UDK 351.861:342.738]:004.738.5
10.7251/ZRSNG2001027C

Internet of Things Security Aspects

Aleksandar Sandro Cvetković [1*], Stevo Jokić [1], Saša Adamović [1], Nenad Ristić [1], Nikola Pavlović [2]

[1] Faculty of Computing and Informatics, Sinergija University, Bijeljina, Bosnia and Herzegovina
*ascvetkovic@sinergija.edu.ba

[2] Faculty of Informatics and Computing, Singidunum University, Belgrade, Serbia

Abstract **-** The Internet of Things (IoT) connects almost all objects in the environment, whether they are physical or virtual using the Internet with the aim of creating new digital services that will improve lifestyle of the people. Currently, IoT devices cover a wide range of applications across the globe, such as smart cities, smart healthcare, smart transportation, smart homes, smart education, smart supply chains, smart agriculture, wearable devices, Industrial IoT (IIoT), smart energy where several have a direct impact on our daily life activities. With the advent of the Internet of Things, the size of the network has expanded beyond all boundaries, in which various IoT applications generate enormous amounts of data and require continuous Internet connection for communication between devices. Despite the countless benefits that IoT provides, there are some security challenges in this scenario. As data is communicated through wireless networks, challenges in the security domain can be such as data confidentiality, data authentication, data reliability, privacy.

Keywords – Internet of Things, WSN, IoT Security, Cybersecurity, IoT.

Introduction

IoT is a well-balanced platform where everyday device procedures turn into intellectual, everyday communication turns into helpful, and everyday processing turns into intelligent [1].

Internet of things is all about connecting varity of things, providing useful services and communication between connected devices. IoT aims to allow people and things to be connected anytime, anywhere via anything. There are currently about 30.73 billion connected devices through IoT while it is estimated that by 2025 there will be about 75.44 billion connected devices.

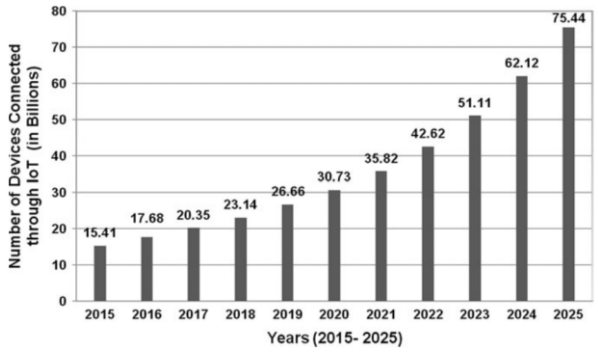

Figure 1. Projected number of devices using IoT technology (str. 456) [2]

That is almost 10 devices (things) per person in day to day activities. This is the next major step in delivering Internet's promise of making the world a connected place.

Because IoT devices provide useful services that will make it easier for people to live their daily lives, a large amount of data will circulate through the network, of which certain data will be of great importance. The large number of connected devices and the enormous increase in the number of computer networks create opportunities for attackers to easily find and exploit vulnerabilities. With such devices, vulnerabilities are not only related to software but also to hardware, as IoT devices are usually limited in terms of memory, computation, power, and energy, making them vulnerable to a large number of attacks. In addition, since it is data of great importance to the user and data that could be certainly abused, the number of attacks will increase significantly. Therefore, data of great importance must remain private and protected, which will present various security challenges and a difficult task.

I. INTERNET OF THINGS

IoT Architecture

What makes the Internet of Things so popular is the ability to connect millions of heterogeneous devices over the Internet, creating the need for a flexible layered architecture. Because there is no unique consensus for the standard IoT architecture and since each IoT application has different requirements, there are currently 3, 4, 5 or even 7 layer architectures based on those requirements.

