www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 13 Issue 04 April 2024, Page No. 26121-26129
ISSN: 2319-7242 DOI: 10.18535/ijecs/v13i04.4810

A Secure Authentication mechanism for wireless sensor network using standardized IoT protocols

Lakhveer Kaur[1], Dr Kulwinder Singh[2]
Research Scholar[1] ,Professor[2]
Bhai Maha Singh College Of Engineering, PTU, Muktsar, Punjab, India

Abstract

Next-generation wireless sensor networks comprise low-cost, power-constrained nodes with limited data transfer, memory, and computational abilities, forming the backbone of IoT deployments across diverse domains. IoT sensor nodes play a pivotal role in collecting and disseminating critical environmental data using protocols like MQTT. However, ensuring secure communication channels between nodes remains paramount, necessitating robust measures for authentication, confidentiality, and data integrity. This abstract introduces a secure mechanism tailored for next-gen wireless sensor networks, employing the MQTTS (MQTT over TLS) IoT protocol. The proposed mechanism aims to bolster network defenses against various attacks, including masquerade, man-in-the-middle, replay, password guessing, and denial-of-service attacks, ensuring the resilience and reliability of next-gen IoT deployments.

Keywords—IoT, security, Authentication, WSN, IoT devices

I. Introduction

Nowadays IoT is a fast growing new industry and almost all experts believe that in the coming years IoT will be used in many different aspects. However, this phenomenon, like many other IT-related phenomena, faces different challenges[1].

The IoT is a world where billions of objects can communicate and share information, all of these objects are connected over the Internet protocol (IP). These connected objects generate huge amounts of data regularly which is collected, analyzed and used to perform actions, providing intelligence for decision making[2].

The number of connected devices with the IoT environment is increasing every day. The reason for this rapid increase is; connected devices provide comfort and produce good results compared to humans.The number of connected devices is increasing with enormous speed[3]. The concept of the Internet that we have in mind is a global network in which personal computers, cell phones, etc. are connected, and humans are communicating with each other using these connected devices everywhere. Now consider a world in which the Internet goes beyond its current concept and includes the objects/things around us. The Internet of Things is an emerging technology in which each “Thing” can send and receive data through various communication networks. Specifically, a “Thing” in IoT has the ability to collect data, control, or communicate remotely. A smart lock connected to your mobile phone, CCTV cameras which can be controlled remotely or a sprinkle in your garden that can be programmed are all examples of IoT devices[4].

The evolution of wireless sensor networks into the next generation presents a landscape characterized by numerous sensor nodes embodying low-cost attributes coupled with constrained power, data transfer capabilities, memory, transmission reach, and computational prowess. Termed as the backbone of Internet of Things (IoT) deployments, these networks find pervasive applications spanning area monitoring, healthcare surveillance, medical device integration (inclusive of implanted, wearable, and environment-embedded solutions), environmental sensing, industrial monitoring, and multifaceted threat detection across domains.

In this milieu, IoT sensor nodes assume the pivotal role of data collection and dissemination, orchestrating the flow of critical information from the ambient environment to the cloud infrastructure via diverse transmission protocols. Among these, the MQTT (Message Queuing Telemetry Transport) protocol emerges as a prime enabler, facilitating swift and lightweight message propagation. However, the exigencies of security loom large over this interconnected ecosystem. Authentication, confidentiality, and data integrity emerge as linchpins in ensuring secure communication channels between sensor nodes and designated sink nodes.

It can be said that the Internet of Things is a network of networks in which a large number of things, sensors and devices are connected through the communication and information infrastructure to provide value-added services through intelligent data processing and management for various applications

Along with the tremendous benefits of the Internet of Things, this technology faces some challenges. One of the main challenges of the IoT is the security of these devices. Unauthorized access, data hijacking, data manipulation, network penetration, eavesdropping, etc. are among the IoT security challenges. Therefore, new standards and protocols are always required to solve sustainability, reliability, service quality, confidentiality and integrity. Smart home and smart cities are also in need of these updates. In order to achieve this goal, it is very important to examine the protocols and standards of IoT. Actually, by using these surveys, we can provide better protocols and standards to address the challenges and limitations that currently exist[6][7].

