Security in the IoT: State-of-the-Art, Issues, Solutions, and Challenges

Ahmed SRHIR[1], Tomader MAZRI[2], Mohammed, BENBRAHIM[3]
Department of Electrical Engineering-Networks and Telecommunication Systems-National School of Applied Sciences,
Ibn Tofail University, Kenitra, Morocco

***Abstract*—Now-a-days, the Internet of Things (IoT) has enormous potential and growth impact due to the technological revolution and the spread and appearance of events. It has received considerable attention from researchers and is considered the future of the Internet; however, according to Cisco Inc. reports, the IoT will be crucial in transforming our standards of living, as well as our corporate and commercial models. By 2023, the number of devices connected to IP networks will reach more than three times the population of the entire world. In addition, there will be 5.3 billion Internet users worldwide, representing 66% of the world's population, up from 3.9 billion in 2018. IoT enables billions of devices and services to connect to each other and exchange information; however, most of these IoT devices can be easily compromised and are subject to various security attacks. In this article, we present and discuss the main IoT security issues, categorizing them according to the IoT layer architecture and the protocols used for networking. In the following, we describe the security requirements as well as the current attacks and methods with adequate solutions and architecture for avoiding these issues and security breaches.**

Keywords—Internet of things (IoT); IoT security; IoT protocols; security issues in IoT; network security; data security

I. Introduction

Due to the continuous fast development of smart environments and broadband networks, the Internet of Things is now widely accepted and popular, earning its designation as the main standard for low-loss networks (LLN) with limited resources. It refers to a network where "objects" or devices that are integrated with sensors are interlinked through a network that may either be private or public [1, 2]. The sharing of information between the different devices is done through the network using standard communication protocols. The intelligent connected devices, or "objects," range from basic accessories to larger devices that each includes chips and detection sensors. For example, smart shoes contain chips that track and analyze fitness data [3]. Likewise, electric devices that may be operated remotely through the IoT, as well as any security cameras that are installed for surveillance of a place can be controlled remotely from anywhere. In addition to personal use, IoT also meets community needs. Several intelligent devices perform various functions such as surgical operation monitoring in hospitals, detection of weather conditions, automobile tracking, and connectivity. Due to its use in daily life, the IoT's potential size is obvious. It keeps expanding quickly as a result of the development of hardware techniques like bandwidth augmentation using networks based on cognitive radio to solve the underutilization of frequency spectrum resources [4,5]. Limited resources are one of the major challenges to IoT security, given that small devices or objects with sensors have limited computing and processing power and memory, making it easy for attackers to exploit these devices. On the other hand, the main challenge is ensuring consistency and adaptation between solutions with these limited architectures. For this reason, the global deployment architecture should be secured and reinforced against attacks that could impact the services offered by the IoT. In the last few years, considerable work has been done to solve security in the IoT ecosystem paradigm. While some methodologies focus on addressing security concerns at a particular layer, others strive to offer comprehensive end-to-end security for the entire Internet of Things (IoT) layer.

Security issues are categorized according to application, architecture, communication, and data in research by Alaba et al. [6]. The traditional layered design differs from the suggested topology for IoT security. After that, hardware, network, and application component threats are analyzed. Another study by Granjal et al. [7] examines and addresses security risks with IoT protocol definitions. The security studies detailed in [8–9] analyze and contrast various cryptographic algorithms and key management systems. Similar goals are shared by the authors of [10–11], who want to compare and evaluate intrusion detection technologies. IoT privacy, security, access control, and confidentiality contributions, as well as cross-software security, are examined in a review by Sicari et al. [12]. Additionally, Oleshchuk [13] presents an overview of IoT privacy preservation strategies. The author outlines secure multi-party computations that can be used to maintain user privacy, and attribute-based access control mechanisms are outlined as an efficient solution to ensure privacy in the Internet of Things. Numerous security risks for cloud-based IoT are covered by Zhou et al. [14], along with potential preventative measures. They discuss IoT employing clouds for key management, node compromise, layer removal or addition, identity and location privacy, and node compromise. In their article [15], Zhang et al. highlight the fundamental issues with IoT security including the requirement for lightweight cryptographic processes, privacy, unique object identification, authentication and authorization, malware, and software susceptibility.

Our primary contributions and methods are enumerated below in comparison to survey studies that have been published in the literature:

- A parametric examination of security risks and how well they fit with potential IoT solutions.

- IoT security challenges classification and categorization in relation to the various tiers, as well as the solutions employed.
- Future views providing workable answers to security issues with the Internet of Things.

The remaining sections of the paper are structured as follows: The IoT architecture is explained in Section II, as well as the security challenges encountered at every level of the IoT protocol stack. In Section III, the major security challenges and issues are categorized, while Section IV examines and provides a map of potential solutions, and finally, Section V concludes the paper.

II. IoT Architecture and Security Requirements

The integration of the Internet of Things is a fundamental element in the development of an intelligent ecosystem, connecting physical objects to the internet. It lets sensors, controllers, machines, people, and objects work together in a new way so that they can be intelligently identified, located, tracked, and monitored. While the Internet of Things is still in its development, many applications and standards must be adopted, including home automation, traffic control, smart cars, smart grids, etc. [16]. Fig. 1 illustrates how an IoT deployment typically consists of a number of heterogeneous devices with embedded sensors connected to one another through a network. These devices are all individually recognizable and typically have low power consumption, little memory, and limited computational power. In order to remotely transmit data and services to IoT consumers, gateways are used to link IoT devices to the public domain.

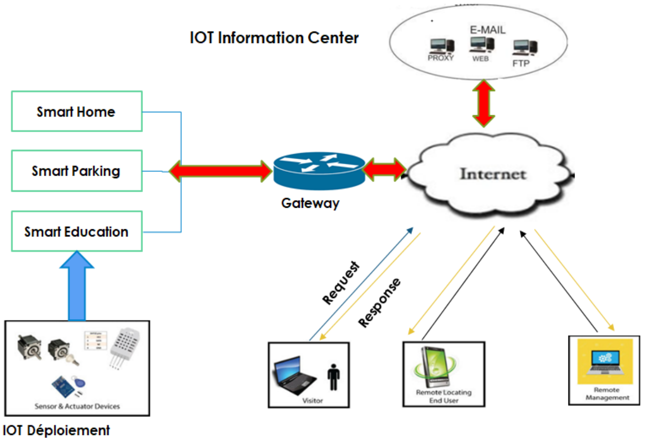

Fig. 1. Overview of IoT components.