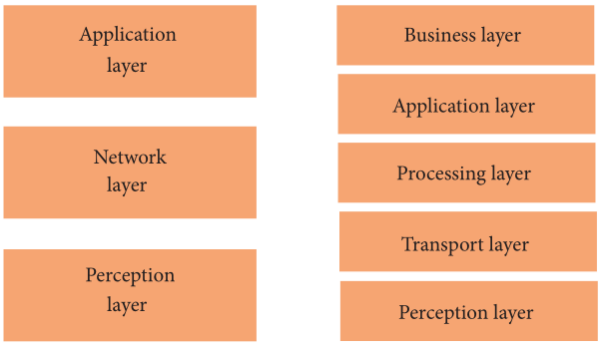

Figure 2. Architecture of IoT (left: three layers, right: five layers) [3]

A basic three layered architecture consist of perception, network and application layer. The three layer architecture defines the main idea of the Internet of Things, however, it is

not enough to solve IoT problems. The five layer architecture, which includes two additional layers in addition to the basic three, the processing and business layer provides options for solving cloud computing issues, big data processing and middleware. It also helps to address the issue of heterogeneity and interoperability. In five layer architecture, the layer of perception and application play the same role as in the three layer architecture.

All these architectures perform almost the same set of tasks: connecting all the devices wired or wirelessly, gathering and processing data and using the processed data to do the automated tasks.

IoT Technology and Protocols

The Internet of Things connects devices, collects and processes data and provides useful services to people based on the data processed. In order for the IoT to be able to fulfill all these requirements, real-time data transfer is required. The data generated by the sensors is transferred to a data center or cloud where they are further integrated with other data as required. This functionality can be represented in a multi-layered architecture whereby each layer manages a set of protocols.

Session		**MQTT, SMQTT, CoRE, DDS, AMQP, XMPP, CoAP, ...**	**Security**	**Management**
Network	**Encapsulation**	**6LowPAN, 6TiSCH, 6Lo,** Therad, ...	TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, ...	**IEEE 1905, IEEE 1451, ...**
	Routing	**RPL, CORPL, CARP, ...**		
Datalink		WiFi, **Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE,** 3G LTE, NFC, **Weighless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7,** ANT+, **LTE-A, LoRaWAN, ...**		

Figure 3. IoT protocols [4]

Data link protocols define a strategy for communication between nodes, standards for synchronization, and bidirectional packet exchange. Network protocols perform routing and are responsible for the reliable transfer of data packets from source to destination. Session protocols are used to define secure messaging standards. Management protocols aim to allow interconnection between heterogeneous data links and sensors or smart inverters for the system to interpret the data correctly. Security protocols have the most difficult task of ensuring confidentiality, authentication, privacy, access mechanisms, synchronization of data and participating devices.

IoT Applications

Internet of Things technology has found appliance in almost everything. This technology is used in homes, offices, industries, healthcare, agriculture, etc. IoT technology is accepted for both commercial and personal purposes. On the one hand, IoT has helped make life easier for all people by automating things and providing useful information, and on the other hand, many industries are using IoT to automate their tasks in their organization [5]. There are various Internet of Things applications such as smart cities, smart education, smart healthcare, smart transportation, smart homes, smart supply chains, smart agriculture, wearable devices, industrial IoT (IIoT) and smart energy.

II. INTERNET OF THINGS SECURITY

IoT Security Challenges

Notwithstanding the various benefits that IoT provides, there are concerns about accepting IoT devices because of certain challenges. These challenges must be addressed in order to increase the acceptance rate of IoT devices. Security challenges are the most difficult problem and the reason why IoT devices are hard to accept. The most common security challenge is the hacking of IoT devices, compromising user confidential information. However, not only sensitive information is compromised but also the life and health of users.

In addition to security challenges, there are others, such as connectivity challenges or the choice of network structure, whether a centralized, decentralized or distributed network will be used for IoT. A centralized network structure has the least chance of being used. There are also challenges related to system requirements, hardware longevity, and compatibility of different IoT devices in terms of technology and hardware and software. Wireless communication is mostly used as a method of communication for IoT. The most commonly used technology is the Wireless Sensor Network (WSN). However, wireless networks are vulnerable and can easily be compromised. There is a barrier to implementing secure and complex security protocols due to hardware performance limitations. In addition, there are various challenges due to the large amount of data generated by IoT devices, especially in terms of security and privacy. How to separate useful and important information from irrelevant information is a challenge.

