Security and Threats of RFID and WSNs: Comparative Study

Ghada Hisham Alzeer[1], Ghada Sultam Aljumaie[2], Wajdi Alhakami[3]
Taif University, College of Computers and Information Technology, Taif, KSA

***Abstract*—The Internet of Things (IoT) has garnered significant attention from people with growing changes in human life over the last few years. IoT is a network of a group of smart devices that use sensors to collect information and conduct events in their environments. The information can then be shared on the Internet. IoT uses a range of technologies and finds various applications such as smart homes, environmental monitoring, and healthcare. In this paper, we conducted a comparative study to analyze the difference between two technologies—Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID). It is pertinent to note that these technologies would not be effective without incorporating security aspects due to a potential number of threats and attacks on the network. This paper provides a comprehensive review of the recent approaches to securing RFID and WSNs. We have carefully chosen most of these studies to investigate only the recent technique from 2017 to 2020. The paper also highlights common attacks on RFID and WSNs and the secure authentication mechanisms on these technologies. It further provides a different way of detecting varying attacks in RFID and WSNs.**

***Keywords*—Security; IoT; WSN; RFID**

I. Introduction

The Internet of Things (IoT) is a network of a group of smart devices that use sensors to collect information and conduct events in their environments. The information can then be shared on the Internet. IoT has witnessed rapid growth recently; Cisco reported a remarkable increase in the number of IoT devices to nearly 50 billion in 2020 [1]. IoT is used in several areas such as industrial automation (Industrial IoT), sensing applications in smart homes, traffic control, and other applications that deal less with sensors and more with data analysis. Industrial IoT and smart homes deal more with sensors and less with data analysis. The IoT that focuses more on data analysis is used in the transformation of business processes (BPs) such as banking, organizational operations, and healthcare optimization [2][3].

IoT uses a wide range of technologies such as Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), and Near Field Communication (NFC), as shown in Fig. 1 [4].

Among these technologies, WSNs and RFID are mainly used and have become the two main pillars [4].

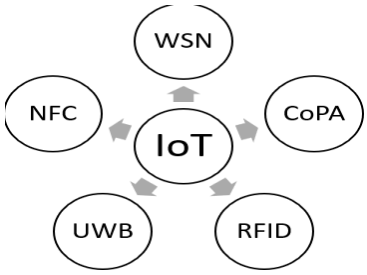

Fig. 1. IoT Technologies.

II. Radio Frequency Identification

RFID can be defined as the nonlinear network system that replaces barcodes and QR codes for a rapid response and relies on radio waves to capture and disseminate information [5]. It was first designed in 1948 and took many years to mature and become affordable and reliable for widespread use. Some considered RFID as the most widespread computing technology in history [6]. Today, it has become an important and integral part of current technologies such as computing and IoT [7], [8]. RFID is composed of four parts: tag, an antenna and transceiver tag processor, a database, and a backend. Tags are connected to items to store their information, the RFID reader reads the data coming from the tag and writes it to the transponder, and the backend database links that data with records. See Fig. 2 [6], [5], [9].

Active tags include a battery that allows automatic data transfer to the readers. On the other hand, passive tags are triggered by the electromagnetic waves of the reader.

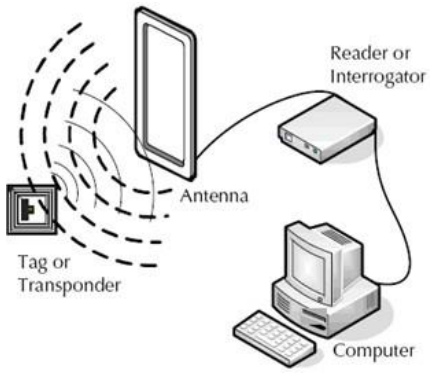

Fig. 2. Components of RFID.

These tags are more commonly used than their active counterparts on the account of their low cost and infinite life. Tags contain read-only memory (ROM), that stores data classified as security data, system ID, and OS instructions and volatile read/write or random access memory (RAM) that stores data during transmission and response [6], [5]. They are used in various applications such as transportation, logistics, manufacturing, healthcare/pharmaceutical industry, processing, and security [9], [7]. With the advent of IoT technology and the development of signal processing technology and distributed network technology for IoT nodes to acquire signals, a model has been established to acquire radio frequency signals within an IoT environment to add more features that are important in many fields [10].

III. Wireless Sensor Networks

WSNs have been becoming the area of interest for various researchers due to the rapid development of wireless technology and embedded electronics. WSN contains node sensors – small devices used to sense their current environment [11]. It is a distinct type of network containing small distributed devices called sensor nodes. They are considered low-power devices that communicate with each other without infrastructure and used for sensing and collecting data through wireless communication [12]. The basic components of sensor nodes include microcontrollers that perform data processing and control other components to perform their functions [13]. Transmitter and receiver use radio waves to send and receive data over wireless networks. Wireless sensors are powered by batteries or a power source. The choice of power source depends on the deployment environment and energy availability of the applications [14]. As provided in Fig. 3, EEPROM or Flash memory [15] are also the key components of sensor nodes.

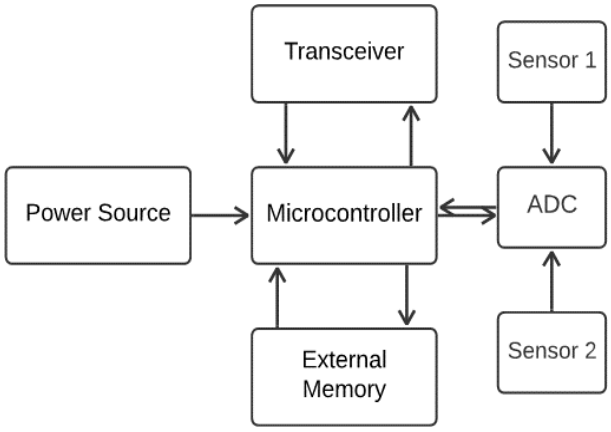

Fig. 3. Basic Components of WSN Node.

IoT model enables computers to access data about objects and the environment without human interaction [10]. Such model involves the integration of 'physical things' and IT infrastructure to transfer and collect data through a wireless network. It further allows to understand, interpret, communicate, and exchange data without any communication units and human participation [16], [10]. WSN plays an important role in IoT applications [17], as it provides IoT applications with high sensing and operational capabilities. WSNs are the eyes and ears of IoT; they convert physical phenomena into digital signals and transmit these signals for processing and analysis [18]. Today, there is a myriad of applications that depend on WSN and IoT technology, such as patient monitoring (measuring blood pressure, heart rate, and oxygen concentration) [19] and smart homes and buildings [17]. With the tremendous growth of IoT devices with high connectivity, there has been an increasing concern about their security and the data they store and transmit across various devices. Moreover, there has been an increase in the number of attacks on these devices. The current security challenges of IoT devices are generally due to their limited capacity, processing power, and battery life [20]. These limitations have made IoT devices a target for attackers such as hackers, hacktivists, and cybercriminals. Cybersecurity is therefore important to secure IoT and ensure protection from malicious activities such as data theft, modification, unauthorized access attempt, or network attack [20].