A. IoT Architecture

Protocols are a group of instructions that allow data to be sent and received between electronic devices while respecting the agreements made in advance regarding the structure of the data. Accordingly, IoT protocols are standards that allow data to be exchanged and transmitted across the internet and between devices. Different IoT architectures are proposed by different authors, such as middleware-based architectures, Service-oriented architecture (SOA), architectures with six layers and three layers [17], In our case, and to address the fundamental communication issue, we will focus on the fundamental three-layer IoT architecture depicted in Fig. 2, which provides a general list of the most widely used protocols and standards for powering IoT devices, applications, and systems. As stated below, these three levels consist of a "perception layer," a "network layer," and an "application layer":

- The perception layer consists of physical and communication devices composed of captors and controllers that collect, desensitize, and treat information before transmitting it to the network layer. It includes the physical devices like cameras, Radio Frequency Identification (RFID),
- The network and transport layer represents a communication tier that uses gateways, switches, and routers to transmit and route data aggregated at the perception layer and delivered to the application layer.
- The application layer is a communication layer that contains the application in charge of the interaction with the users.

Every IoT layer employs a distinct set of protocols and standards, as shown in Fig. 2, protocols used by physical devices and communication technology include Zigbee Wi-Fi, 4G/5G, NB-IoT, and LoRaWAN. Different protocols are used by the network and the transport, including IPv6, 6LowPAN, RPL, TCP/UDP TLS, and DTLS. The message and application protocols include XML, HTTP, MQTT, and CoAP. Additionally, many protocols, including OAuth 2.0, OpenID, and PKI, are used for key management and authentication [17, 18]. Fig. 2 also illustrates a structured architecture based on the most prevalent IoT protocols for applications, emailing, authentication, key management, routing and transfer, and those for physical devices. The physical layer and the MAC (Media Access Control) layer are two low-level layers specified by the IEEE 802.15.4 standard. The physical layer specification relates to data rates and frequency bands for wireless channels used for communication. The channel access techniques and synchronization are covered by the MAC layer specification. Routing Protocol for Low Power and Lossy Networks (RPL) [19] is used to provide IPv6 across low-power wireless personal area network (6LoWPAN) environments, enabling connection and exchange between numerous points and a single point; this standard also permits point-to-point traffic. Due to the limited payload, User Datagram Protocol (UDP) [20] is used in the IoT application architecture for communication. The UDP protocol is considered more efficient and simpler than the TCP protocol. Additionally, UDP header compression guarantees that the restricted payload space is used more effectively [21]. CoAP (Constrained Application Protocol) [22] presents a model for low-power loss networks working in confined spaces based on demand response. Additionally, it permits asynchronous message transmission and has the ability to connect to IoT resources using HTTP mapping, LPWAN enables long-range connections of IoT "objects." It provides low-power and low-bit-rate connectivity compared to a wireless WAN that demands more energy to operate at a high bit rate. LPWAN provides connectivity between gateways and end devices to manage changing data rates.

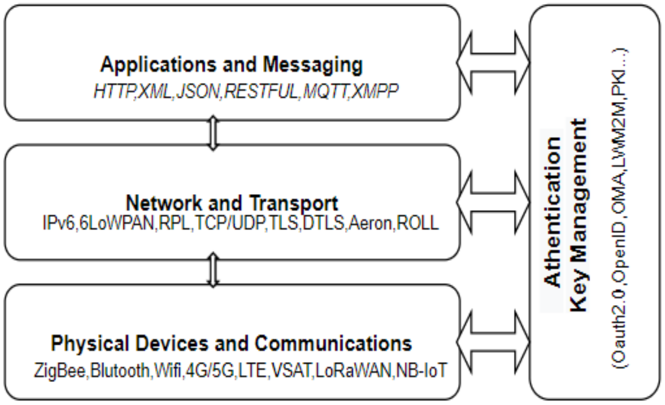
Applications and Messaging
HTTP,XML,JSON,RESTFUL,MQTT,XMPP
Network and Transport
IPv6,6LoWPAN,RPL,TCP/UDP,TLS,DTLS,Aeron,ROLL
Physical Devices and Communications
ZigBee,Blutooth,Wifi,4G/5G,LTE,VSAT,LoRaWAN,NB-IoT
Athentication
Key Management
(Oauth2.0,OpenID,OMA,LWM2M,PKI...)

Fig. 2. The protocols and standards of IoT.

B. Security Requirements

Several research initiatives have been proposed in recent years to identify various methods for securing the connection between an end device and its components. The primary objectives of the Internet of Things are the configuration of a smart environment and autonomous devices, such as smart living, smart objects, smart health, and smart cities, among others domains [23]. Ensuring security in smart systems poses a major challenge, due to the diversity and complexity of the end device and its components [24,25]. Fig. 3 illustrates the considerations that must be made to ensure the reliability and security of IoT implementation.

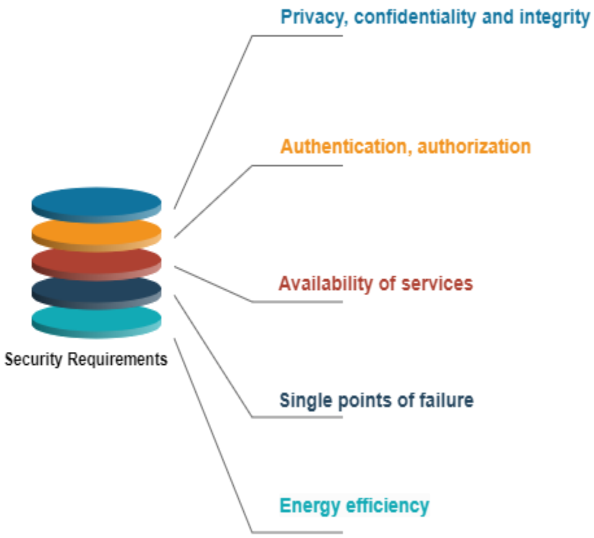

Fig. 3. Security requirements for IoT.

- Privacy, confidentiality, and integrity

Given that IoT data moves over several network hops, an appropriate encryption technique is needed in order to assure the privacy of the data. And this, because of the diversity of services and microservices integration, means that the vast majority of the information saved and kept on any device is exposed to invasions of privacy, and assaults can allow a malicious user to gain data integrity by changing the saved data for illegal uses.

- Authentication and authorization

In order to ensure secured IoT communication between different devices, authentication is paramount between the different parties who are communicating. the multiplicity of IoT device architectures and different underlying ecosystems are primarily responsible for the IoT devices' wide range of authentication procedures. Creating an associated standard protocol for authentication in the IoT will be extremely difficult in these situations. Similar to that, authorization methods make sure that only authorized people are allowed access to systems or information. Additionally, keeping track of how resources are used and making sure they are used correctly through audits and reports is a reliable and effective way to manage network security.

- Availability of services

Traditional denial-of-service attacks against IoT devices could obstruct the delivery of services. Different tactics, such as replay assaults, sinkhole attacks, and jammer advertisements, employ IoT components at various stages to reduce the quality of service (QoS) offered to IoT users.