IoT Security Threats

Generally, IoT security attacks can be divided into two groups, the first being data disclosure and the second being denial of service. Data disclosure attacks violate user privacy, while denial of service attacks block the operation of IoT devices or their services. Data disclosure attacks can lead to a denial of service or network breach, which again affects the availability of services to the user. Because IoT devices use wireless networks where eavesdropping is easier, it is important to find the right network solution. Data disclosure attacks can be network sniffing, device cloning, side channel attacks and cryptographic attacks. DoS attacks can be device jamming, device cloning, battery exhaustion and routing attacks [6].

Perception Layer Attacks

- Jamming Attack - In a jamming attack, the attacker interferes with the radio communication used in the network. Such an attack can interfere with the entire network and the attacker can perform this attack with low jamming resources [7].
- Deactivation - A “kill” instruction by unauthorized application or physical destruction of the node.

- Tampering - An unauthorized attack can be the physical damage, stopping or alteration of node services. This kind of attack causes node capture and node replication attack. An attacker can gain complete control of the captured node and compromise the entire WSN. The captured node can be replaced or cloned. This way the attacker can gain access to the IoT devices and then use them to capture the network and launch various insider attacks, icluding DoS and DDoS.
- Collision - There is a major possibility of collision in IoT, because of the simultaneous occurrence of various set of rules in the WiFi 2.4 GHz band. Also, message collisions can occur if the clock of one node is not synchronized with other neighboring nodes in the network.
- Exhaustion – The DoS and tunneling attacks in the network lead to IoT Devices energy exhaustion [8].

Network Layer Attacks

- Spoofing - In this type of attack, the attacker sends a false broadcast message to a sensor network that does not have a protocol to identify the originality of the message from the source. This way the attacker gains access to confidential information and uses the situation to make even more security breaches. This type of attack is divided into two categories, IP spoofing and RFID spoofing. Both types of attacks target and spoof the IoT control system in order to transmit malicious scripts across the network.
- Sybil - in this attack, the attacker uses a single sensor node that uses multiple identifications against the other sensor nodes in the sensor network. The attacker creates a scenario where one node duplicates its node and acts as if it were in multiple different locations.
- Hello Flood - WSN uses HELLO packets or messages to let the packet receiving node know that the packet sending node is within its broadcast range. In this attack, the attacker uses a high power transmitter to generate packets with HELLO messages that he sends to all nodes within the IoT network. Due to the strong transmitter in this scenario, it seems as if messages were sent from the neighborhood. In this way, the sensors are convinced that the attacker is their neighbor and the information is routed incorrectly. Then the attacker can set the infected node to be the parent node which results in data loss, high network traffic and false routes.
- Sinkhole - An attacker attacks a node that uses to advertise false routing information to redirect all network data to that node. This is how neighboring nodes select that node to route their data to that network. This will reduce the network traffic flow and fool the senders that their sent packet of data was received by the recipient. In this scenario, the attacker gets all the data instead of the recipient. Sinkhole attack can further lead to DoS attack and selective forwarding attack.
- Selective forwarding - An attacker can interfere with communication by compromising one node by selectively sending a small amount of messages and delivering them using longer routing routes or simply dropping them. In case they are dropped, neighboring nodes assume that communication has failed and they are looking for new routes.
- Wormhole - In this attack, the attacker tries to find a good strategic place in the network so that it has the shortest route within the nodes. After the attacker finds the right location, he starts listening and recording the network. The attacker then creates a direct link between adjacent nodes and forms a tunnel between them to transfer traffic.
- Eavesdropping - this attack directly affects privacy. The attacker uses special monitoring software to eavesdrop or sniff on packages to gain access to private network communications.
- Denial of Service (DoS) - this is one of the commonly performed network attacks aimed at making the computer infrastructure in the network inaccessible to its client users. In this attack, a large amount of network data traffic is redirected to the victim node, which cannot process everything at the same time, causing the server or controller node to be unavailable or shut down. Attackers constantly send false requests to network systems so that the network is not available to communicate with users in that network.
- Man in the Middle (MITM) - The attacker is placed between two victim nodes, intercepts communication and gains access to information without their knowledge [9].