It is very important that IoT devices have adequate security. At the moment, given the fact that manufacturers are rushing to introduce new smart devices to the market, so the security of these devices is usually not the first priority for them. Consumers and businesses are often unaware of how their devices' security affects their lives or business. This will increase the risk of data breach or hacking these devices[5].

The survey paper is structured as follows: Section two highlights the related work in the field of IoT security & Privacy. Section three describes the problem statement and Section four the summary of the survey in the form of conclusion.

II. Related work

A. *Internet of Things (IoT)*

The Internet of Things (IoT) is a network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to collect and exchange data. IoT technology has the potential to revolutionize the way we live, work and communicate by allowing everyday objects to communicate with each other and with us. One of the key benefits of IoT is the ability to gather data from a wide range of sources, including sensors, cameras, and other devices. This data can be analyzed to gain insights and make more informed decisions. IoT also plays a major role in the development of smart cities, where the integration of IoT technology can help to improve public services, reduce environmental impact and increase the overall quality of life for citizens. For example, smart streetlights equipped with sensors can collect data on traffic, weather, and air quality, which can then be used to optimize energy consumption, reduce pollution, and improve public safety. However, as IoT technology becomes more widely adopted, there are also concerns about security and privacy. As IoT devices collect and transmit large amounts of personal data, it is important to ensure that this data is protected from unauthorized access and breaches. It is also important to ensure that IoT devices are secure by design, and that security is integrated throughout the entire product development process. Overall, IoT technology has the potential to change the way we live, work, and communicate, and has already begun to have a major impact on various industries. However, it is important to consider the security and privacy implications of this technology, and to ensure that IoT devices are designed and implemented with these concerns in mind.

B. *Security Challenges*

The Internet of Things (IoT) has the potential to revolutionize the way we live, work and communicate by allowing everyday objects to communicate with each other and with us. However, as IoT technology becomes more widely adopted, there are also concerns about security and privacy. IoT devices are vulnerable to cyber attacks, and if compromised, can cause serious harm to individuals, organizations, and even society as a whole. One of the main security challenges of IoT is that many devices are not designed with security in mind. Many IoT devices have limited processing power, memory and storage, making it difficult to implement traditional security measures such as encryption and firewalls. Additionally, many IoT devices have limited or no user interface, making it difficult for users to change default passwords or update software. Another security challenge of IoT is the lack of standardization. The vast number of IoT devices, platforms, and protocols currently in use makes it difficult to ensure that all devices are secure and that they can communicate with each other in a secure manner. This lack of standardization also makes it difficult for security professionals to protect against threats and to manage the security of IoT devices. IoT devices also pose a risk to the overall security of networks they are connected to. As IoT devices are often connected to the internet, they can be used as entry points for cyber attackers to gain access to a network. Once attackers are able to gain access to a network, they can use the connected devices to launch further attacks or steal sensitive information. Another significant security challenge of IoT is the lack of visibility and control over the devices. As IoT devices are often deployed in remote locations, it can be difficult to monitor and manage them. This lack of visibility and control makes it difficult to identify and respond to security threats in a timely manner. To address these challenges, it is important to adopt a holistic approach to IoT security. This includes implementing security by design, where security is integrated throughout the entire product development process. It also includes implementing security measures such as encryption, firewalls and secure boot processes. Additionally, it is important to ensure that all IoT devices are regularly updated and patched to protect against known vulnerabilities. In conclusion, IoT technology has the potential to change the way we live, work, and communicate, but it also poses significant security challenges. It is important for individuals, organizations, and society as a whole to be aware of these challenges and to take steps to address them in order to ensure the secure and safe deployment of IoT devices.