- Single points of failure

IoT-based infrastructure's continuous reliance on heterogeneous networks has the potential to expose numerous single points of failure, which could harm the IoT's intended services. As a result, it's necessary to create a safe environment in order to accommodate a greater number of Internet of Things devices and to propose other techniques to build a fault-tolerant system.

- Energy management

IoT devices frequently have a small battery life and a weak storage capacity. Attacks on IoT systems can lead to increased power usage by saturating the network and draining device resources with repetitive and false service queries.

III. Security Issues Classification

Nowadays, several reports and research findings indicate that the IoT is susceptible to various forms of attack, such as active and passive attacks, which have the potential to disrupt the operation of the device as well as affect its functionality and remove the benefits of its services. A taxonomy of security issues related to the Internet of Things has been developed and presented in Fig. 4 based on the IoT deployment architecture, as mentioned below:

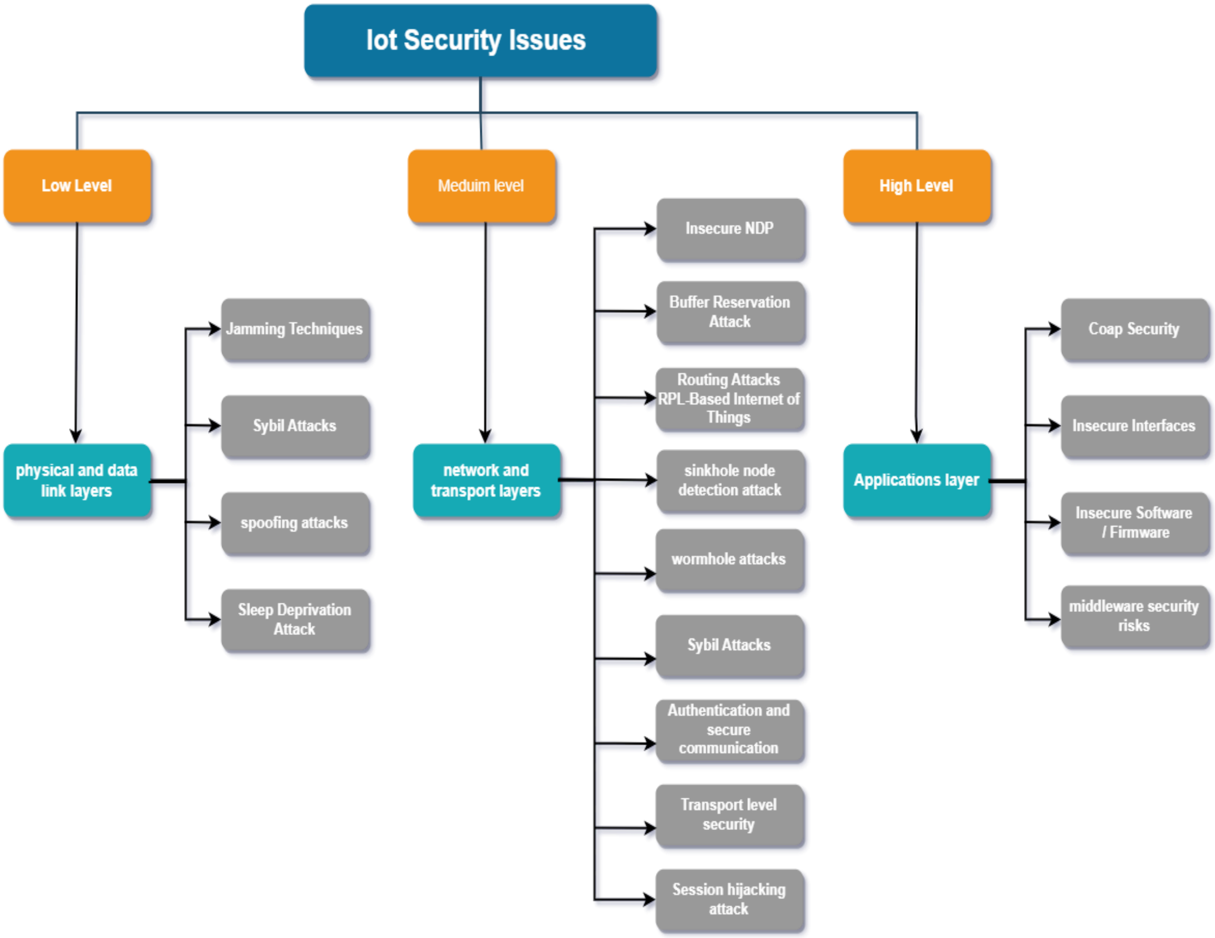

Fig. 4. Classification of security issues.

A. Low Security Issues

It relates to security vulnerabilities at the hardware level as well as the physical and data link levels of communication, as described below:

- Jamming attacks

Jamming is an attack method that disrupts the radio signals utilized by nodes in a network. It's characterized as the intentional use of electromagnetic radiation to disrupt or disable a communication system. These attacks aim to degrade networks by transmitting Radio frequency (RF) signals without having to adhere to a specified protocol [26, 27]. Radio interference has a significant impact on how a network operates because it interferes with authorized nodes' ability to send and receive data, which makes the system unstable or dysfunctional.

- Low-level Sybil attacks:

Malicious Sybil nodes utilize false identities to carry out Sybil attacks on wireless networks and impair IoT capabilities. A Sybil node may employ random, fabricated MAC values on the physical layer to pretend to be another device in order to drain network resources [28]. This could prevent the authorized nodes from getting access to resources.

- Spoofing attacks

Spoofing attacks are simple to launch on an access IoT network. An attacker can pretend to be another approved IoT device by claiming the real user's MAC or IP (internet protocol) address. The attacker can perform attacks on the IoT network after gaining illegal access.

- Sleep deprivation attack

The target of this attack is battery-operated computational hardware, like a sensor node, which is trying to conserve power by entering a low-power sleep state for as long as feasible without disrupting the node's activities [29].

By keeping the sensor nodes awake, "sleep deprivation" attacks can take advantage of energy-constrained IoT devices [30]. The battery is drained when too many tasks are scheduled to run in 6LoWPAN.

B. Meduim-Level Security Issues

The security concerns at the intermediate level primarily pertain to the communication, routing, and session management that occur at the network and transport layers of IoT, as outlined below:

- Insecure NDP

Every device must have a unique network identifier in order to comply with the IoT deployment architecture. Secure communication transmission is required for security purposes. To ensure that all information sent to a device across a continuous connection reaches its intended destination, the phase of neighbor discovery performs a number of operations prior to data transfer, including router detection and resolving addresses [31]. Utilizing neighbor discovery packets without conducting adequate verification could have serious consequences, including distributed denial of service (DDoS) attacks.

- Buffer reservation attack.

An attacker may take advantage of this by delivering incomplete packets to a receiving node must allocate slots for the reassembling of received packets [32]. Due to the attacker's unfinished packets taking up space and causing other fragment packets to be deleted, this attack causes denial-of-service.