RFID and WSN technologies are widely used in many applications, such as in the scientific or medical fields and even in our home life, so achieving security in them is very important because they may deal with very sensitive data. Therefore, security became sour main motivation in this paper, we discussed the security requirements and how to achieve them, the common attacks based on current research also discussed protection and detection mechanisms suggested by other researchers. Our research paper is one of the few that discusses both RFID and WSN in terms of security requirements and common attacks.

This paper is divided into nine sections: Section IV introduces the required security applied in RFID and WSNs. The common threats and attacks on RFID and WSNs are presented in Section V. The following Sections VI and VII, respectively focus on the security of RFID followed by WSNs for achieving secure authentication, ensuring confidentiality, and detecting common attacks on both. In Section VIII we discussed the papers mentioned in our paper from various aspects. Lastly, we mentioned our future work on RFID and WSNs in Section IX.

IV. Security Requirements of Internet of Things

To secure IoT deployment, we classified IoT security into three categories as listed in Fig. 4.

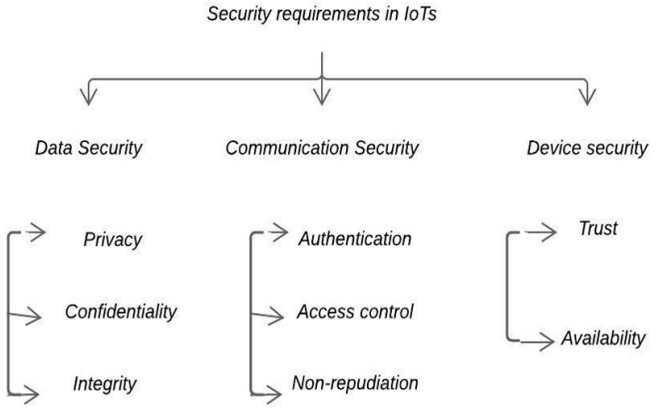

Fig. 4. Security Requirements of IoT.

A. Data Security (Privacy, Confidentiality, and Integrity)

Privacy includes the ability to hide personal information and control the use of that information [21]. There are several techniques to deal with data privacy, such as pseudo-random number generators, block and stream cipher, and anonymization [22]. Confidentiality, on the other hand, means that the communication between the sender and receiver must be protected from any malicious or unauthenticated users [23]. The integrity of data stored on remote servers must be protected on the IoT framework that preserves stored data, ensures its correctness, and provides protection from any loss or tampering. Many protocols were designed to achieve data integrity by using either encryption or anonymization techniques [24].

B. Communication Security (Authentication, Access Control, and Non-repudiation)

Authentication before communication is the key to the success of IoT and an important component of any security model [25]. The two parties must authenticate their communication [26]. It ensures the identification of these parties before making any contact [25]. Identity verification is carried out using several methods such as passwords, digital certificates, lightweight cryptography algorithms, or biometric identification [27]. IoT authentication is a complex process as it involves heterogeneous network authentication. Before joining a network, identification and authentication must be applied to all objects or sensors. It is imperative to note that IoT requires a unique code (UID) to identify each entity in the network [28]. Access control involves the authorization of users. A system administrator specifies access privileges for different users with which they can only access the relevant parts of system resources to protect their resources and information [29]. Access control algorithms can be divided into five types [22]:

1) Task-based Access Control (RBAC): RBAC manages all user-assigned access to roles and grants multiple user permissions to roles. For more efficiency, roles can be organized into a hierarchy, allowing some roles to inherit permissions from others. RBAC is generally used to simplify access control. It reduces complex protection management and endorses the analysis of user-assigned permissions [30].

2) Organization-based Access Control (OrBAC): An improved version of the RBAC model. However, it has a time limitation and supports the periodic activation of roles [31].

3) Capability-based Access Control (CapBAC): CapBAC gives each user a capability – a key that gives access rights. The admin then decides if the user can access the network by checking the validity of the key [32].

4) Attribute-based Access Control (ABAC): Depending on the characteristics of the requester and resource, users do not need to know the resources before they submit the request. ABAC has become significant recently, particularly in web service applications [33].

5) Trust-based Access Control (TBAC): It gives users a high level of trust to support dynamically changing permissions assigned to them [34]. Non-repudiation refers to a situation where data must be checked in a way that a sender has sent a message and it can be rejected or a receiver cannot refuse receipt of the message [35]. It can be achieved using Public Key Cryptography (PKC) and Digital signature [36].

C. Device Security (Trust and Availability)

Trust is critical to achieving security in an IoT system. Additionally, IoT devices must be trusted to prevent unwanted actions by malicious nodes [37]. The stages of trust-building start from the establishment stage to the operational and transmission stages of IoT. This trust is formed by two mechanisms – key generation and token. A key generated by the entitlement system is allocated to each new unit and introduced by a consumer device. Token, on the other hand, is generated by the owner or producer and coupled with an RFID indication of the device. [38]. In IoT, the availability of hardware and software remains essential. Hardware availability implies to the availability of devices for IoT applications at all times. Software availability is the ability to provide services at any place and time [39]. Moreover, in IoT devices, all data should be available to users whenever they need it. The devices and services must also be available and reachable whenever the users need them at the right time to achieve IoT expectations [38].

V. Attacks on Radio Frequency Identification and Wireless Sesnsor Network

In this section, we highlight some of the common attacks on RFID and WSNs.

A. Security Threats and Attacks on Radio Frequency Identification

The author in [40] summarized several threats directed towards RFIDs. A key reason behind most of these attacks is the security of the communication channel between the user and tags. A group of famous attacks on RFID is revealed below:

1) Action threat: In this type of threat, the tags possessed by an individual are monitored and predicted for his future intentions and actions.

2) Association threat: Electronic Product Code (EPC) tag is a unique number for each product. When a consumer purchases a product, a link between the consumer's identity and the product is created.

3) Location threat: By tracking the tags associated with a user's site, an attacker could obtain the exact location of the user.

4) Preference threat: It is possible to obtain consumer preferences illegally by tracking unique EPC tags for each product that identify company name and product type.

