacy concerns for these devices are paramount, given their unique vulnerabilities compared to traditional wireless applications. Detecting and preventing threats in IoT systems is crucial but challenging, as traditional detection techniques may not be directly applicable due to IoT's distinct architecture, resource-constrained devices, specific integration protocols, and diverse standards. Creating algorithms especially for IoT contexts is necessary to address these issues. This study critically analyzes detection techniques, their effectiveness in addressing IoT threats, and the ongoing challenges that need to be addressed.

10. O. Flauzac (2015) et.al proposed SDN Based Architecture for IoT and Improvement of the Security. With the exponential growth of Internet-connected devices, securing networks has become one of the most challenging tasks for network managers. Large-scale, diverse network maintenance and security are extremely difficult. In this context, Software Defined Networking (SDN) presents a new networking paradigm that offers numerous opportunities to address these challenges. This article introduces several new SDN-based architectures. Firstly, we propose an SDN domain architecture that integrates wired, wireless, and Ad-Hoc networks, whether they have existing infrastructure or not. Secondly, we present an architecture that incorporates sensor networks into an SDN-based network within a domain. Thirdly, we explore interconnecting multiple domains and enhancing the security of each domain while ensuring that the distribution of security rules does not compromise the security of any single domain. Finally, we propose a new secure and distributed architecture for the Internet of Things (IoT).

11. K. Harsanyi (2018) et.al proposed Wormhole detection in wireless sensor networks using spanning trees. Ad-hoc and wireless sensor networks are becoming more and more popular because they can solve difficult problems, and recent technology developments have made it possible for networks to become denser and smarter. These networks serve as the foundation of the Internet of Things (IoT), offering diverse applications. However, ensuring network security is crucial, especially in scenarios where sensors operate in unknown or hostile environments. Wireless communication channels used in ad-hoc networks are vulnerable to various attacks, with the wormhole attack posing a severe threat. Unlike other attacks, the wormhole attack doesn't require compromising sensors or breaking cryptographic defenses. In response, this paper proposes a novel method to detect wormhole attacks and identify affected sensors using only network connectivity information, without requiring special measurements.

12. A. Aliti (2019) et.al proposed a security model for Wireless Sensor Networks. State-of-the-art security frameworks have extensively addressed security issues for web resources, agents, and services in the Semantic Web. The emergence of Stream Reasoning, blending Semantic Web and Data Stream Management Systems, has introduced new challenges due to its decentralized nature, metadata descriptions, and the involvement of numerous users, agents, and services, making securing these systems complex.

There is a clear need for developing new security models capable of handling security and automating security mechanisms in a more autonomous manner to support dynamic relationships between data, clients, and service providers. With a focus on Wireless Sensor Networks (WSNs) for water quality monitoring, we use stream data applications to verify the effectiveness of our suggested security approach. This model serves as a guide for deploying and maintaining WSNs in various contexts, emphasizing critical segments for ensuring security in semantic stream reasoning systems and their interrelationships. Additionally, we anticipate that our framework will inspire further research into improving information security within semantic stream reasoning systems.

13. R. AL Mogbil (2020) et.al proposed IoT: Security Challenges and Issues of Smart Homes/Cities. The Internet of Things, or IoT, has become a game-changing technology that has an enormous influence on many facets of our life. It began with smart phones, opening new perspectives in the tech world, followed by cloud computing which revolutionized computational power usage. Computing power was further increased via machine learning and artificial intelligence. Recently, IoT has introduced a new technological future, creating intelligent environments like smart homes and cities, enhancing convenience and quality of life. Despite its advancements, IoT faces significant security challenges. This paper proposes an IoT architecture design, highlighting security issues and requirements in smart home/city environments. It discusses IoT security attacks, countermeasures, and presents a real-life scenario, aiming to address these challenges and foster a secure IoT environment.

Here's Comparison table summarizing the content

Paper	Title	Protocol Name	Merits	Demerits
A. Viswanathan (2017)	Security Challenges in the Integration of IoT with WSN for Smart Grid Applications	Not specified	- Improves reliability through real-time monitoring and predictive maintenance - Introduces a cost-effective Smart Grid model using distributed renewable energy	- Increases risk of cyber attacks, potentially compromising Smart Grid reliability
N.b.H.Kasah (2020)	Investigation on 6LoWPAN Data Security for Internet of Things	6LoWPAN	- Enables efficient transfer of IPv6 packets over low-power wireless networks	- Trust issues require robust solutions, complicating secure 6LoWPAN systems
H. Garg (2019)	Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware	REST API and Middleware	- Facilitates secure communication between IoT devices and the cloud - Reduces risk of data breaches during transmission	- Adds complexity to the system, requiring specialized knowledge and resources
M.A.Saleem (2021)	Security Analysis on A Secure Three-Factor User Authentication Protocol with Forward Secrecy for Wireless	Three-Factor User Authentication Protocol	- Offers solutions to improve the protocol's robustness - Contributes to secure authentication in WMSNs	- The analyzed protocol fails to resist sensor node impersonation attacks and does not ensure user anonymity