- Routing Attacks RPL-Based

The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is susceptible to numerous attacks that are launched by infected network nodes [33]. This attack might cause resource exhaustion and eavesdropping.

- Sinkhole Node detection attacks

The attacker uses falsified routing information to lure nearby nodes, after which it performs selective forwarding or modifies the data traveling through them as illustrated in Fig. 5. The attacking node asserts that it is providing a very alluring link. As a result, this node is skipped by a lot of traffic. The sinkhole attack can be combined with other attacks besides straightforward traffic analysis, such as selective forwarding or denial of service.

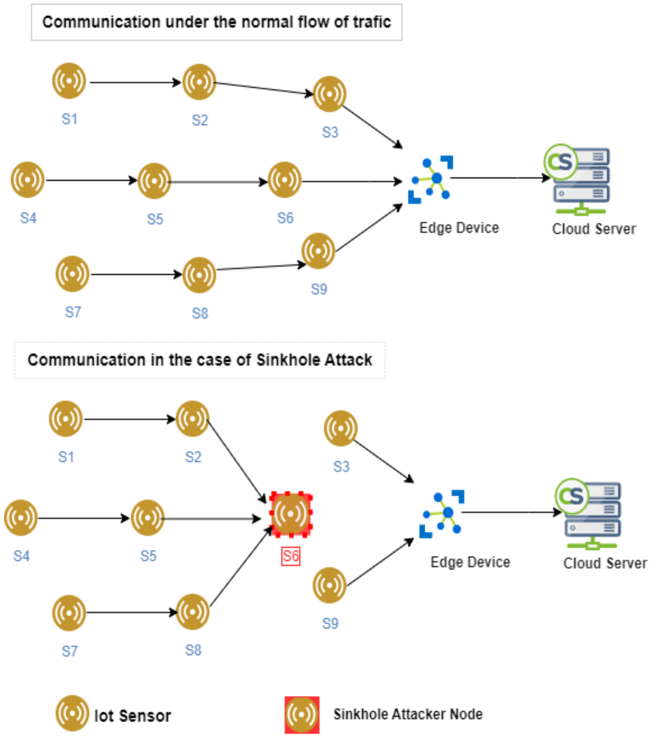

Fig. 5. Sinkhole attack in Internet of Things communication.

- wormhole attacks

During a wormhole attack, as illustrated in Fig. 6 the data is delivered across many channels, or the malicious node makes use of the incoming data in various ways. Due to these attacks, which form a tunnel connecting two nodes to ensure that the packets coming from one node immediately reach the other node, 6LoWPAN operations can be further hampered by network attacks [34].

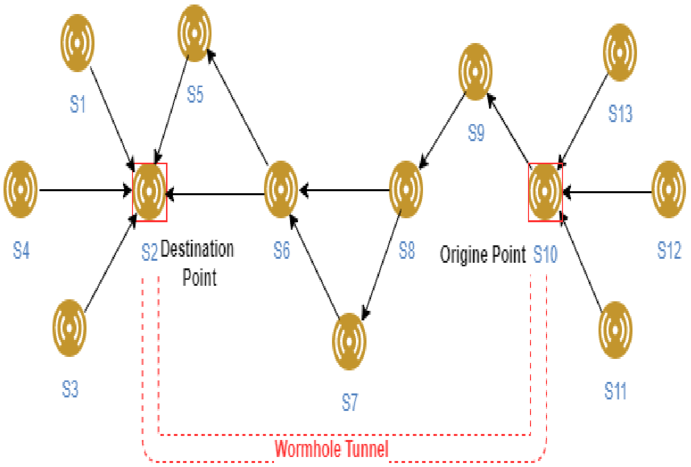

Fig. 6. Wormhole attack in internet of things.

- Sybil Attacks

The deployment of Sybil nodes can affect network performance and breach data privacy. In a network, Sybil nodes communicating under false identities run the risk of sending spam, spreading malicious software, or conducting phishing attacks [35].

In Fig. 7, the lowest layer contains one Sybil node and four regular nodes. However, due to the fact that the Sybil node carries several identities in the overlay network, there are three Sybil nodes in the top layer. In this situation, the Sybil node has the ability to seize network control. For instance, the Sybil node has the ability to transmit malicious software to conduct a DDoS attack or fake computation results to disrupt the nodes that are not malicious.

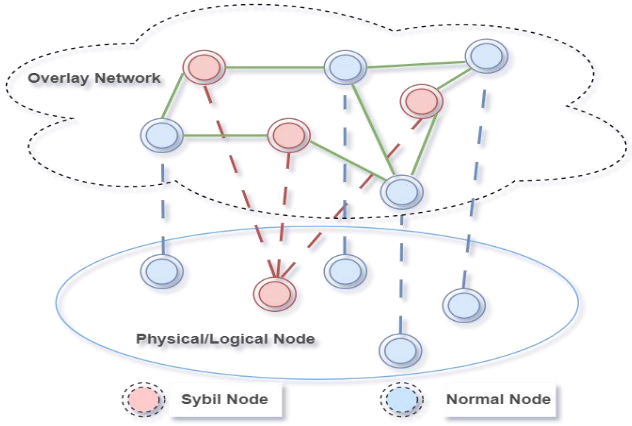

Fig. 7. illustration of Sybil nodes and the Sybil attack.

- Authentication and secure communication

Device identification is done through authentication, and permissions are given through authorization. IoT devices employ these procedures to perform role-based access control and make sure that only the access and permissions necessary for their tasks are granted to devices. The use of applications and other devices requires authorization. Cloud accounts, gateways, and key management systems are required for the IoT to authenticate people and devices. Any security flaw at the network layer or significant cost associated with communication security may expose the network to several vulnerabilities [36–38]. Due to limited resources, for example, Datagram Transport Level Security (DTLS) overhead must be kept to a minimum, and the cryptographic algorithms enabling secure data flow in the Internet of Things require consideration of the lack of other resources and performance [39].

- Transport level security

The goal of end-to-end security at the transport level is to provide secure mechanisms which ensure that the sending node's data is reliably received by the target destination node [37]. It required extensive authentication processes that offer encrypted secure message transfer while maintaining privacy and run with the least amount of overhead possible [40,41].

- Session hijacking attack

Denial-of-service may be caused via the hijacking of a session on the transport layer using falsified messages [42]. An attacker node might prolong the session between the two nodes by acting as though it is the victim node by faking its identity. By changing the sequence numbers, the communicating nodes may even need to resend messages.