Application Layer Attacks

- Phishing attack – Attackers use this method to obtain credentials for authentication and authorization, including passwords, by sending countless spam emails and creating fake websites and forums.
- Distributed Denial of Service (DDoS) – A DDoS attack is like a DoS attack except that a DoS attack uses one source for attack, while a DDoS attack uses multiple sources for a simultaneous attack. An attacker can communicate with various computers around the world and direct them to attack the same server at the same time. In this way, the server will be overwhelmed. All server resources will be used such as cpu and memory, and also the network bandwidth will be flooded, after which users will no longer be able to use the services of that server.
- Loggers attack – The attacker uses loggers to collect confidential information from the network. This information can be important files, emails or passwords. An attack method that uses loggers and sniffers is common and hackers use it to hack confidential emails and passwords.

- Malicious code / Injections – In this attack, the attacker accesses and manipulates the application code through the server. Such an attack causes data to be lost and confidential information leaked from the security network.
- Session Hijacking - The attacker exploits gaps in the authentication protocols to retrieve the user session. In this scenario, the attacker gains access to the user's personal identities and uses the network like a real user. The server is then tricked and treats the attacker's connection as a valid original user's session [10].

III. IoT Security Solutions

In the state-of-the-art, security goals are divided into three categories: confidentiality, integrity and availability. These three categories are known as the CIA triad. Confidentiality refers mostly to the fact that only authorized entities can gain access to information. Since sensitive data is often transmitted, it is important to ensure confidentiality of IoT objects. To ensure that IoT objects have received only legitimate commands and data to provide reliable services IoT requires integrity. IoT availability ensures that IoT services are accessible only by authorized users or objects.

The authors [11] state that the CIA triad fails in addressing novel threats and that IoT security requirements are more demanding. To fill this gap in the CIA security model, the authors cite a new comprehensive set of security goals known as an IAS relating to Information Assurance & Security. The security goals of the IAS reference model are:

- Confidentility - only authorized objects or users can get access to the data.
- Integrity - The process in which data completeness and accuracy is preserved.
- Non-Repudiation - IoT system can validate the incident or non-incident of an event.
- Availability - An ability of an IoT system to make sure its services are accessible, when demanded by authorized objects or users.
- Privacy - IoT system follows privacy rules or policies and allowing users to control their sensitive data.
- Auditability - Ensuring the ability of an IoT system to perform firm monitoring on its actions.
- Accountability - IoT system holds users taking charge of their actions.
- Trustworthiness - Ensuring the ability of an IoT system to prove identity and confirm trust in third party.

The IoT device security starts with the devices themselves and the manufacturers. Due to the rapid development of technology, the short time of new devices on the market, providing affordable prices for new devices, the security of IoT devices is often neglected or set aside by IoT manufacturers. Some of these devices come with security software solutions however such devices leave the hardware unintentionally vulnerable. An insecure hardware platform will inevitably lead to software insecurity.

In the following, the focus will be mostly on the basic three-layer IoT architecture.

In [12], the authors state that the perception layer can be classified as the layer with the greatest security risks due to the physical exposure of IoT devices, which can also be located in an open environment. The authors state that in addition, such a device has very large hardware limitations and technological heterogeneity that limits the implementation of effective security measures.

On the other side, the transport layer in relation to the perception layer can be classified as a lower risk layer due to the known drawbacks of standard wireless data transmission technology as well as the known threats in access networks. The advantage of this layer is intensive vulnerability research and continuous development of new protection methods.

For the application layer, the authors state that there is a variable level of risk that depends on the specific implementation of the application. This layer can be accessed by a large number of users and other IoT applications. Protection in this layer is very important as data losses and breaches of services such as confidentiality, integrity and availability can cause enormous damage. Compared to the perception layer, this layer has more mature technology, less threats and already tested security methods.