5) Constellation threat: It is one of the threats where the illegal parties track transactions between users.

6) Breadcrumb threat: Also known as electronic breadcrumbs, this threat occurs when a consumer buys a product that creates a link between his/her identity and EPC tag product number. Consequently, when the consumer gets rid of this product, the link is not broken and can be used.

Some common attacks on RFID systems mentioned in paper [41] are summarized in Table I.

TABLE I. SUMMARY OF SECURITY ATTACKS ON RFID TECHNOLOGY

Attacks	*Descriptions*
Temporariy disabling tags	The signs may be unintended – any event due to natural factors or interference of frequencies. They may also be intentional, such as Passive Interference and Active Jamming.
Removal or destruction of RFID readers	Because of its small pilgrimage, an RFID reader is vulnerable to attackers who use it to obtain data or modify it.
Relay attacks	Also known as MITMA; the intruder intercepts the radio signal between the sender and receiver and may modify it.
Attacks on the tags	Making a copy of the tag (Cloning) or impersonating the tag (Spoofing).
Reader attacks	Impersonating a legitimate reader (Impersonation) or recording the legitimate RFID tags (Eavesdropping).
Unauthorized tag reading	Since authentication protocol RFID tags are not supported, an attacker can read the contents of the RFID tags.
Tag modification	The data on RFID tags can be modified or deleted by the attacker.
Middleware attacks	The attacker uses RFID tags to either cause an attack (Buffer Overflows or end RFID middleware) or spread malicious code with an attack (Malicious Code Injection)
Covert channels	Using RFID tags, an attacker could create unauthorized channels for transmitting data.
DoS	The attacker blocks or disconnects RFID tags service from users.
Traffic analysis	Attacks by monitoring and analyzing traffic patterns
Crypto	Uses encryption methods to break encryption algorithms and access data
Side-channel	Leverages the physical application of encryption algorithms

B. Security attacks and challenges of Wireless Sensor Networks.

Fig. 5 [42] generally demonstrates the classification of the common security threats and attacks in WSNs.

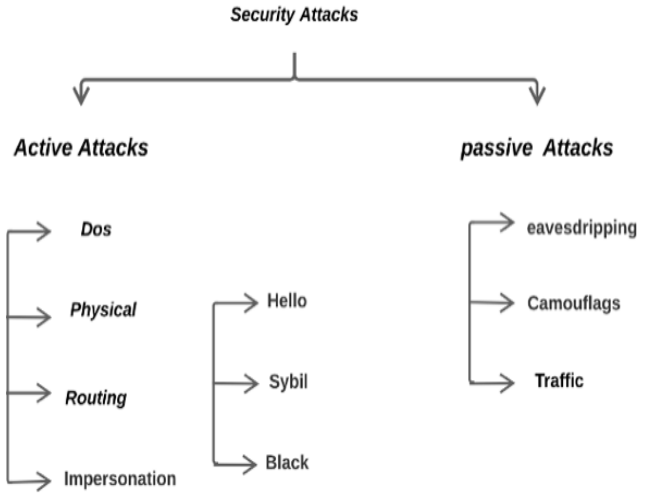

Fig. 5. Security Attacks in General.

The author in [43] notes Sybil attacks as the most common attacks observed in WSN, followed by wormhole and DoS attacks. DDoS attacks are relatively less on this type of network. The authors of paper [42] mentioned some common attacks on WSN systems, as shown in Table II.

TABLE II. SUMMARY OF SECURITY ATTACKS ON WSNS

Attacks	*Descriptions*
DoS	The attacker tries to sabotage the data and disable the system that reduces network efficiency
Sybil	In WSN networks, there are several sub-tasks such as duplicating information that you do not perform and assigning it to one node This node is attacked by Sybil Attacks, targeting the schemes of fault tolerance.
Blackhole	It is more severe than a Sally attack, as the attacker offers a shorter path to the nodes, acts as a black hole, and completely captures the data traffic. The attacker can also affect the data traffic.
HELLO Flood	This attack occurs in the network layer where the attacker fabricates hello, sends it to convince the sensor in WSN, and then changes the scenario
Wormhole	A common attack that occurs in two separate nodes carrying important parts of the message when a low-latency bandwidth is directed to them

VI. SECURITY IN RADIO FREQUENCY IDENTIFICATION TECHNOLOGY

This section includes an overview of previous works on RFID network security divided into several sections:

A. Authentication Protocols for Radio Frequency Identification

In [8], the authors introduced a new authentication protocol that offers an acceptable level of protection. It is also resistant to the risks reported in the article and evaluates the security of mutual authentication suggested by Wang and Ma. This review demonstrates the key security pitfalls of the protocol. Firstly, they presented two methods used by an opponent to make valid readers believe that they are dealing with a valid database. Next, they demonstrated how an adversary can turn an RFID reader into a legal database and introduced a new adversary model. Finally, they implemented an improved server method named ISMAP and demonstrated that this protocol provides sufficient protection against different types of attacks including the current adversary model discussed in the article. Additionally, the authors in [44] introduced a new lightweight RFID security authentication protocol (LRSAS). They analyzed the security properties of the protocol, containing data confidentiality and integrity (DCI), replay attack (RA), desynchronization attack (DA), impersonation attack (IA), tracking attack (TA), denial of service attack (DoS), and forward security (FS). Finally, they compared the LRSAS protocol with other protocols in terms of communications, computation, and storage. The authors also showed that the protocol is efficient in terms of security and cost requirements.

In [45], the authors presented two lightweight RFID protocols that provide security, identity authentication, and privacy and have multiple tag groups. They used a filtering process to decrease collision between tags, sleep activation

mechanism, RFID system, and computing load. They also used a pseudorandom number generator (PRNG) and hash function to encrypt all sessions between the reader and tags. These protocols can resist eavesdropping, replay, and desynchronized attacks.

In [46], the authors introduced a group-based authentication protocol for the RFID system. It uses only mod operation and bitwise XOR. Additionally, two standard measures were used to measure the privacy of the system, resulting in anonymity when the opponent conducts numerous operations. Experimental results showed that their scheme maintains a high level of privacy when some tags are compromised. After the analysis, the authors proved that their protocol is safe and effective for a reduced RFID system.

B. Security Communication in Radio Frequency Identification to Ensure Confidentiality

In [47], the authors studied elliptical curve coding (ECC) protocol based on RFID security protocol, as it has several important features such as high strength ECC encryption that provides high security for communication and access to tag memory data. The new protocol relies on simple calculations such as XOR and bitwise AND which reduces complex calculations for low-cost tags. The authors analyzed their protocol for security and performance by using BAN logic. The analysis demonstrated that the protocol can provide mutual authentication of the tags and reader at the same time.