C. High Level Security Issues

Most high-level security problems affect IoT apps that run at the application and communications layers, as will be discussed below:

- CoAP security

A CoAP (Constrained Application Protocol) is an IETF standard, and RFC 7252 defines the basic protocol. Additional extensions are defined in several RFCs. It works well for nodes that communicate over LPWAN, such as 6LoWPAN, and are powered by basic microcontrollers with little ROM and RAM. UDP is used as the underlying transport protocol, and it operates at the application layer of the TCP/IP stack. RFC 8323, a new standard that covers CoAP over TCP, TLS, and WebSockets, was published in 2018. Attacks can potentially target the high-level layer, which houses the application layer [43–44]. In order to guarantee end-to-end security, the Limited Application Protocol (CoAP) combines DTLS bindings with a variety of security options. The CoAP messages must be encrypted for safe communication and adhere to a certain format specified in RFC-7252 [22]. Similar to this, suitable key management and authentication techniques are needed for CoAP's multicast capability.

- Insecure Ecosystem interfaces

The user interfaces for IoT services on the web, mobile, and cloud are vulnerable to a number of risks that pose a major risk to data privacy [45].

- Insecure Software / Firmware

Insecure software/firmware is one source of numerous IoT vulnerabilities [45]. Carefully testing the code that uses languages like JSON, XML, SQLi, and XSS is necessary. Similar to this, firmware and software upgrades should be made properly.

- Middleware security

The Internet of Things middleware must be sufficiently secure to enable service delivery among the diverse elements of the Internet of Things paradigm [61,62]. To offer reliable and safe communication, several middleware-based interfaces and environments must be used.

IV. Security Solutions for IoT

IoT security threats take advantage of flaws in a variety of components, including applications and interfaces, network components, and different levels of software, firmware, and physical devices. In the IoT paradigm, users communicate with these components using protocols that might not be secure. We've broken out the security risks for each IoT layer level in this area, along with their relevance and the suggested appropriate solutions for each of the cases listed in Section III.

This section examines the key security solutions that have been put forth. Table I presents a comparative analysis of security threats and potential countermeasures for the lowest level, the middle level, which includes the transit layer, and the highest level, respectively. All of the threat parameters, their effects, and comparative analyses are taken into consideration.

A. Low-Level Security Solutions

Jamming attacks on Wireless Sensor Networks (WSN) involve interference that causes message collisions or channel floods. Young et al. [48] present a method for detecting jamming attacks by determining the signal quality, which will be used to extract noisy signals; attacks can be detected in this manner. Then, for attack detection, these statistics are compared to preset threshold levels. False MAC values could be used by a malicious Sybil node to impersonate another device. It may lead to resource exhaustion and the denial of access to authorized network devices. Demirbas et al. [49] provide a method for identifying Sybil attacks using signal strength measures. In order to determine the sender position during message communication, their method deploys detector nodes. When a different message communication has the same sender location but a different sender identity, a Sybil attack is suspected. MAC address signal strength measurements are used to spot spoofing attempts. The study [30] outlines a methodology for preventing sleep deprivation attacks in WSNs. The suggested architecture uses a cluster-oriented model, in which each cluster is further broken down across various areas. Avoiding long-distance communication lowers energy use. A wireless sensor network architecture with five layers is used by the framework to perform intrusion detection.

TABLE I. COMPARATIVE ANALYSIS OF SECURITY THREATS AT THE IOT LEVEL, IMPLICATIONS, AND POTENTIAL COUNTERMEASURES

IoT levels	Security issue	Implications	layers	Suggested Solution
Low	Jamming Technique	Destabilization and Denial of service (DoS)	Physical	Changing frequencies and locations, encoding packets, and measuring the packet delivery ratio.
	Sybil attacks	Network disruption, DoS	Physical	Measurements of the signal strength and channel estimation
	Spoofing attacks	Network disruption, DDoS	Physical	Measurements of the signal intensity and channel estimation
	Sleep deprivation attack	Energy consumption	Link	Intrusion detection system with multiple layers
Medium	Insecure NDP	IP Spoofing	Network	Using SEND's signature algorithm agility and multiple-key CGA to secure NDP messages Signature authentication using Elliptic Curve Cryptography (ECC)
	wormhole attacks	DoS	Network	Rank verification through hashing chain function Anomaly detection through IDS rank verification via the hash chain function
	Buffer reservation attack	Closing reassembly buffer	6LoWPAN adaptation, Network	Address space layout randomization (ASLR) Split buffer approach
	Authentication and secure communication	Privacy violation	6LoWPAN adaptation, Transport Network	OTP, Digital Signature, and Mutual Authentication Using ECDSA for signing and verification and ECDH for encryption Public Key Cryptography TPM employing RSA, hybrid authentication, compression and software-based AES IACAC using the Elliptic Curve Cryptography
	Routing Attacks RPL-Based	Eavesdropping, man-in-the-middle attacks	Network	Monitoring node behavior and authentication Using hashing and signatures Placement of an IDS or IPS in the IoT Eliminating malicious nodes from RPL by using a whitelist or a blacklist Nodes
	Sinkhole Node detection attacks	DoS	Network	Signal intensity measurement, Graph Traversal Analysis, IDS anomaly detection, cryptographic key management, communication behavior analysis, rank verification via hash chain function
	Sybil Attacks	Privacy violation, spamming	Network	verification of identities observing user behavior and keeping a list of trusted and untrusted users
	Transport level security	Privacy violation eavesdropping	Transport, Network	Using the 6LoWPAN Border Router (6LBR) as a conduit between nodes and the inter-net IKEv2 employing compressed UDP, compressed IPSEC, and DTLS header compression.
	Session hijacking attack	DoS	Transport	Encrypting all data transmitted Session Management Session Key
High	CoAP security	Network bottleneck, DoS	Application, Network	protection by Datagram Transport Layer Security (DTLS) TLS-tunnel Filtering messages using 6LBR
	Insecure interfaces	DoS, invasion of privacy, and network disruption	Application	Use of https and firewalls; prevention of the use of weak passwords by enforcing expiration policies and forcing compliance with password complexity requirements; assessment of the interface against software tool vulnerabilities (SQLi and XSS).
	Insecure Software / Firmware	DoS, invasion of privacy, and network failure	Application, Transport	updating software and firmware securely on a regular basis, using file signatures, and encrypting data with validation
	Middleware security	DoS, invasion of privacy, and network failure	Application, Transport, Network	The safeguarding of communication is achieved through the implementation of authentication protocols, security policies, key management mechanisms between devices, gateways, and M2M components, as well as transparent middleware.

B. Mediate-Level Security Solutions

Riaz et al. [31] suggest a security system that includes modules for secure neighbor finding, authentication, key generation, and data encryption. Elliptic Curve Cryptography (ECC) [50] is utilized for secure neighbor finding. In the neighbor discovery phase, nodes are identified using ECC public key signatures. Depending on the needs of the application, both symmetric and asymmetric key management solutions are recommended for deployment. Then, in order to guarantee node-to-node security, the encrypted data is transmitted.