Hardware constraints on IoT devices are an important problem because traditional IT devices that are rich in resources can use a variety of cryptographic algorithms while due to limited resources IoT devices can only use lightweight algorithms.

Table 1. Cyber-security attacks towards WSNs and IoT along with the proposed solutions to defend against those attacks

Attacks	**Layers involved**	**Proposed solutions for prevention/mitigation**
Jamming	Perception/Physical	Spread spectrum, priority messages, lower duty cycle, swarm intelligence, JAM (region mapping), JAM (re-routing)
Deactivation	Perception/Physical, Data Link	Users or objects authentication, secure physical design, tamper proofing and self-destruction, hiding
Tampering	Perception/Physical	Tamper proofing, hiding or camouflaging
Collision and Exhaustion	Data Link/MAC	Error correction codes, TDM
Spoofing	Data Link, Network, Application	Authentication mechanism (variants of ECC), RFID authentication and encryption techniques
Sybil	Network, Application	Identity verification, isolation
Hello Flood	Network	Identity verification, multi-path multi-base station routing
Sinkhole	Network, Data Link	Secure routing algorithm

Selective Forwarding (Grayhole)	Network	Multi-path routing, usage of source authorization
Wormhole	Network, Data Link	Dawwsen proactive routing protocol
Eavesdropping (Sniffing)	All layers	Link-layer encryption, key pre-distribution
Denial of Service - DoS	Perception/Physical, Data Link, Network, Transport	Priority messages, hiding, monitoring, authorization, redundancy, encryption, keeping a list of suspicious devices
Man in the Middle	Network	Encryption of the RFID communication channel, authentication techniques
Phishing	Application	Cryptographic methods
Malicious code / Injections	Physical/Application	Tamper proofing and self-destruction, IDS
Session Hijacking	Transport	Light-weight user authentication algorithm for optimized routing in mobile networks

Defense against Jamming

In [13], the authors propose a “Swarm Intelligence” cross-layer security mechanism for detecting jamming attacks. The authors also provide countermeasures to mitigate this type of attack.

The authors [14] suggest a jammed area mapping service JAM . It serves to detect jamming attacks against WSNs. In addition, JAM avoids the jammed part of the WSN by redirecting packets thus mitigating the Jamming DoS attack.

Defense against Deactivation

Killing tag attack on RFID system can stop tags communication with their reader. It is absolutely essential to make sure that RFID tags are not killed by an illegal party. Kill command should be secured by a strong password [15]. Physical destruction of node can be protected by secure physical design, tamper proofing [16] and hiding or camouflaging.

Defense against Tampering

To protect the WSN from node tampering attacks, nodes must be equipped with tamper-resistant hardware in which any type of unauthorized interference attempt would wipe out memory as well as data storage so that confidential information such as secret keys would not leak. The basic way to protect against such attacks is to simply hide or camouflage the nodes.

Defense against Collision and Exhaustion

In order for WSNs to defend against collision and exhaustion attacks, the request rate of each node must be limited. In this way, the network could reject all additional requests from the same node (attacker). Another solution would be to use a time division multiplexing TDM technique that provides each node with certain time intervals for packet transmission. In this case, the nodes would have a short period to access the channel thus preventing an attack related to channel abuse. In order for WSNs to defend against collision and exhaustion attacks, the request rate of each node must be limited. In this way, the network could reject all additional requests from the same node (attacker). Another solution would be to use a time division multiplexing TDM technique that provides each node with certain time intervals for packet transmission. In this case, the nodes would have a short period to access the channel thus preventing an attack related to channel abuse. If the corruption of the packets occurs partially, the use of error detection and correction codes would be useful to combat this type of attack [17].

Defense against Spoofing

The authors of [18] present an authentication mechanism that uses variants of elliptic curve cryptography to protect against spoofing attacks on the IoT home network without exhausting the devices (computational power and storage area). The authors also state that they used asymmetric key cryptography in this solution, however they state that in terms of computation a better solution would be one that uses symmetric key cryptography.