C. Detection Mechanisms in Radio Frequency Identification

In [48], the authors presented new effective research to preserve the privacy of cloning, as it is relevant and effective to preserve the privacy to explore cloning for all supplies that support RFID technology. They analyzed and evaluated the proposed mechanism through simulations which proved to be effective under various conditions. They then designed and implemented Multilateral Secure Computing (SMC) protocols to implement private-preserving for clone estimate that shows changes in efficiency regarding similar programs inside the existing SMC system. In [49], the authors discussed important problems associated with tag detection in RFID systems, including reader collision avoidance, optimal tag reporting, and optimal tag coverage problems. These issues occur due to the inability of collision intrusion detection and RFID readers that transmit packets created by other readers and poor access to resources in RFID tags on the account of severe limitations.

In [50], the authors presented an approach that implements MAC, routing, and application layer outlier detection processes in three different regions. Multiple invigilator regions executed internal or external detections after data collection. The proposed system has consequently been found to be efficient in terms of performance indicators. These indicators may be internal or external based on service quality. Various internal indicators used to measure the stability of structures are DI, RMSSDI, RSI, SI, CHI, and DBI. Additionally, various external indicators used to measure the stability of structures are FI, NMII, PI, and EI. Both internal and external indicators confirm the formation of structure and external detection processes. Furthermore, two indicators based on QoS (productivity and jitter) are used in this work.

The authors in [51] presented an efficient hash-based RFID authentication protocol that provides miss-tag detection. They presumed that for each user, an authentication system would validate large quantities with RFID tags inside its ranges. Their protocol can detect and reset lost tags if the missing tag can rejoin the system. After analyzing the protocol in terms of security, they proved that it can provide adequate security guarantees, resist various attacks, and offer better performance. Moreover, the protocol achieves both security and performance characteristics. See the summary of security in RFID technology in Table III.

TABLE III. DIFFERENT SECURITY TECHNIQUES ON RFID

Paper	Year	Techniques	Contribution
[8]	2020	GNY Logic and Scyther	The authors introduced a modern authentication protocol that offers an acceptable level of protection and is immune to security risks.
[44]	2020	Hash function, PRG, SKINNY encryption algorithm	The authors introduced a new lightweight RFID security authentication protocol (LRSAS). They analyzed security properties of the protocol that contain Data Confidentiality and Integrity (DCI), Replay Attack (RA), Desynchronization Attack (DA), Impersonation Attack (IA), Tracking Attack (TA), Denial of Service Attack (DoS), and Forward Security (FS).
[45]	2020	Hash function, PRG, activate-sleep mechanism,and filtering process	The authors presented two lightweight RFID protocols that provide security, identity authentication, and privacy.
[46]	2020	XOR operation	The authors introduced a group-based authentication protocol for the RFID system.
[47]	2016	XOR and bit wise AND	The authors studied elliptical curve coding (ECC) protocol based on RFID security protocol as it has several important features
[48]	2010	Algamal encryption system	The authors presented a novel efficient, private information mechanism to detect clones for RFID-enabled supply chain operations.
[49]	2009	Tree flow algorithm	The authors discussed many important problems associated with tag detection in RFID systems, such as reader collision avoidance, optimal tag reporting, and optimal tag coverage problems.
[50]	2019	DI, RMSSDI, RSI, SI, CHI, DBI, FI, NMII, PI, and EI	The authors presented an approach that implements MAC, routing, and application layer outlier detection processes in three different regions. The multiple invigilator region executes internal or external detections.
[51]	2018	Hash function	The authors presented an efficient hash-based RFID authentication protocol that provides miss-tag detection.

VII. Security in Wireless Sensor Networks

In this section, many papers written on the security of WSNs have been compiled and divided into several sections as shown in the following:

A. Authentication Protocols for Wireless Sensor Networks

In [52], the authors mentioned weaknesses in traditional authentication methods found in IoT and suggested the use of a system based on WSN identity authentication and blockchain technology. Blockchain is a book of accounts that cannot be modified or tampered with and where transactions or data are generally recorded. They integrated blockchain decentralization with the nodes that formed the IoT structure. In a public blockchain, several private blockchains are connected and each private blockchain is connected between the cluster heads of a WSN. In the end, we have a hybrid blockchain for the whole network. The authors also created a model where the identification data was recorded between cluster head nodes and ordinary nodes. Finally, a connection authentication is done between these nodes. After analyzing the model, it became clear that the system has a greater and more efficient level of safety.

The researchers in [53] submitted a proposal to make the use of authentication protocols in WSN more secure and focused on reducing the cost as compared to other conventional protocols. They used the Altera DE2 demo board and implemented several corresponding device structures such as the Altera Cyclone II field-programmable gate array. Finally, they showed the waves produced from this process – 16702A – a logic analysis device. Additionally, the process XOR was used for encoding the key. The results showed the effectiveness of the experiment.

Paper [54] also mentioned many concerns about the difficulty of preventing smartcard stolen and off-line guessing attacks. To prevent these attacks, the paper suggested using a protocol that uses honey-list technology and relies on three-factor authentication. As the sensor performance is limited, the protocol also encodes the elliptic curve that relies on the public key and uses only hash functions. The authors performed a formal security analysis using the real-or-random (ROR) and Burrows Abadi Needham (BAN) models. For verification, they used simulation software called Automated Validation of Internet Security Protocols and Applications (AVISPA) that resulted as a safe protocol.

The author in [55] focused on lightweight and cost as the two main features; the authors saw that WSN devices need strong and light authentication protocols that can withstand any difficult environment. They proposed a model that uses XOR and hash functions. This model was effective in terms of reducing the use of resources and speed while maintaining data security.

B. Secure Communication in Wireless Sensor Networks to Ensure Confidentiality

There has been a growing need to guarantee the high security of WSNs used in various applications such as home, industrial, and healthcare. Therefore, paper [56] proposed a protocol that improves the security of WSN by distributing the main keys, identifying the node, and verifying the identity of messages in WSN. The password is updated and changed for the message verifier and connected to the dynamic node on the network. The authors concluded that this method outperformed previous methods. Subsequently, paper [57] used a scheme based on additive homomorphic encryption algorithm in WSN, whereby a symmetric-key homomorphic is used to provide more protection for the confidentiality of data. This key also combines the data with a homomorphic signature to achieve integrity. After decoding, the data is classified according to various symmetric-key homomorphic. Furthermore, after analyzing the results, it became clear that using this method is effective in reducing cost and increasing effectiveness in terms of protecting the data from any tampering during its transmission and ensuring the accuracy of its collection.