A node's reassembly buffer could be prevented by a buffer reservation attack. This attack is lessened by the split buffer technique [32], which raises the cost of launching the attack by necessitating the transmission of full fragmented packets in brief bursts. Each node must calculate the completion rate of the packet and monitor the behavior of sending pieces. When under load, the node may reject packets that have low fragment percentages or a high fragment sending pattern fluctuation.

The Directed Acyclic Graph (DAG) is created by the RPL protocol with root at any of the gateways. RPL utilizes ranks to describe the quality of the path to the last sink node. To link to the root for eavesdropping, a node's rank value may be reduced. Version Number and Rank Authentication (VeRA), a proposed security technique, authenticates version numbers and rankings using the hash function (SHA), MAC function (HMAC), and digital signature (RSA) [51,52].

Weekly et al. propose a strategy that involves failover and authentication techniques to counter sinkhole attacks. [53], Pirzada et al. [54] provide another approach to thwart sinkhole attacks by utilizing various trust levels. Their method makes use of a variety of Dynamic Source Routing (DSR) protocol features to identify and prevent wormhole and sinkhole attacks in wireless networks.

Pseudo-identities, also known as Sybil nodes, are used in Sybil attacks on the network layer to impersonate numerous distinct identities. Peer-to-peer (P2P) and distributed systems, such as the Internet of Things, are seriously at risk from these attacks. A trust connection is added to social networks to prevent the establishment of Sybil identities [55]. By moving across the graph randomly or utilizing community detection methods, legitimate nodes can use the countermeasures employing social graphs to identify Sybil nodes. [42,56–57] Similar to this, users' behavior in relation to network activity is examined; users who consistently follow the same pattern are automatically labeled as sybils. [35]. Mahalle et al. have proposed a method that can protect the Internet of Things against attacks involving a man-in-the-middle as well as denial-of-service (DoS) attacks.

In a networked environment, man-in-the-middle attacks resulting from secret keys exposed as a result of eavesdropping may lead to identity theft. Additionally, the credentials or identity information might be replayed by attackers to influence network traffic. The Elliptic Curve Cryptography-based Diffie Hellman algorithm is used to mutually authenticate devices for communication and access via encryption and secret keys. With capability-based access, two devices' capacity to communicate is first confirmed. Additionally, before performing the actual operation, the device's capacity to carry out the specified functionality is verified. To create secret keys in the proposed method is known as Identity Authentication and Capability-based Access Control (IACAC). Kothmayr et al. [59, 60] detail a strategy for achieving end-to-end security by employing public key cryptography in conjunction with two-way authentication. For the purpose of storing the network's publishers' access privileges, a reliable access control server is built, and the publisher's website must store both the publisher's and the Authority's certificates. Authentication can be done with RSA or DTLS preshared keys by the Trusted Platform Module (TPM) processors [61], whereas TPMs are utilized to transmit RSA certificates in X.509 format.

Alghamdi et al. [62] recommend using Transport Layer Security pre-shared key ciphersuites (TLS-PSK) to ensure security during the entire transaction, allowing communication to occur between HTTP and CoAP. This necessitates a conversion message on the DTLS layer. Similar to this, a DTLS extension including pre-shared key (PSK) is recommended to provide processing of session keys for multicast message security. The 6LoWPAN Border Router (6LBR) is proposed as a dedicated authentication approach for transport-level security [37]. The 6LBR is able to intercept packets, compute for public key authentication, and then forward them. For the implementation of transport-level security, elliptic curve cryptography (ECC) is used. Also, end-to-end security at the transport level has been proposed using a variety of header compression approaches. Raza et al. [63] offer a method for reducing the size of the maximum transmission unit (MTU) of 6LoWPAN packets by compressing DTLS Record and Handshake headers and other Handshake data. An additional technique for encryption that employs hash functions for devices with limited resources has been suggested. The efficiency of the system is attributed to its minimal computational overhead. A proposed approach for achieving mutual authentication in fog computing environments that involve devices with limited resources is presented in research [58].

Park et al. [42] provide a mutual authentication strategy for safe session management with symmetric key-based encryption techniques. The suggested method first chooses a random number, encrypts it, and creates a session key that is then used to encrypt another random number. The encrypted number serves as an authentication key. Another hash-based encryption technique is also suggested for devices with limited resources that implement hash functions. As a result of the minimal computational overhead, it operates effectively.

C. High-Level Security Solutions

A method using TLS and DTLS is suggested by Brachmann et al. [43] to secure CoAP-based Low-power and Lossy Networks (LLN) connected to the internet. The suggested method is effective in situations where a 6LoWPAN Border Router (6LBR) connects the LLN to the internet so that devices can be accessed remotely. The CoAP and HTTP clients are serviced by the LLN nodes. It is suggested to map TLS and DTLS to provide end-to-end security that shields LLNs against internet-based threats.

Granjal et al. [64] present a different method of protecting messages for applications connecting across the internet utilizing various CoAP security parameters. SecurityOn, SecurityToken, and SecurityEncap are the new security settings for CoAP.

The SecurityOn option is important for the security of CoAP messages at the application level. Through identity and permission, the SecurityToken option at the application level makes it easier to access CoAP resources. The SecurityEncap option performs [65] and proposes a security paradigm that uses 6LBR for message filtration to guarantee end-to-end security for IoT. The TLS-DTLS tunnel can be formed. Similar to this, it is advised that message verification or replay detection be carried out at the CoAP device when two hosts share the same key. Sethi et al. [44] present an energy-efficient security paradigm for IoT-based CoAP based on public key cryptography. The proposed security architecture, which is a model, employs a mirror proxy (MP) and resource directory to service demands throughout the server's sleep process and to supply a catalog of the endpoint's resources.

The OWASP project [45] offers suggestions for IoT security countermeasures to deal with vulnerable high-level interfaces, including setups that prevent the use of weak passwords and evaluate the interface for common software tool weaknesses (SQLi and XSS), and utilize firewalls and secure HTTPS connections. Additionally, through a secure transfer method, the device's software or firmware should be frequently updated. The updated files need to be signed and correctly validated before installation, and they should be downloaded from a secure site.

Conzon et al. [46] have proposed the utilization of VIRTUS middleware to provide authentication and encryption for safeguarding distributed applications that operate within an IoT ecosystem.

IoT middleware solutions are heavily used in contexts with limited resources, such as memory, computational power, and the network. Because of this, middleware system components must cope with lightweight security techniques. However, it is seen as difficult to deploy new security strategies in accordance with the demands of certain Internet of Things applications. Liu et al. [47] propose a middleware server that provides data filtering during communication among heterogeneous IoT environments. The suggested middleware offers effective methods for addressing, naming, and profiling in a variety of settings. A key hierarchy comprising keys for the root, applications, and services is used to achieve the common authentication, authorization, and accounting (AAA) functionalities. A web-based portal is used to register for services, limiting access to those services to approved users. A common architecture with various security layers is suggested for machine-to-machine (M2M) communications in the IoT environment [66].