C. *Communication Protocols*

The Internet of Things (IoT) is a network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to collect and exchange data. In order for these devices to communicate and exchange data, they rely on communication protocols. Communication protocols are the set of rules and standards that govern the exchange of information between devices. One of the most widely used IoT communication protocols is TCP/IP, which stands for Transmission Control Protocol/Internet Protocol. This protocol is responsible for routing data packets between devices over the internet. It is based on the same principles as the traditional internet and is used for many IoT applications such as web browsing and email. Another important IoT communication protocol is MQTT, which stands for Message Queue Telemetry Transport. It is a lightweight protocol designed for low-power devices and networks with limited bandwidth. It is commonly used in IoT applications such as sensor networks and machine-to-machine communications. Bluetooth is another popular IoT communication protocol. It is a wireless technology that allows devices to communicate over short distances. It is used in a wide range of IoT applications, including wearables, smart home devices, and industrial automation. Zigbee is a communication protocol that is specifically designed for IoT applications. It is a low-power, low-cost, and low-data-rate wireless communication protocol that is well-suited for devices that have limited power and processing capabilities. It is commonly used in smart home devices, building automation, and industrial control systems. Another protocol that is gaining popularity in IoT communication is LoRaWAN, which stands for Long Range Wide Area Network. It is a low-power, wide-area network protocol that allows for long-range communications between devices. It is well-suited for IoT applications such as smart cities, agriculture, and logistics. In addition to these protocols, there are many other IoT communication protocols that are used in various applications such as Zigbee, Z-Wave, CoAP, DDS, and AMQP. In order to ensure the interoperability and scalability of IoT systems, it is important to adopt standard communication protocols and to allow devices to communicate with different protocols. In conclusion, IoT communication protocols are an essential component of IoT systems, as they allow devices to communicate and exchange data. The selection of the right protocol depends on the specific requirements of the application, such as the type of data being exchanged, the range, power and cost constraints. As IoT technology evolves, new protocols will emerge to meet the new requirements of IoT applications.

D. *IoT security vs traditional IT security*

The Internet of Things (IoT) has the potential to revolutionize the way we live, work, and communicate by allowing everyday objects to communicate with each other and with us. However, as IoT technology becomes more widely adopted, it is important to consider the security implications of this technology. IoT security is different from traditional IT security in several ways. One of the main differences between IoT security and traditional IT security is the number and diversity of devices. IoT devices come in many different forms, from simple sensors to complex industrial machines. This makes it difficult to secure all of these devices, as they may have different capabilities and vulnerabilities. Additionally, many IoT devices are small, low-power and have limited processing power, storage, and memory, making it difficult to implement traditional security measures such as encryption and firewalls. Another difference between IoT security and traditional IT security is the lack of standardization. The vast number of IoT devices, platforms, and protocols currently in use makes it difficult to ensure that all devices are secure and that they can communicate with each other in a secure manner. This lack of standardization also makes it difficult for security professionals to protect against threats and to manage the security of IoT devices. IoT devices also pose a risk to the overall security of networks they are connected to. As IoT devices are often connected to the internet, they can be used as entry points for cyber attackers to gain access to a network. Once attackers are able to gain access to a network, they can use the connected devices to launch further attacks or steal sensitive information. Another significant security challenge of IoT is the lack of visibility and control over the devices. As IoT devices are often deployed in remote locations, it can be difficult to monitor and manage them. This lack of visibility and control makes it difficult to identify and respond to security threats in a timely manner. To address these challenges, it is important to adopt a holistic approach to IoT security. This includes implementing security by design, where security is integrated throughout the entire product development process. It also includes implementing security measures such as encryption, firewalls and secure boot processes. Additionally, it is important to ensure that all IoT devices are regularly updated and patched to protect against known vulnerabilities. In conclusion, IoT technology has the potential to change the way we live, work, and communicate, but it also poses significant security challenges. IoT security is different from traditional IT security because of the number and diversity of devices, lack of standardization and lack of visibility and control over the devices. It is important for individuals, organizations, and society as a whole to be aware of these challenges and to take steps to address them in order to ensure the secure and safe deployment of IoT devices.

Both Wireless Sensor Networks (WSN) and the Internet of Things (IoT) face a multitude of security threats that can compromise their functionality and integrity. In WSN, attacks such as spoofed routing information, selective forwarding, sinkhole attacks, Sybil attacks, and wormholes pose significant risks. Additionally, replay attacks, denial of service attacks, man-in-the-middle attacks, traffic analysis attacks, acknowledgement spoofing, and brute force attacks are prevalent in both WSN and IoT environments. These threats range from disrupting communication paths to compromising the confidentiality and integrity of transmitted messages. Understanding and addressing these security challenges is crucial for safeguarding the reliability and effectiveness of both WSN and IoT deployments.