Defense against Sybil

In [19] the authors presented two protocols for protection against sybil attacks. The first protocol uses "radio resource testing" in which each sensor node assigns a unique channel to each of its neighbors. Radio circuitry of a sensor node generally cannot handle simultaneous send and receive operations on more than one channel, which means that a failure to communicate through a single channel can be an indicator of a sybil attack.

The second protocol uses "ID-based symmetric keys". Each sensor node has a key associated with its ID and each node has these keys preloaded. If a suspicious node appears, its ID is examined by witness nodes based on the shared keys between the suspicious node and the witness sensor node.

The authors [20] propose a “rule-based anomaly detection system (RADS)” that monitors and on time detects a sybil attack on a sensor network. The method relies on the "ultra-wideband ranging-based detection algorithm". RADS works so that each node has the ability to trigger alarms if a suspicious node appears nearby. This method, in addition to being able to detect a sybil attack, can also prevent it by isolating the attacker sensor node and compromised nodes. For defense against sybil attacks, the most important thing is that the identities of each node be verified.

Defense against Hello Flood

To defend against HELLO Flooding attacks, the authors [21] suggest forcing each node to verify the identity of each of its neighboring nodes with an identity verification protocol using a trusted base station. If the protocol sends messages in both directions over the link between the nodes, a HELLO flood attack is prevented when the attacker has only a strong transmitter because the protocol checks the directionality of the link.

Defense against Sinkhole

In [22] the authors proposed a secure routing algorithm SeRA to protect against sinkhole attacks for mobile WSNs. The proposed algorithm is based on the Tiny-AODV protocol. First, several mobile agents communicate with each sensor node to collect network data all with the goal of building a global data matrix of the sensor nodes. After that, by using the SeRA routing algorithm, the sinkhole attack can be effectively avoided.

Defense against Selective forwarding (Grayhole)

There are two approaches to defend against selective forwarding attacks, detecting nodes that selectively forwarding and developing resilient routing schemes that can deliver packets even when there is a selective forwarding attack.

Multi-path routing can be an effective way to mitigate selective forwarding attacks and blackhole attacks. However there is a scenario where an attack can be as effective as in single-path routing.

Defense against Wormhole

Authors in [23] propose "DAWWSEN", a proactive routing protocol based on the construction of a hierarchical tree where the base station is in the root node while the sensor nodes are the inner or leaf nodes of the tree. DAWWSEN fights against wormhole attacks by creating a hierarchical three-way handshake routing tree and any attempt to create wormholes is rejected by this generated routing tree.

Defense against Eavesdropping (Sniffing)

Since communication in WSNs takes place by air, we have no information whether the packages came only to the people for whom they were intended or not. Therefore, the detection of eavesdropping is almost impossible. The solution to this problem is encryption. Link layer encryption would prevent outsider attacks such as eavesdropping. Also random key pre-distribution schemes [24] help link layer encryption schemes by distributing keys required for encryption algorithms, thus helping WSNs to protect information in transmission and prevent eavesdropping, data and information spoofing. An eavesdropping attack, also known as a sniffing or snooping attack.

Defense against Denial of Service (DoS)

Attacks like jamming, tampering, collision, exhaustion, blackholes, flooding fall under the types of DoS attacks. In addition to the above methods for protection against these attacks, the following methods are most often used to defend against DoS attacks: priority messages, hiding, monitoring, authorization, redundancy, encryption and keeping a list of suspicious devices.

Defense against Man in the Middle (MITM)

In addition to the close proximity that makes this attack very difficult, the encryption technique if properly implemented can completely block this type of attack. [25]

Defense against Phishing

A simple algorithm that detects phishing email traffic and thus protects household devices can be used to protect against phishing attacks. Sometimes legitimate email addresses can be marked as spam which is why there is a need to filter phishing emails based on which the user will be warned not to open filtered emails [26]. Most of the approaches use encryption.