The author in [58] suggested the use of hybrid technology from Diffie-Hellman key exchange and Elliptic Curve cryptography. The combination of these two technologies allowed for increased security of data traffic, confidentiality, authentication, and time savings. These techniques are simulated, applied to a Java platform, and implemented in a WSN environment. The authors of [59] directed their efforts towards solving the security problems of sensitive data, as it traveled through WSN for various applications, by applying new technologies. They integrated discrete chaotic map and genetic cryptography as 2DES and 3DES for WSN, which increased the security regardless of limited resources. For a text and visual data, Henon map encryption was used due to its strong encryption. They encoded these processes under the Arduino microcontroller and determined that the attacker might need time depending on the speed of his device. They concluded that using random numbers increases the robustness of the system and prevents attacks. They preserve the confidentiality of data from unauthorized disclosure and collect it with high accuracy, as shown in Fig. 6.

To increase security and make IoT devices more independent, the authors in the paper [60] suggested the use of blockchain security features such as availability to users, data integrity, and various cryptographic tools. The model was applied to the WSNs that were used to measure moisture and temperature. It was found that the transmission of information between the nodes became more secure, independent, and less vulnerable to various types of attacks such a DoS and MITM attacks.

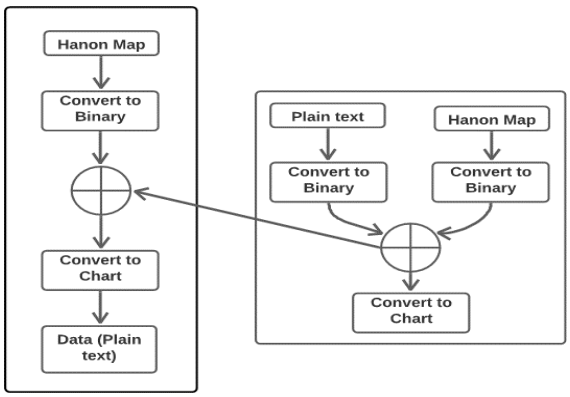

Fig. 6. General Block Diagram of Henon Map.

C. Detection Mechanisms in Wireless Sensor Networks

DoS jamming attack is one of the common attacks on WSN, as discussed in [61]. It aimed at sending many signals to jam the main signal. A denial of service occurred consequently and caused disruption of functions in the WSN nodes.

The authors in [61] proposed an exponentially weighted moving average (EWMA). They deployed an exponential moving variable that detects any change occurring in the traffic. The authors concluded that this model can accurately detect different jamming attacks and be used in situations where sensitive instantaneous information is transmitted.

Due to the sensitivity of information transmitted through WSN, a solution has been proposed in [62] to discover the unauthorized and intentional sequences of WSN. The sequence detection methodology in this paper relied on the use of MATLAB Simulink that uses an artificial neural network. In the first session, a large discrepancy in node values makes them a harmful contract for WSN. For the second session, the results of the regression of the artificial neural network for both packet delivery ratio (PDR) and energy consumption variables were analyzed. It was observed that ANN-based PDR is stronger and quicker than ANN-based energy usage. However, the results for both were good.

In the survey paper [63], a part of its objectives was to provide a comparison of different intrusion detection protocols of each WSN and IoT. It mentions the uses and efficiency of each type.

The authors in [65] aimed at using a new system that detects the sequence and has a longer residence time by adding a low-power resistance and survival continuity to IDS. The paper showed that nodes continue to work efficiently on algorithm strength, mobile nodes, and attack strength. See the summary of security in WSNs in Table IV.

TABLE IV. DIFFERENT SECURITY TECHNIQUES ON WSNS.

Paper	Year	Techniques used	Contribution
[52]	2020	Hybrid blockchain	The authors mentioned weaknesses in the traditional authentication methods of IoT and suggested the use of a system based on many WSN identity authentication with blockchain.
[53]	2015	XOR arithmetic	The researchers submitted a proposal to make the use of authentication protocols in WSN more secure and focused on reducing the cost as compared to other conventional protocols.
[54]	2020	Honey-list, three-factor authentication	The paper suggested using a protocol that uses honey-list technology and relies on three-factor authentication for preventing smartcard stolen and off-line guessing attacks.
[55]	2020	XOR and hash functions	The authors saw that WSN devices need strong and light authentication protocols and that can withstand any difficult environment.
[56]	2017	The protocol distributing the main keys, identifying the node and verifying the identity	The paper proposed a protocol that increases the security of the WSN by distributing the main keys, identifying the node also verifying the identity of the messages in the WSN.
[5]	2015	Symmetric-key homomorphic, homomorphic signature	The authors proposed a scheme based on an additive homomorphic encryption algorithm in WSN for the confidentiality of data.
[58]	2018	Diffie-Hellman, Elliptic Curve	Suggested the use of hybrid technology from Diffie-Hellman key exchange and Elliptic Curve cryptography. The combination of these two technologies allowed for increased security of data traffic, confidentiality, authentication, and time savings.
[59]	2020	Discrete chaotic map, genetic cryptography, Henon map	Solving the security problems of sensitive data, as it traveled through WSN for various applications, by applying new technologies. The authors integrated discrete chaotic map and genetic cryptography as 2DES and 3DES for WSN which increased security regardless of limited resources.
[60]	2020	Blockchain	To improve security and make IoT devices more independent, the authors suggested the use of blockchain security features such as availability to users, data integrity, and various cryptographic tools.
[61]	2018	Exponentially weighted moving average (EWMA)	The authors proposed an exponentially weighted moving average (EWMA). They deployed an exponential moving variable that detects any change occurring in the traffic. It can accurately detect different jamming attacks.
[62]	2020	Artificial neural network, MATLAB Simulink	Due to the sensitivity of information transmitted through WSN, a solution has been proposed by researchers to discover the unauthorized and intentional sequences of WSN. They relied on the use of MATLAB Simulink which uses an artificial neural network.
[63]	2019	Survey (e.g. Intrusion detection by cluster head, Hybrid anomaly detection..)	The paper provides a survey comparison of various intrusion detection protocols in both WSN and IoT. It mentions the uses and efficiency of each type.
[64]	2015	Low-power resistance and survival continuity to IDS	The paper aimed at using a new system that detects the sequence and has a longer residence time

VIII. DISCUSSION

This part focuses on discussing the above-mentioned recent techniques for protection and detection mechanisms. The discussion section has been divided into two parts:

A. Critical Review of Radio Frequency Identification Security

This section discusses the most important recent approaches which aim to secure an RFID environment. These approaches are selected as the most relevant and have novelty. For example, many research papers have discussed

authentication and their protocols are distinguished using lightweight encryption algorithms. They consume fewer resources during calculation and are more efficient compared to traditional encryption algorithms. They are also suitable for devices with limited computing power such as RFID. The authors in papers [8] took a few measures to overcome some of the flaws and introduced an improved protocol using Scyther and GNY Logic. These are two excellent ways to assess security for the protocol of cryptography. However, the protocol has a drawback – it does not take into account multi-server or multi-reader environments. In two other researches [44] [45], the authors used hashing function to encrypt all session between tags and reader that ensures data integrity. They also used a pseudo-random number process to strengthen the encryption, making it difficult for the attacker to guess the key used. Both protocols proved effective in protecting against many types of attacks such as restart attack (RA), trace attack (TA), denial of service attack (DoS), and security forwarding (FS). The difference between the two papers is that the authors in [45] used the SKINNY encryption algorithm for the data used by the tag and reader to achieve mutual authentication. In our opinion, their protocol was good because it balanced security requirements and costs. Additionally, the use of SKINNY was well-suited for a scenario where the server is connected to numerous lightweight devices. In [44], we liked that they used the activate-sleep mechanism efficiently and filtering process which reduced collision on the tags. In the paper [46], the authors not only used a pseudo system that provides a feature on the side of the tag but also used that feature in the reader to generate the nonce. Their protocol only uses bit-wise XOR operation in the authentication stage along with symmetric encryption and decryption. It was an excellent protocol, as it uses fewer resources in the tags to achieve arithmetic work and store data. Moreover, it maintains a high level of privacy when attacking some tags.

In the next section, we discussed RFID security communication to ensure confidentiality. The authors in [47] presented a protocol based on an elliptical curve for coding. From our point of view, their protocol has several advantages. It provides mutual authentication for the tag and reader and is good at resisting some of the common attacks related to RFID technology. Additionally, their protocol only relies on a few simple operations such as XOR and bitwise AND which reduces the complexity of computation in low-cost tags. In the following section, we discussed several research papers regarding detection mechanisms in RFID. The researchers in the [48] presented a novel, reliable, privacy-preserving mechanism for detecting clones for RFID-enabled supply chain operations. They used the Algamal encryption system, which is an asymmetric encryption system, in their protocol that achieved both authentication and confidentiality. Their protocol has been effective at detecting RFID supply chain clones. However, from our point of view, their protocol has many weaknesses such as the need for more robust hardware. They also need to reduce the security level to n/2 to improve the performance of their protocols. The authors in [49] provide a distributed and localized algorithm. They used a tree flow algorithm centered on the recursive direction of the binary tree for tag identifiers and the problem of tag collision where the reader initially sends a broadcast including the string of "0". The ID of all these tags in the interrogation space starts with a "0" bit. When an answer is received or a collision of the tag is observed, the reader will iterate on both sub-trees "0" rooted at "00" and "01" However, if there is no answer, the reader assumes that there is no "0"-tags preceded in their interrogation region and sends a question "1" afterward. For the reader, the difficulty of TWA is proportional to the number of tags in TWA. The researchers introduced in [51] the protocol for dealing with lost tags. Their protocol depends on lightweight cryptographic techniques and the key size is taken into account. In their protocol, RFID tags and key size are the two main factors that affect the entire group authentication process. From our perspective, their protocol is unique because they considered the effect of key size on authentication efficiency, assuming the presence of a large number of RFID tags. They also proved their protocol efficient, as it requires less time to authenticate the tag, provides resistance to a replay attack, and all the tags are independently verified. In another in research [50], the authors suggested a scheme. It was found to be effective in terms of performance indicators. These indicators can be internal, external, or QoS-based. Internal indicators that have been used to measure structural stability are DI, RMSSDI, RSI, SI, CHI, and DBI. External indicators that were used to measure the stability of structures are FI, NMII, PI, and EI. Two additional indicators were also used based on service quality (productivity and jitter). One of the advantages of their model is that it observed an improvement of 0.15% in minimum and 14.9% in maximum in the case of network instability without outliers compared to that of the network with outliers. It has further proven high efficiency.

B. A Critical Review of Wireless Sensor Networks Security

After addressing the security requirements of WSN, we are reviewing various scientific papers focusing on their security. It was noted that in terms of authentication, blockchain technology is considered one of the leading modern techniques. Some researchers [52] used the technology in several ways; some used it as a blockchain structure linked to the head node. It is followed by the blockchain linked to sub-nodes that formed a structure distinguished by its effectiveness in the authentication. However, it can take more time in the case of a large number of nodes and become immune to the attacks of concurrent guessing against IDs and passwords. Some [60] have applied this technique to other ways on the IoT, but its effectiveness cannot be confirmed when applied to WSN, except through experience. It was also noticeable that the AVISPA tool was used [54], which aims to analyze the Internet safety protocols on a large scale and increases the strength of the experiment results. The authors were also focused on making security protocols that are lightweight, affordable, and offer high security in return. However, lightweight protocols may not be able to detect harmful nodes in WSN. Concerning secure communication in WSN, one of the research papers [57] suggested the use of homomorphic encryption. However, this type of encryption is known to be vulnerable to compromise attacks. To solve this dilemma, you can attempt to split the data into pieces and send them to different aggregators. Another type of encryption was also mentioned in one of the papers [58] that merges Diffie-Hellman key exchange and Elliptic Curve cryptography. It

was an effective method in terms of time-saving, data security, and authentication. Another paper [59] proposed encryption based on data clutter that uses Hénon map to generate random numbers. However, it can break after several attempts, depending on the ability of the attacker. One work [51] mentioned updating the key periodically without the need for any sync, but the work did not mention time and efficiency factors. In the algorithms for the detection of attacks, Exponentially Weighted Moving Average (EWMA) [61] was used and the results were accurate, indicating the superiority of this method. Sequence attacks were detected in one work using algorithms [62] and in another work [64] using resistances placed on nodes. Both the studies gave positive results. We noticed a difference between RFID and WSN; in terms of security techniques, most of the references we discussed on RFID used a simple approach to achieve security, as the RFID tag has a short reading range from 5 meters (ideal conditions) to less than 1 meter (not ideal conditions). In contrast, a more sophisticated approach was used in most of the literature we discussed on WSNs. It is observed that authentication is different in these two technologies the reason behind that the different capabilities of them e.g., we can apply only lightweight approaches on RFID while we can apply the complex algorithms on WSN. This paper provides a comprehensive review of the recent approaches for securing RFID and WSNs.