There are various threats that can affect a Wireless Sensor Network, few of them are:

A. *Spoofed, altered, or replayed routing information:*

In this attack an attacker can create routing loops, generate false messages regarding routing updates, increase end to end delay, etc.[6]

B. *Selective forwarding:*

Some malicious nodes can delay or stop the transmission of messages by refusing to forward certain messages. In this case some messages are not propagated further. The malicious node can also behave like a black hole which rejects all the received messages. It will result in loss or drop of messages.[6]

C. *Sinkhole attacks:*

In this the attacker forces all the traffic of a specific area to pass through a compromised node.[6]

D. *Sybil attacks:*

In this a single node presents multiple identities to other nodes.[4]

E. *Wormholes:*

In this an attacker can capture messages and replays them to different nodes or in different parts by means of a tunnel.[6]

F. *Replay Attack:*

An attacker copies a forwarded packet and sends out the copies of the captured or intercepted traffic repeatedly and continuously to the destination node in order to exhaust the power source i.e. battery of the node , or to base stations in order to block the communication which results in degradation of network performance.

G. *Denial of service attack:*

The goal of this is to make the network unavailable for the legitimate users. One common method of implementing this attack is to consume all the resources by sending a large number of false requests so that the network is not able to provide the intended services and cannot communicate with the authenticated entities in the network [6]. The most common attack in Wireless sensor networks is to flood the base station or the sink node by sending a large number of false communication requests so that it cannot communicate with registered sensor nodes which lead to the failure of tasks assigned to the network.

H. *Man in Middle Attack:*

The man-in-the-middle attack is a form of active attack in which the attacker establishes connections with the entities and transfers messages between them and makes the entities believe that they are communicating with each other outside a private connection. The attacker will be able to intercept all messages exchanging between the two entities and also sends new Messages.

I. *Traffic Analysis Attack:*

In this the attacker node attempts to examine the traffic to know the message length, communication delay, message pattern, message encoding techniques, frequency of communication etc. Traffic analysis helps in implementing other attacks which involves violation of integrity and confidentiality of messages.

J. *Acknowledgement spoofing:*

The goal is to convince the sender that a dead node is still alive. All the information sent to the weak links or dead node can be removed by the attacker. [6]

K. *Brute Force Attack:*

A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you find the correct one. This type of attack may take a long time to complete. A complex password can make the time for identifying the password by brute force long.[2]

III.Security Requirements

Security requirements in both Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) are paramount for ensuring the resilience and integrity of these interconnected systems. The common security requisites include, Following are the security requirements:

• *Availability:* It ensures the availability of the services offered by wireless sensor networks or by a single sensor node. Resources should be available whenever required. The availability of resources can be mollified by denial of service attack [6].

• *Authentication:* It ensures that the entities involved in the communication are authenticated prior to the transmission of messages. The data and information should not b e available to the unauthorized no des. Only the authorized or registered no des should b e given available resources. Sensor nodes, Base station and cluster heads should b e authenticated through a proper mechanism to avoid a number of attacks possible such as impersonation attack, man in the middle attack, information theft etc. Authentication mechanism ensures that the control information or data is originated from the correct source as well as received by authenticated node [6],[7].

• *Authorization:* It ensures that only authorized nodes are involved in the communication[9].

• *Integrity and freshness:* It ensures that the received message has not been changed i.e. the message must be received as it was sent by the source node. The message should be a fresh message. The sensor node or the base station must be capable of rejecting the replayed message. Adversary should not be able to forge the communication packet.

•*Confidentiality:* It provides privacy for wireless communication channels so that the messages are not dropped or changed by an adversary. The messages exchanged between the sensor nodes or with the base station must be kept secret. The communication information must be known to the source and the destination nodes.

•*Re-authentication:* Re Authentication must involve less communication and computational overhead than the initial authentication.

•*Untraceability:* In re-authentication of a node, source should only be able to remember the identity of the node but not direction.