The resource contents should be encrypted for M2M service layer security, and securing message transmission using TLS or DTLS sessions is recommended. The study [67] suggests a security architecture for IoT middleware that makes use of accepted encryption techniques like AES to ensure data confidentiality. The proposed architecture-based approach has the ability to secure the communications of IoT entities, such as users, devices, and services.

V. Conclusion

Today's Internet of Things devices are unsafe and vulnerable, and they are not able to provide any security to protect themselves. This is due to the resource limitations in IoT devices as well as the lack of developed standards and weakly implemented security measures in hardware and software.

This paper presents an analysis of IoT security issues. The components of IoT technology are defined, and the areas of its application are considered. An analysis of the security of the Internet of Things has been carried out; looking at assets and technologies, and a classification of these issues has been compiled into three groups according to the standard IoT layers: high, medium, and low. We briefly go over the literature-proposed approaches for utilizing IoT security at various tiers; requirement for security, including privacy, authenticity, and integrity, is discussed; in addition, we present a parametric evaluation of IoT possible attacks and countermeasures. We analyze the effects of the attack and connect them to countermeasures that have been presented in the literature. The ultimate goal of addressing IoT security and protection issues is to ensure that all assets are prioritized, maintain the required level of privacy, and achieve and maintain a high level of attack resistance, thereby ensuring comprehensive security.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) pp.2787–2805.doi.org/10.1016/j.comnet.2010.05.010.

[2] D. Giusto, A. Iera, G. Morabito, L. Atzori, The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications’. Springer Publishing Company, Incorporated, 2014.

[3] Stolojescu-Crisan, C., Crisan, C., & Butunoi, B.-P. (2021). Access Control and Surveillance in a Smart Home. High-Confidence Computing, 100036. doi: 10.1016/j.hcc.2021.100036

[4] Khan, A. A., Rehmani, M. H., & Rachedi, A. (2017). Cognitive-Radio-Based Internet of Things: Applications, Architectures, Spectrum Related Functionalities, and Future Research Directions. IEEE Wireless Communications, 24(3), 17–25. doi:10.1109/mwc.2017.1600404

[5] Akhtar, F., Rehmani, M. H., & Reisslein, M. (2016). White space: Definitional perspectives and their role in exploiting spectrum opportunities. Telecommunications Policy, 40(4), 319–331. doi: 10.1016/j.telpol.2016.01.003

[6] M.Sadeeq, M. A., Zeebaree, S. R. M., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018). Internet of Things Security: A Survey. 2018 International Conference on Advanced Science and Engineering (ICOASE). doi:10.1109/icoase.2018.8548785.

[7] Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials, 17(3), 1294–1312. doi:10.1109/comst.2015.2388550.

[8] Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials, 17(3), 1294–1312. doi:10.1109/comst.2015.2388550.

[9] Cirani, S., Ferrari, G., & Veltri, L. (2013). Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview. Algorithms, 6(2), 197–226. doi:10.3390/a6020197.

[10] utun, I., Morgera, S. D., & Sankar, R. (2014). A Survey of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications

Surveys & Tutorials, 16(1), 266–282. doi :10.1109/surv.2013.050113.00191 .

[11] Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection in wireless network applications. Computer Communications, 42, 1–23. doi: 10.1016/j.comcom.2014.01.012.

[12] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. doi:10.1016/j.comnet.2014.11.008.

[13] Oleshchuk, V. (2009). Internet of things and privacy preserving technologies. 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology. doi:10.1109/wirelessvitae.2009.51.

[14] Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, 55(1), 26–33. doi:10.1109/mcom.2017.1600363.

[15] Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). IoT Security: Ongoing Challenges and Research Opportunities. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. doi:10.1109/soca.2014.58 .

[16] Alghamdi, A., Mohammed, T., Alsulami,. (2019). Toward a Smart Campus Using IoT: Framework for Safety and Security System on a University Campus.doi: 10.25046/aj040512.

[17] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017, 1–25. doi:10.1155/2017/9324035.

[18] Wang, Y., Uehara, T., & Sasaki, R. (2015). Fog Computing: Issues and Challenges in Security and Forensics. 2015 IEEE 39th Annual Computer Software and Applications Conference. doi:10.1109/compsac.2015.173.

[19] Mercy Amrita C., & Pravin Renold A. (2014). Routing protocol for low power lossy networks. 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies. doi:10.1109/icaccct.2014.7019343.

[20] J. Postel, User datagram protocol, 1980. URL https://tools.ietf.org/html/ rfc768.

[21] J.W. Hui, P. Thubert, Compression format for IPv6 datagrams over IEEE 802.15.4-based networks, 2011. URL https://tools.ietf.org/html/rfc6282.

[22] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (CoAP), 2014. URL https://tools.ietf.org/html/rfc7252

[23] Abomhara, M., Ien, G.M.K., 2015. Cyber Security and the Internet of Things: Vulnerabili-ties, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility 4, 60–90.

[24] Hager, M., Schellenberg, S., Seitz, J., Mann, S., & Schorcht, G. (2012). Secure and QoS-aware communications for smart home services. 2012 35th International Conference on Telecommunications and Signal Processing (TSP). doi:10.1109/tsp.2012.6256188.

[25] G. Mantas, D. Lymberopoulos and N. Komninos, Security in smart home environment,Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications (Medical Information Science, Hershey, PA, 2010), pp. 170–191.

[26] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc '05. doi:10.1145/1062689.1062697.

[27] Noubir, G., & Lin, G. (2003). Low-power DoS attacks in data wireless LANs and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3), 29. doi:10.1145/961268.961277.

[28] Chen, Y., Trappe, W., & Martin, R. P. (2007). Detecting and Localizing Wireless Spoofing Attacks. 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. doi:10.1109/sahcn.2007.4292831.

[29] Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M., & Brooks, R. (2006). The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. International Journal of Distributed Sensor Networks, 2(3), 267–287. doi:10.1080/15501320600642718.

[30] Bhattasali, T., & Chaki, R. (2011). A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network. Communications in Computer and Information Science, 268–280. doi:10.1007/978-3-642-22540-6_27.

[31] Riaz, R., Kim, K.-H., & Ahmed, H. F. (2009). Security analysis survey and framework design for IP connected LoWPANs. 2009 International Symposium on Autonomous Decentralized Systems. doi:10.1109/isads.2009.5207373.

[32] Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (2013). 6LoWPAN fragmentation attacks and mitigation mechanisms. Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '13. doi:10.1145/2462096.2462107.

[33] Dvir, A., Holczer, T´., & Buttyan, L. (2011). VeRA - Version Number and Rank Authentication in RPL. 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. doi:10.1109/mass.2011.76.