IX. Conclusion

IoT technology has become an essential part of our era. It is defined as the set of devices connected for collecting and analyzing data from their environments. The types of technologies that use IoT are bifurcated. In this paper, we have highlighted the security and attacks of both WSNs and RFID since they are parts of the IoTs environments. The goal of providing a comprehensive study and investigate the recent research related to the security of WSN and RFID technologies in terms of security requirements, detection techniques, and prevention of attacks against them are accomplished. Thus the comprehensive discussion of these technologies of research observed in terms of efficiency, comparison of protocol security, cost, and weight is included.

In the future, we will keep up with the new approaches, further investigate, and compare the performance and security mechanisms of RFID and WSN.

References

[1] Bhabendu. Kumar. Mohanta,. Debasish. Jena,. Utkalika. Satapathy,. Srikanta. Patnaik,. Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11:100227, 2020.

[2] Daniel Minoli and Benedict Occhiogrosso. Blockchain mechanisms for iot security. Internet of Things, pages 1 – 13, 2018.

[3] Ahmet Arıs, Sema F Oktug, and Thiemo Voigt. Security of internet of things for a reliable internet of services. 2018.

[4] Yasmine Harbi, Zibouda Aliouat, Saad Harous, Abdelhak Bentaleb, and Allaoua Refoufi. A review of security in internet of things. Wireless Personal Communications, 108(1):325–344, 2019.

[5] You-Chiun Wang and Shu-Ju Liu.Minimum-cost deployment of adjustable readers to provide complete coverage of tags in rfid systems. Journal of Systems and Software, 134:228–241, 2017.

[6] Anas Mouattah and Khalid Hachemi. The feasibility of motion sensor-based smart rfid system in improving the power saving. 2020.

[7] Chris M Roberts. Radio frequency identification (rfid).Computers & security, 25(1):18–26, 2006.

[8] Mehdi Hosseinzadeh, Jan Lansky, Amir Masoud Rahmani, Cuong Trinh, Masoumeh Safkhani, Nasour Bagheri, and Bao Huynh. A new strong adversary model for rfid authentication protocols. IEEE Access, 8:125029–125045, 2020.

[9] Andreas Koschan, Suhong Li, John K Visich, Basheer M Khumawala, and Chen Zhang. Radio frequency identification technology: applications, technical challenges and strategies. Sensor Review, 2006.

[10] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems, 29(7):1645–1660, 2013.

[11] Mustafa Kocakulak and Ismail Butun. An overview of wireless sensor networks towards internet of things. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pages 1–6. IEEE, 2017.

[12] Surbhi Gupta. Prosperity, vulnerabilities and security threats in wsn. International Journal of Advanced Research in Computer Science, 3(5), 2012.

[13] Marcos Augusto M Vieira, Claudionor N Coelho, DC jr da Silva, and Jose´ Monteiro da Mata. Survey on wireless sensor network devices. In EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 03TH8696), volume 1, pages 537–544. IEEE, 2003.

[14] Michal Prauzek, Jaromir Konecny, Monika Borova, Karolina Janosova, Jakub Hlavica, and Petr Musilek. Energy harvesting sources, storage devices and system topologies for environmental wireless sensor networks: A review. Sensors, 18(8):2446, 2018.

[15] Niels Reijers and Koen Langendoen. Efficient code distribution in wireless sensor networks. In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pages 60–67, 2003.

[16] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. Computer communications, 30(14-15):2826–2841, 2007.

[17] Nayef Abdulwahab Mohammed Alduais, Jiwa Abdullah, and Ansar Jamil. Rdcm: An efficient real-time data collection model for iot/wsn edge with multivariate sensors. IEEE Access, 7:89063–89082, 2019.

[18] Xiaochen Lai, Quanli Liu, Xin Wei, Wei Wang, Guoqiao Zhou, and Guangyi Han. A survey of body sensor networks. Sensors, 13(5):5406–5447, 2013.

[19] Afsaneh Minaie, Ali Sanati-Mehrizy, Paymon Sanati-Mehrizy, and Reza Sanati-Mehrizy. Application of wireless sensor networks in health care system. age, 23(1), 2013.

[20] Gowthamaraj Rajendran, RS Ragul Nivash, Purushotham Parthiban Parthy, and S Balamurugan. Modern security threats in the internet of things (iot): Attacks and countermeasures. In 2019 International Carnahan Conference on Security Technology (ICCST), pages 1–6. IEEE, 2019.

[21] Sridipta Misra, Muthucumaru Maheswaran, and Salman Hashmi.Security challenges and approaches in internet of things. Springer, 2017.

[22] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou.

[23] A roadmap for security challenges in the internet of things. Digital Communications and Networks, pages 118–137, 2018.

[24] Carsten Maple. Security and privacy in the internet of things. Journal of Cyber Policy, 2(2):155–184, 2017.

[25] Israa Alqassem and Davor Svetinovic. A taxonomy of security and privacy requirements for the internet of things (iot). In 2014 IEEE International Conference on Industrial Engineering and Engineering Management, pages 1244–1248. IEEE, 2014.

[26] Isha Bhardwaj, Ajay Kumar, and Manu Bansal. A review on lightweight cryptography algorithms for data security and authentication in iots. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pages 504–509. IEEE, 2017.

[27] Minhaj Ahmad Khan and Khaled Salah.Iot security: Review, blockchain solutions, and open challenges. Future Generation Com- puter Systems, 82:395–411, 2018.

[28] Mohammad Reza Sohizadeh Abyaneh. Security analysis of lightweight schemes for rfid systems. 2012.

[29] Shruti Jaiswal and Daya Gupta. Security requirements for internet of things (iot). In Proceedings of International Conference on Communication and Networks, pages 419–427. Springer, 2017.

[30] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, and Saleem Ullah. Security issues in the internet of things (iot): a comprehensive study. International Journal of Advanced Computer Science and Applications, 8(6):383, 2017.

[31] D Richard Kuhn, Edward J Coyne, and Timothy R Weil. Adding attributes to role-based access control. Computer, 43(6):79–81, 2010.

[32] Anas Abou El Kalam, R El Baida, Philippe Balbiani, Salem Benferhat, Fre´de´ric Cuppens, Yves Deswarte, Alexandre Miege, Claire Saurel, and Gilles Trouessin. Organization based access control. In Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, pages 120–131. IEEE, 2003.

[33] Yuta Nakamura, Yuanyu Zhang, Masahiro Sasabe, and Shoji Kasahara. Exploiting smart contracts for capability-based access control in the internet of things. Sensors, 20(6):1793, 2020.

[34] Bo Lang, Ian Foster, Frank Siebenlist, Rachana Ananthakrishnan, and Tim Freeman. A flexible attribute based access control method for grid computing. Journal of Grid Computing, 7(2):169, 2009.