•*Key Freshness:* The communicating entities should be able to verify whether the key is generated during the current session or not.

•*Node/Sink Resiliency:* If a node is compromised by an adversary it should not have any effect on the network. It is a practical threat as sensor nodes are deployed in remote areas or hostile environments.

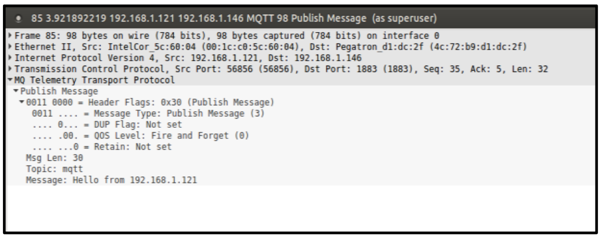
Proposed Model

Authentication stands as a cornerstone in Wireless Sensor Networks (WSNs) to counter potential threats in unattended environments. Without robust authentication mechanisms, adversaries exploit vulnerabilities, impersonate nodes, and compromise network integrity. This paper proposes a triple-layered security approach integrating self-signed SSL certificates, username-password authentication, and topic verification to fortify communication between nodes. Our method ensures secure data transmission, thwarting intrusion attempts and guaranteeing data integrity. Simulation results validate the effectiveness of our approach, highlighting its resilience against various attacks.

Wireless Sensor Networks (WSNs) deploy sensor nodes in diverse environments, necessitating robust security measures to prevent unauthorized access and data manipulation. This section outlines the importance of authentication and proposes a novel security paradigm integrating SSL certificates, username-password authentication, and topic verification.

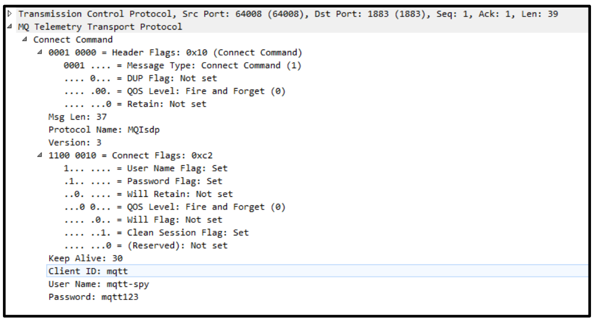
We delve into existing authentication techniques, highlighting their limitations and vulnerabilities. Traditional methods lack comprehensive security, exposing networks to potential breaches. The need for a robust, multi-layered approach to address these shortcomings is emphasized.

Our proposed algorithm combines SSL certificates, username-password authentication, and topic verification to establish secure communication channels between nodes. We detail each layer's functionality and their collective role in safeguarding network integrity.



```
85 3.921892219 192.168.1.121 192.168.1.146 MQTT 98 Publish Message  (as superuser)
▸Frame 85: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸Ethernet II, Src: IntelCor_5c:60:04 (00:1c:c0:5c:60:04), Dst: Pegatron_d1:dc:2f (4c:72:b9:d1:dc:2f)
▸Internet Protocol Version 4, Src: 192.168.1.121, Dst: 192.168.1.146
▸Transmission Control Protocol, Src Port: 56856 (56856), Dst Port: 1883 (1883), Seq: 35, Ack: 5, Len: 32
▾MQ Telemetry Transport Protocol
 ▾Publish Message
  ▾0011 0000 = Header Flags: 0x30 (Publish Message)
    0011 .... = Message Type: Publish Message (3)
    .... 0... = DUP Flag: Not set
    .... .00. = QOS Level: Fire and Forget (0)
    .... ...0 = Retain: Not set
   Msg Len: 30
   Topic: mqtt
   Message: Hello from 192.168.1.121
```