[34] Wazid, M., Das, A. K., Kumari, S., & Khan, M. K. (2016). Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Security and Communication Networks, 9(17), 4596–4614. doi:10.1002/sec.1652.

[35] Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil Attacks and Their Defenses in the Internet of Things. IEEE Internet of Things Journal, 1(5), 372–383. doi:10.1109/jiot.2014.2344013 .

[36] Granjal, J., Monteiro, E., & Silva, J. S. (2012). Network-layer security for the Internet of Things using TinyOS and BLIP. International Journal of Communication Systems, 27(10), 1938–1963. doi:10.1002/dac.2444.

[37] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ecc public-key authentication, in: 2013 IFIP Networking Conference, 2013, pp.1–9.

[38] Granjal, J., Monteiro, E., & Silva, J. S. (2010). Enabling Network-Layer Security on IPv6 Wireless Sensor Networks. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010. doi:10.1109/glocom.2010.5684293.

[39] D.U. Sinthan, M.-S. Balamurugan, Identity authentication and capability-based access control (IACAC) for the Internet of Things, J. Cyber Secur. Mob.1 (4) (2013) 309–348.

[40] Peretti, G., Lakkundi, V., & Zorzi, M. (2015). BlinkToSCoAP: An end-to-end security framework for the Internet of Things. 2015 7th International Conference on Communication Systems and Networks (COMSNETS). doi:10.1109/comsnets.2015.7098708.

[41] S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in: Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.

[42] Park, N., & Kang, N. (2015). Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle. Sensors, 16(1), 20. doi:10.3390/s16010020.

[43] Brachmann, M., Keoh, S. L., Morchon, O. G., & Kumar, S. S. (2012). End-to-End Transport Security in the IP-Based Internet of Things. 2012 21st International Conference on Computer Communications and Networks (ICCCN). doi:10.1109/icccn.2012.6289292.

[44] Sethi, M., Arkko, J., & Keranen, A. (2012). End-to-end security for sleepy smart object networks. 37th Annual IEEE Conference on Local Computer Networks - Workshops. doi:10.1109/lcnw.2012.6424089.

[45] OWASP, Top IoT Vulnerabilities, 2019. URL https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf.

[46] Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., & Spirito, M. A. (2012). The VIRTUS Middleware: An XMPP Based Architecture for Secure IoT Communications. 2012 21st International Conference on Computer Communications and Networks (ICCCN). doi:10.1109/icccn.2012.6289309 .

[47] Liu, C. H., Yang, B., & Liu, T. (2014). Efficient naming, addressing and profile services in Internet-of-Things sensory environments. Ad Hoc Networks, 18, 85–101. doi:10.1016/j.adhoc.2013.02.008.

[48] Young, M., & Boutaba, R. (2011). Overcoming Adversaries in Sensor Networks: A Survey of Theoretical Models and Algorithmic Approaches

for Tolerating Malicious Interference. IEEE Communications Surveys & Tutorials, 13(4), 617–641. doi:10.1109/surv.2011.041311.0015.

[49] Demirbas, M., & Youngwhan Song. (n.d.). An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06). doi:10.1109/wowmom.2006.27 .

[50] R. Harkanson, Y. Kim, Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications, in: Proceedings of the 12th Annual Conference on Cyber and Information Security Research, CISRC '17, ACM, New York, NY, USA, 2017, pp. 6:1–6:7.

[51] D. Eastlake, P.E. Jones, RFC 3174 - US Secure Hash Algorithm 1 (SHA1), 2001. URL https://tools.ietf.org/html/rfc3174.

[52] H. Krawczyk, M. Bellare, R. Canetti, HMAC: keyed-hashing for message authentication, 1997. URL https://tools.ietf.org/rfc/rfc2104.txt.

[53] Weekly, K., & Pister, K. (2012). Evaluating sinkhole defense techniques in RPL networks. 2012 20th IEEE International Conference on Network Protocols (ICNP). doi:10.1109/icnp.2012.6459948.

[54] A.A. Pirzada, C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks, in: International Workshop on Wireless Ad-Hoc Networks, 2005.

[55] Alvisi, L., Clement, A., Epasto, A., Lattanzi, S., & Panconesi, A. (2013). SoK: The Evolution of Sybil Defense via Social Networks. 2013 IEEE Symposium on Security and Privacy. doi:10.1109/sp.2013.33 .

[56] Mohaisen, A., Hopper, N., & Kim, Y. (2011). Keep your friends close: Incorporating trust into social network-based Sybil defenses. 2011 Proceedings IEEE INFOCOM. doi:10.1109/infcom.2011.5934998.

[57] Kim, H. (2008). Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer. 2008 International Conference on Convergence and Hybrid Information Technology. doi:10.1109/ichit.2008.261.

[58] M.H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, International Journal of Network Security, 18, 6, 2016 PP.1089-1101, Nov.

[59] Kothmayr, T., Schmitt, C., Hu, W., Brunig, M., & Carle, G. (2012). A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. 37th Annual IEEE Conference on Local Computer Networks -- Workshops. doi:10.1109/lcnw.2012.6424088.

[60] Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks, 11(8), 2710–2723. doi:10.1016/j.adhoc.2013.05.003.

[61] S.L. Kinney, Trusted Platform Module Basics: Using TPM in Embedded Systems, Newnes, Newton, MA, USA, 2006.

[62] Alghamdi, T. A., Lasebae, A., & Aiash, M. (2013). Security analysis of the constrained application protocol in the Internet of Things. Second International Conference on Future Generation Communication Technologies (FGCT 2013). doi:10.1109/fgct.2013.6767217.

[63] Raza, S., Trabalza, D., & Voigt, T. (2012). 6LoWPAN Compressed DTLS for CoAP. 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems. doi:10.1109/dcoss.2012.55.

[64] Granjal, J., Monteiro, E., & Silva, J. S. (2013). Application-Layer Security for the WoT: Extending CoAP to Support End-to-End Message Security for Internet-Integrated Sensing Applications. Lecture Notes in Computer Science, 140–153. doi:10.1007/978-3-642-38401-1.

[65] M. Brachmann, O. Garcia-Morchon, S.-L. Keoh, S.S. Kumar, Security considerations around end-to-end security in the IP-based Internet of Things, Workshop on Smart Object Security, in Conjunction with IETF83, 2012.

[66] OneM2M,Security solutions –OneM2M Technical Specification, 2019. URL https://www.onem2m.org/images/files/deliverables/Release3/TS-0003_Security_Solutions-v3_10_2.pdf.

[67] Ferreira, H. G. C., de Sousa, R. T., de Deus, F. E. G., & Canedo, E. D. (2014). Proposal of a secure, deployable and transparent middleware for Internet of Things. 2014 9th Iberian Conference on Information Systems and Technologies (CISTI). doi:10.1109/cisti.2014.6877069.