Defense against Malicious code / Injections

Intrusion Detection System IDS usually serves as a second line of defense to monitor network operations, communication links and to warn in case of any anomaly. Traditional IDS approaches are usually tailored for WSNs. SVELETE is one of the first IDSs designed to meet the requirements of the IPv6-connected IoT nodes. It is capable of detecting routing attacks, such as spoofed or altered information, and blackhole attack. An attacker can also physically insert malicious code into an IoT object, this approach is solved by tamper proofing and self-destruction.

Defense against Session Hijacking

The authors in [27] present a lightweight user authentication algorithm for optimized routing in mobile networks and defending against session hijacking attacks.

They proposed a new Routing Optimization mechanism, the RO protocol. It requires only a light computational load and is compatible with the legacy protocol. The protocol provides Binding Update BU and Return Routability RR. The authors state that the protocol proved to be excellent in terms of low computational cost and minimal delay.

CONCLUSION

IoT has a complex architecture consisting of a variety of heterogeneous devices. Due to this architecture, IoT represents a great challenge in the field of security because it is necessary to solve the problem of scalability, transparency and reliability. IoT security is not only related to software but also to hardware, which means that the number of possible attacks is much higher. In this paper, we focus mostly on WSN and IoT security threats, as well as certain countermeasures to prevent and mitigate IoT attacks. Although some solutions have already been proposed, there is no single solution to defend WSNs and IoT against cyber attacks. Therefore, countermeasures represent potential solutions for the safety of certain characteristics of WSNs, especially IoT. Since it all depends on the needs of IoT devices, future research should focus on optimizing the resources that IoT devices will use as well as designing lightweight security protocols and cryptographic algorithms that are tailored to the specific needs of IoT devices.

References

[1] B. Chander and G. Kumaravelan, "Internet of Things: Foundation," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, Cham, 2019, pp. 3-33, doi: https://doi.org/10.1007/978-3-030-33596-0_1.

[2] M. Abdul Ahad, G. Tripathi, S. Zafar and F. Doja, "IoT Data Management—Security Aspects of Information Linkage in IoT Systems," in *Principles of Internet of Things (IoT) Ecosystem:*

Insight Paradigm, Springer, Cham, 2019, pp. 439-464, doi: https://doi.org/10.1007/978-3-030-33596-0_18.

[3] S. Pallavi and R. S. Smruti, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering,* vol. 2017, 2017, doi: https://doi.org/10.1155/2017/9324035.

[4] T. Salman and R. Jain, "NETWORKING PROTOCOLS AND STANDARDS FOR INTERNET OF THINGS," in *Internet of Things and Data Analytics Handbook*, John Wiley & Sons, Inc., 2017, pp. 215-238, doi: https://doi.org/10.1002/9781119173601.ch13.

[5] R. Sapra and P. Dhaliwal, "Blockchain for Security Issues of Internet of Things (IoT)," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, Cham, 2019, pp. 599-626, doi: http://doi-org-443.webvpn.fjmu.edu.cn/10.1007/978-3-030-33596-0_24.

[6] S. S. Dhanda, B. Singh and J. Poonam, "IoT Security: A Comprehensive View," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, Cham, 2020, pp. 467-494, doi: https://doi.org/10.1007/978-3-030-33596-0_19.

[7] B. Chander and G. Kumaravelan, "Security Vulnerabilities and Issues of Traditional Wireless Sensors Networks in IoT," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, Cham, 2019, pp. 519-549, doi: https://doi.org/10.1007/978-3-030-33596-0_21.

[8] V. Manjula and R. Thalapathi Rajasekaran, "Security Vulnerabilities in Traditional Wireless Sensor Networks by an Intern in IoT, Blockchain Technology for Data Sharing in IoT," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, 2019, pp. 579-597, doi: https://doi.org/10.1007/978-3-030-33596-0_23.