	Medical Sensor Network Systems			
R.Mahmoud (2015)	Internet of things (IoT) security: Current status, challenges and prospective measures	Not specified	- Provides thorough survey and analysis of current IoT security issues - Covers all three layers of the IoT architecture	- Comprehensive nature may be complex and challenging for readers without strong IoT security background
M.Azarmehr (2017)	Secure authentication and access mechanism for IoT wireless sensors	Integrated Access Control and Authentication Method	- Ensures secure communication with wireless sensor nodes - Maintains data integrity and confidentiality	- Requires significant technical expertise and resources to implement
Z.Hamici (2018)	Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways	Genetic Algorithm for Data Security	- High level of security with one-time keys - Exhibits avalanche effect, enhancing immunity to cryptanalysis	- Introduces complexity in algorithm design and understanding due to biological concepts
R. Johari (2020)	START: Smart Stick based on TLC Algorithm in IoT Network for Visually Challenged Persons	TLC Algorithm	- Improves safety by detecting obstacles and traffic light changes	- Increases complexity and cost due to multiple sensors and modules
S.Mishra (2020)	A Critical Analysis of Attack Detection Schemes in IoT and Open Challenges	Not specified	- Addresses unique IoT threats with specific detection techniques	- Developing specific algorithms for IoT increases system complexity and requires significant expertise
O.Flauzac (2015)	SDN Based Architecture for IoT and Improvement of the Security	SDN-Based Architecture	- Centralized management and control improves security monitoring - Enhances security enforcement across diverse networks	- Dependency on centralized controller poses risks if compromised, affecting entire network operations
K.Harsanyi (2018)	Wormhole detection in wireless sensor networks using spanning trees	Spanning Tree Method	- Effectively detects wormhole attacks without relying on complex defenses - Does not compromise sensor nodes	- May not detect sophisticated wormhole variants or attacks manipulating connectivity information
A. Aliti (2019)	A security	Security Model	- Provides practical guide	- Managing

	model for Wireless Sensor Networks	for WSNs	for deploying and maintaining secure WSNs - Focuses on critical segments for ensuring security in stream reasoning systems	decentralized systems and numerous users, agents, and services increases complexity
R.ALMogbil (2020)	IoT: Security Challenges and Issues of Smart Homes/Cities	Not specified	- Outlines IoT architecture and addresses security requirements and challenges - Provides advice on securing IoT-based systems	- Lacks specific details or case studies to substantiate claims

III. CONCLUSION

In conclusion, securing IoT and Wireless Sensor Networks (WSNs) is a multifaceted challenge requiring a holistic approach. Robust encryption, authentication, and access control are vital to protect sensitive data and ensure device integrity. Addressing physical security and implementing resilient network designs are also crucial. As IoT and WSN adoption grows, establishing standardized security protocols and frameworks will be essential to mitigate risks and safeguard operations. By prioritizing security, we can fully harness the transformative potential of these technologies across diverse sectors while ensuring their safe and reliable deployment.

REFERENCES

[1] A. Viswanathan, N. B. Sai Shibu, S. N. Rao and M. V. Ramesh, "Security Challenges in the Integration of IoT with WSNfor Smart Grid Applications," *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICCIC.2017.8524233.

[2] N. b. H. Kasah, A. H. b. M. Aman, Z. S. M. Attarbashi and Y. Fazea, "Investigation on 6LoWPAN Data Security for Internet of Things," *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257661.

[3] H. Garg and M. Dave, "Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777334.

[4] M. A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar and K. Mahmood, "Security Analysis on "A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems"," in *IEEE Systems Journal*, vol. 15, no. 4, pp. 5557-5559, Dec. 2021, doi: 10.1109/JSYST.2021.3073537.

[5] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[6] M. Azarmehr, A. Ahmadi and R. Rashidzadeh, "Secure authentication and access mechanism for IoT wireless sensors," *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD, USA, 2017, pp. 1-4, doi: 10.1109/ISCAS.2017.8050446.

[7] Z. Hamici, "Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways," in *IEEE Journal of Biomedical and Health Informatics,* vol. 22, no. 6, pp. 1814-1823, Nov. 2018, doi: 10.1109/JBHI.2018.2860980.

[8] R. Johari, N. K. Gaurav, S. Chaudhary and A. Pramanik, "START: Smart Stick based on TLC Algorithm in IoT Network for Visually Challenged Persons," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* Palladam, India, 2020, pp. 605-610, doi: 10.1109/I-SMAC49090.2020.9243517.

[9] S. Mishra and A. Paul, "A Critical Analysis of Attack Detection Schemes in IoT and Open Challenges," *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON),* Greater Noida, India, 2020, pp. 57-62, doi: 10.1109/GUCON48875.2020.9231077.

[10] O. Flauzac, C. González, A. Hachani and F. Nolot, "SDN Based Architecture for IoT and Improvement of the Security," *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops,* Gwangju, Korea (South), 2015, pp. 688-693, doi: 10.1109/WAINA.2015.110.

[11] K. Harsányi, A. Kiss and T. Szirányi, "Wormhole detection in wireless sensor networks using spanning trees," *2018 IEEE International Conference on Future IoT Technologies (Future IoT),* Eger, Hungary, 2018, pp. 1-6, doi: 10.1109/FIOT.2018.8325596.

[12] A. Aliti and K. Sevrani, "A security model for Wireless Sensor Networks," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* Opatija, Croatia, 2019, pp. 1165-1168, doi: 10.23919/MIPRO.2019.8756647.

[13] R.AL MOGBIL, M. AL ASQAH and S. EL KHEDIRI, "IoT: Security Challenges and Issues of Smart Homes/Cities," *2020 International Conference on Computing and Information Technology (ICCIT-1441),* Tabuk, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCIT-144147971.2020.9213827.