Fifure1: Tracing messages using WireShark-I



```
▷ Transmission Control Protocol, Src Port: 64008 (64008), Dst Port: 1883 (1883), Seq: 1, Ack: 1, Len: 39
◿ MQ Telemetry Transport Protocol
   ◿ Connect Command
      ◿ 0001 0000 = Header Flags: 0x10 (Connect Command)
           0001 .... = Message Type: Connect Command (1)
           .... 0... = DUP Flag: Not set
           .... .00. = QOS Level: Fire and Forget (0)
           .... ...0 = Retain: Not set
        Msg Len: 37
        Protocol Name: MQIsdp
        Version: 3
      ◿ 1100 0010 = Connect Flags: 0xc2
           1... .... = User Name Flag: Set
           .1.. .... = Password Flag: Set
           ..0. .... = Will Retain: Not set
           ...0 0... = QOS Level: Fire and Forget (0)
           .... .0.. = Will Flag: Not set
           .... ..1. = Clean Session Flag: Set
           .... ...0 = (Reserved): Not set
        Keep Alive: 30
        Client ID: mqtt
        User Name: mqtt-spy
        Password: mqtt123
```

Figure2: Tracing messages using WireShark-II

Our study introduces a robust triple-layered security approach for Wireless Sensor Networks, addressing authentication challenges and ensuring data integrity. The proposed solution offers enhanced protection against intrusions, making it a viable choice for securing IoT deployments in diverse environments.

Experiment Analysis

In our experimentation, we compared the security efficacy of MQTT (Message Queuing Telemetry Transport) and MQTTS (MQTT over TLS) protocols. Our analysis revealed that MQTTS offers superior security features compared to MQTT. MQTTS utilizes a secure port along with encrypted techniques and additional parameters, rendering it more robust and reliable for communication. To assess the security levels of both protocols, we conducted data transmission tests in both directions. Our findings indicate a significant disparity in security levels between MQTT and MQTTS. Specifically, MQTT exhibited lower security measures compared to MQTTS, affirming the latter as the preferred choice for secure communication in WSNs.

Overall, our experiment analysis underscores the critical importance of choosing secure communication protocols, such as MQTTS, to mitigate security risks and ensure the integrity of data transmission in Wireless Sensor Networks.

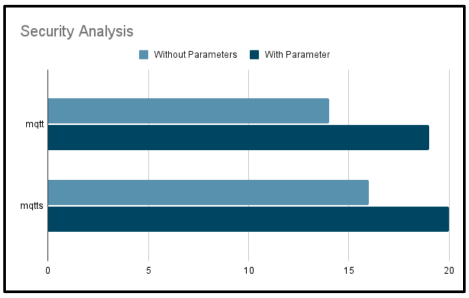


Figure 3: Security breach analysis on IoT devices

III. Conclusion

Security is paramount whenever sensitive information traverses between nodes, necessitating high-level protection to safeguard against virtual threats. With advancements in sensor technology and hardware, it's imperative to continually upgrade security protocols to ensure data integrity and network resilience. Wireless Sensor Networks (WSNs), comprising sensor nodes deployed across fields, are particularly vulnerable to intrusions, posing risks of data compromise and network disruption. To address these security challenges, it's essential to identify potential attacks on Next Generation WSNs. Various security protocols offer protection against attackers, yet adaptation to evolving threats remains crucial. Drawing insights from existing research, we propose an algorithm designed to facilitate secure communication among sensors utilizing the MQTTS IoT protocol. This algorithm ensures comprehensive security measures at each communication level, mitigating risks posed by masquerade attacks, man-in-the-middle attacks, replay attacks, password guessing attacks, denial-of-service (DoS) attacks, and other malicious activities. By fortifying communication channels and implementing robust security measures, our proposed algorithm provides a resilient defense mechanism against diverse forms of attacks, thereby safeguarding sensitive data and preserving network integrity in Next Generation WSNs.

Acknowledge:

I extend my sincere gratitude to my mentors, **Dr. Kulwinder Singh** and **Vijay Paul Singh,** for their invaluable guidance and support throughout the research process. Their expertise and encouragement have been instrumental in shaping the direction and outcomes of this paper.