[9] J. L. Shah and H. F. Bhat, "Towards Integration of Cloud Computing with Internet of Things," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, Cham, 2019, pp. 229-260, doi: https://doi.org/10.1007/978-3-030-33596-0_9.

[10] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi and G. B. Wills, "Security, Cybercrime and Digital Forensics for IoT," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, Cham, 2019, pp. 551-577, doi: https://doi.org/10.1007/978-3-030-33596-0_22.

[11] H. A. Abdul-Ghani, D. Konstantas and M. Mahyoub, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model," *International Journal of Advanced Computer Science and Applications(ijacsa),* vol. 9, no. 3, 2018, doi: http://dx.doi.org/10.14569/IJACSA.2018.090349.

[12] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet of Things Journal,* vol. 5, no. 4, pp. 2483-2495, 2018, doi: https://doi.org/10.1109/JIOT.2017.2767291.

[13] R. Muraleedharan and L. A. Osadciw, "Cross Layer Denial of Service Attacks in Wireless Sensor Network Using Swarm Intelligence," in *40th Annual Conference on Information Sciences and Systems*, Princeton, 2006, doi: https://doi.org/10.1109/CISS.2006.286400.

[14] A. Wood, J. Stankovic and S. Son, "JAM: a jammed-area mapping service for sensor networks," in *IEEE Real-Time Systems Symposium*, Cancun, Mexico, 2003, pp. 286-297, doi: https://doi.org/10.1109/REAL.2003.1253275.

[15] G. Kulkarni, R. Shelke, R. Sutar and S. Mohite, "RFID security issues & challenges," in *International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, 2014, pp. 1-4, doi: https://doi.org/10.1109/ECS.2014.6892730.

[16] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing,* vol. 5, no. 4, pp. 586-602, 2017, doi: https://doi.org/10.1109/TETC.2016.2606384.

[17] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 1, pp. 616-644, 2020, doi: https://doi.org/10.1109/COMST.2019.2953364.

[18] K. C. Archana and N. Harini, "Mitigation of Spoofing Attacks on IOT HomeNetworks," *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 9, no. 1S, 2019, doi: https://doi.org/10.35940/ijeat.A1047.1091S19.

[19] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in *Third International Symposium on Information Processing in Sensor Networks*, CA, USA, 2004, pp. 259-268, doi: 10.1109/IPSN.2004.239019.

[20] P. Sarigiannidis, E. Karapistoli and A. A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Systems with Applications,* vol. 42, no. 21, pp. 7560-7572, 2015, doi: https://doi.org/10.1016/j.eswa.2015.05.057.

[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, AK, USA, 2003, pp.113-127, doi: https://doi.org/10.1109/SNPA.2003.1203362.

[22] L. Teng and Y. Zhang, "SeRA: A Secure Routing Algorithm Against Sinkhole Attacks for Mobile Wireless Sensor Networks," in *2010*, Sanya, Hainan, Second International Conference on Computer Modeling and Simulation, pp. 79-82, doi: https://doi.org/10.1109/ICCMS.2010.95.

[23] R. E. Kaissi, A. Kayssi, A. Chehab and Z. Dawy, "DAWWSEN: A DEFENSE MECHANISM AGAINST WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS," in *The Second International Conference on Innovations in Information Technology*, Dubai, UAE, 2005, doi: https://doi.org/10.13140/2.1.1441.6001.

[24] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in *Symposium on Security and Privacy*, CA, USA, 2003, pp. 197-213, doi: https://doi.org/10.1109/SECPRI.2003.1199337.

[25] A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers,* pp. 491-505, 2010, doi: https://doi.org/10.1007/s10796-009-9210-z.

[26] B. B. Gupta, N. A. G. Arachchilage and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems,* pp. 247-267, 2018, doi: https://doi.org/10.1007/s11235-017-0334-z.

[27] S. Song, H.-K. Choi and J.-Y. Kim, "A Secure and Lightweight Approach for Routing Optimization in Mobile IPv6," *EURASIP Journal on Wireless Communications and Networking,* 2009, doi: https://doi.org/10.1155/2009/957690.