[35] Rajiv Mishra and Rajesh Yadav. Access control in iot networks: Analysis and open challenges. Available at SSRN 3563077, 2020.

[36] Pol Van Aubel, Erik Poll, and Joost Rijneveld. Non-repudiation and end-to-end security for electric-vehicle charging. In 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), pages 1–5. IEEE, 2019.

[37] Edewede Oriwoh, Haider al Khateeb, and Marc Conrad. Responsibility and non-repudiation in resource-constrained internet of things scenarios. International Conference on Computing and Technology Innovation (CTI 2015), 2016.

[38] Sandro Etalle, Jeremy den Hartog, and S. Marsh. Trust and punishment. In Proceedings of the 1st International Conference on Autonomic Computing and Communication Systems, Autonomics, number 302 in ACM International Conference Proceeding Series, pages 5:1–5:6, Belgium, December 2007. ICST. http://eprints.ewi.utwente.nl/12914.

[39] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pages 336–341. IEEE, 2015.

[40] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4):2347–2376, 2015.

[41] Shantanu Rao, Nagaraja Thanthry, and Ravi Pendse. Rfid security threats to consumers: Hype vs. reality. In 2007 41st Annual IEEE International Carnahan Conference on Security Technology, pages 59–63. IEEE, 2007.

[42] Aikaterini Mitrokotsa, Melanie R Rieback, and Andrew S Tanenbaum. Classifying rfid attacks and defenses. Information Systems Frontiers, 12(5):491–505, 2010.

[43] Sayamuddin Ahmed Jilani, Chandan Koner, and Shovon Nandi. Security in wireless sensor networks: Attacks and evasion. In 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), pages 1–5. IEEE, 2020.

[44] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, and Abdul Waheed Khan. A secure routing protocol with trust and energy awareness for wireless sensor network. Mobile Networks and Applications, 21(2):272–285, 2016.

[45] Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, and Peng Li. Skinny-based rfid lightweight authentication protocol. Sensors, 20(5):1366, 2020.

[46] Zhicai Shi, Xiaomei Zhang, and Jin Liu. The lightweight rfid grouping-proof protocols with identity authentication and forward security. Wireless Communications and Mobile Computing, 2020, 2020.

[47] Pramod Kumar Maurya and Satya Bagchi. Cyclic group based mutual authentication protocol for rfid system. Wireless Networks, 26(2):1005–1015, 2020.

[48] Quan Qian, Yan-Long Jia, and Rui Zhang. A lightweight rfid security protocol based on elliptic curve crytography. IJ Network Security, 18(2):354–361, 2016.

[49] Davide Zanetti, Leo Fellmann, Srdjan Capkun, et al. Privacy-preserving clone detection for rfid-enabled supply chains. In 2010 IEEE International Conference on RFID (IEEE RFID 2010), pages 37–44. IEEE, 2010.

[50] Bogdan Carbunar, Murali Krishna Ramanathan, Mehmet Koyut u¨rk, Suresh Jagannathan, and Ananth Grama. Efficient tag detection in rfid systems. Journal of Parallel and Distributed Computing, 69(2):180– 196, 2009.

[51] Adarsh Kumar and Alok Aggarwal. An efficient simulated annealing based constrained optimization approach for outlier detection mechanism in rfid-sensor integrated manet. Int. J. Comput. Inf. Syst. Ind. Manage. Appl., 11:55–64, 2019.

[52] Haowen Tan, Dongmin Choi, Pankoo Kim, Sungbum Pan, and Ilyong Chung. An efficient hash-based rfid grouping authentication protocol providing missing tags detection. Journal of Internet Technology, 19(2):481–488, 2018.

[53] Zhihua Cui, XUE Fei, Shiqiang Zhang, Xingjuan Cai, Yang Cao, Wensheng Zhang, and Jinjun Chen. A hybrid blockchain-based identity authentication scheme for multi-wsn. IEEE Transactions on Services Computing, 13(2):241–251, 2020.

[54] Shao-I Chu, Yu-Jung Huang, and Wei-Cheng Lin. Authentication protocol design and low-cost key encryption function implementation for wireless sensor networks. IEEE Systems Journal, 11(4):2718–2725, 2015.

[55] Joonyoung Lee, Sungjin Yu, Myeonghyun Kim, Youngho Park, and Ashok Kumar Das. On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks. IEEE Access, 8:107046–107062, 2020.

[56] Himani Sikarwar and Debasis Das. A lightweight and secure authentication protocol for wsn. In 2020 International Wireless Communications and Mobile Computing (IWCMC), pages 475–480. IEEE, 2020.

[57] Oguz Ata, Hasan H Balik, and Erdem Ucar. Protocol design for secure communication in wsn. TEM Journal, 6(2):192, 2017.

[58] Soufiene Ben Othman, Abdullah Ali Bahattab, Abdelbasset Trad, and Habib Youssef. Confidentiality and integrity for data aggregation in wsn using homomorphic encryption. Wireless Personal Communications, 80(2):867–889, 2015.

[59] Sunil Kumar, C Rama Krishna, and AK Solanki. A technique to resolve data integrity and confidentiality issues in a wireless sensor network. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pages 183–188. IEEE, 2018.

[60] Alya'a Abdulrazzak Msekh and Jamal Mohamed Kadhim. Security of wireless sensor nodes. Iraqi Journal of Science, 61(7):1773 – 1780, 2020.

[61] Alma E Guerrero-Sanchez, Edgar A Rivas-Araiza, Jose Luis Gonzalez-Cordoba, Manuel Toledano-Ayala, and Andras Takacs. Blockchain mechanism and symmetric encryption in a wireless sensor network. Sensors (Basel, Switzerland), 20(10), 2020.

[62] Opeyemi Osanaiye, Attahiru S Alfa, and Gerhard P Hancke. A statistical approach to detect jamming attacks in wireless sensor networks. Sensors, 18(6):1691, 2018.

[63] Bassam Hasan, Sameer Alani, and Mohammed Ayad Saad. Secured node detection technique based on artificial neural network for wireless sensor network. Int J Elec & Comp Eng ISSN, 2088(8708):8708.

[64] Sumit Pundir, Mohammad Wazid, Devesh Pratap Singh, Ashok Kumar Das, Joel JPC Rodrigues, and Youngho Park. Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: Survey and future challenges. IEEE Access, 8:3343–3363, 2019.

[65] Zixin Zhou, Lei Liu, and Guijie Han. Survival continuity on intrusion detection system of wireless sensor networks. In 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pages 775–779. IEEE, 2015.