References

1. Akyildiz, Ian F., et al. "A survey on sensor networks." Communications magazine, IEEE 40.8 (2002): 102-114.
2. Ling, Chung-Huei, et al. "A Secure and Efficient One-time Password Authentication Scheme for WSN." *International Journal of Network Security*19.2 (2017): 177-181.
3. Tsuji, Takasuke, and Akihiro Shimizu. "One-time password authentication protocol against theft attacks." *IEICE transactions on communications* 87.3 (2004): 523-529.
4. Arampatzis, Th, John Lygeros, and Stamatis Manesis. "A survey of applications of wireless sensors and wireless sensor networks." *Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*. IEEE, 2005.
5. Tsudik, Gene. "Message authentication with one-way hash functions." *INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*. IEEE, 1992.
6. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
7. Dogra, Heena, and Jyoti Kohli. "Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey." *Indian Journal of Science and Technology* 9.47 (2016).
8. Lamport, Leslie. "Password authentication with insecure communication."*Communications of the ACM* 24.11 (1981): 770-772.
9. SHABANA, K., FIDA, N., KHAN, F., JAN, S., REHMAN, M.. Security issues and attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), North America, 5, jul. 2016.
10. Büsching and L. Wolf, "The Rebirth of One-Time Pads—Secure Data Transmission from

BAN to Sink," in *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 63-71, Feb. 2015.

11. P. Singh, M. Hussain and C. K. Raina, "Authentication of base station by HDFS using trust based model in WSN," *2016 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, 2016, pp. 1-5.
12. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
13. Dogra, Heena, and Jyoti Kohli. "Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey." *Indian Journal of Science and Technology* 9.47 (2016).
14. Lamport, Leslie. "Password authentication with insecure communication."*Communications of the ACM* 24.11 (1981): 770-772.
15. SHABANA, K., FIDA, N., KHAN, F., JAN, S., REHMAN, M.. Security issues and attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), North America, 5, jul. 2016.
16. Büsching and L. Wolf, "The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink," in *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 63-71, Feb. 2015.
17. P. Singh, M. Hussain and C. K. Raina, "Authentication of base station by HDFS using trust based model in WSN," *2016 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, 2016, pp. 1-5.
18. W. Choi and I. Y. Lee, "A key distribution system for user authentication using pairing-based in a WSN," *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, 2017, pp. 1-4.
19. S. S. Abd El dayem, M. R. M. Rizk and M. A. Mokhtar, "An efficient authentication protocol and key establishment in dynamic WSN," *2016 6th International Conference on Information Communication and Management (ICICM)*, Hatfield, 2016, pp. 178-182.
20. H. Moon, U. Iqbal and G. M. Bhat, "Light weight Authentication Framework for WSN," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 3099-3105.
21. P. Joshi, M. Verma and P. R. Verma, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN," *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kumaracoil, 2015, pp. 527-532.
22. P. Banerjee, T. Chatterjee and S. DasBit, "LoENA: Low-overhead encryption based node authentication in WSN," *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Kochi, 2015, pp. 2126-2132.
23. Mohamed Hammi, Erwan Livolant, Patrick Bellot, Ahmed Serhrouchni, Pascale Minet. A Lightweight IoT Security Protocol. *1st Cyber Security in Networking Conference (CSNet2017)*, Oct 2017, Rio de Janeiro, Brazil.
24. Armando, Alessandro, et al. "The AVISPA tool for theautomated validation of internet security protocols and applications." *International conference on computer aided verification*. Springer, Berlin, Heidelberg, 2005.
25. Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." *Internet of Things* 5 (2019): 41-70.
26. Ramotsoela, Daniel, Adnan Abu-Mahfouz, and Gerhard Hancke. "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study." *Sensors* 18.8 (2018): 2491.
27. Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." *2014 international conference on privacy and security in mobile systems (PRISMS)*. IEEE, 2014.
28. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.
29. Cerullo, Gianfranco, et al. "Iot and sensor networks security." *Security and Resilience*

in Intelligent Data-Centric Systems and Communication Networks. Academic Press, 2018. 77-101.

30. Tang, Xiao, Pinyi Ren, and Zhu Han. "Jamming mitigation via hierarchical security game for iot communications." *IEEE Access* 6 (2018): 5766-5779.
31. Thakkar, Ankit, and Ritika Lohiya. "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges." Archives of Computational Methods in Engineering 28.4 (2021): 3211-3243.
32. Lin, Yun-Wei, Yi-Bing Lin, and Chun-You Liu. "AItalk: a tutorial to implement AI as IoT devices." IET Networks 8.3 (2019): 195-202.