iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 Issue: II Month of publication: February 2023

DOI: https://doi.org/10.22214/ijraset.2023.49016

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

Review of Threats in IoT Systems: Challenges and Solutions

Rahima Khanam
Department of Computer Science, Jamia Millia Islamia, New Delhi, India.

Abstract: The Internet of Things (IoT) is an emerging technology concept that revolutionizes our way of living, ranging from standard household objects to sophisticated industrial tools. They represent a collection of interconnected devices equipped with software, sensors, and several other tools to interact and share information with gadgets and programs in the network infrastructure through the internet in a bid to enhance their decision-making skills. However, with such significant advancements come several issues that intimidate the IT industry, which has deteriorated due to the lack of capacity of various organizations to identify, evaluate, and monitor essential features to ensure adherence to security policies. The absence of efficient and robust security procedures, inaccurate device upgrades, user unawareness, and system tracking are a few issues IoT faces from a security, privacy, and cybersecurity perspective. Thus, there is a need for comprehensive knowledge of these IoT threats and their solutions to leverage their usage efficiently. Hence, this review paper focuses on exploring the different kinds of IoT risks and their potential solutions, which are necessary for the successful performance of IoT devices.

Keywords: Internet of Things, Privacy, Security, Cybersecurity, IoT challenges, IoT solutions

I. INTRODUCTION

The Internet of Things (IoT) is an emerging technology that facilitates interaction amongst tech devices, physical objects, and sensors over wired or wireless internet connections to simplify our lives. These connected physical objects can collect, store, process, and communicate information with other devices and systems in the network infrastructure with the help of the Internet to enhance decision-making capabilities. This paradigm of hyperconnectivity was introduced by the IoT, which meant individuals and organizations could communicate with each other from distant places conveniently while improving their overall performance [1]. The core emphasis of IoT is to deliver creative solutions to various challenges and concerns in the world's business, government, and public and private sectors [2]. As a result, it has steadily become a crucial aspect of our lifestyle that we experience everywhere around us. Examples of such systems are ubiquitous in the medical field, sophisticated building management systems, smart cities, smart homes, public security, interactive sensing applications, etc. [3, 4].

The figure below demonstrates the general architecture of the IoT and how this innovation encompasses a broad range of smart devices, objects, platforms, and sensors (Fig. 1) [5].

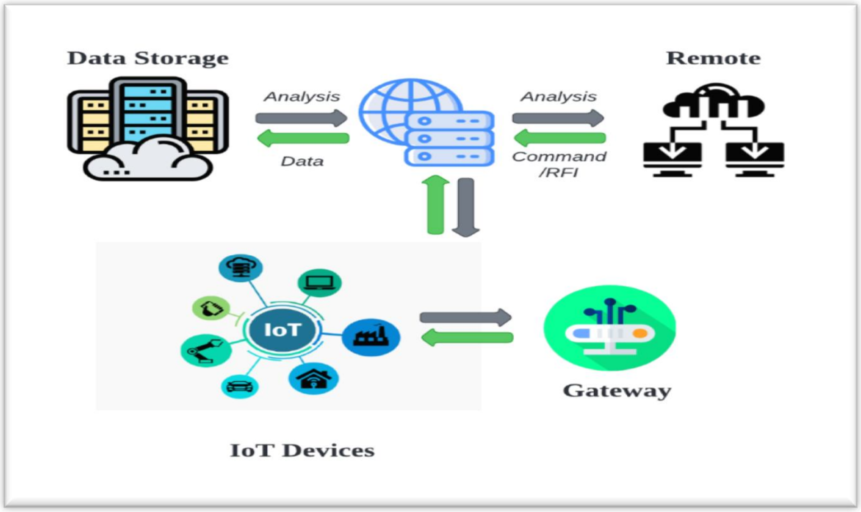

Figure. 1: Common architecture of IoT

Privacy and security challenges have increased due to the increasingly imperceptive, pervasive, and dense collection, processing, and dissemination of data in users' personal lives. In recent years, privacy has been a controversial research topic in the IT industry that is considered a powerful enabler in the world of IoT. It includes radio-frequency identification (RFIDs), wireless sensor networks (WSNs), web personalization, low-power wide area networks (LPWANs), Bluetooth, BLE-enabled devices and apps, etc. Despite significant advances by these organizations, a comprehensive understanding of the emerging privacy challenges in the IoT is lacking due to enormous technological concepts and rapidly evolving features. These advancements will exacerbate security issues and propose unforeseen risks that pose technical challenges. Moreover, unfamiliarity with these concerns might have unanticipated consequences like rejection and breakdown of new services, reputation damage, or costly lawsuits [6].

The author in [30] lists a few examples of the present IoT technologies: Microgrids for decentralized energy resource systems, self-driving cars (SDV) for automatic vehicular technologies, Smart City Drones for monitoring systems, etc. A microgrid system indicates a suitable instance of a cyber-based system that combines all distributed energy resources (DER) to deliver a detailed energy solution to a specific geographic region. Unfortunately, the IoT-based microgrid technology still depends on the classic Supervisory Control and Data Acquisition (SCADA) system. The deployment of the real and cyber areas raises vulnerability to attacks, where the attacker may target the SCADA supervisory control system, block the domain, and interfere with the objects, disrupting the performance of the supervisory control system. Additionally, the drone industry is rapidly heading towards automation and may be included in smart city monitoring, firefighting, police work, and disaster management. As users depend more on such systems, it's also tougher to preserve their security and reliability.

Cybersecurity and privacy threats are essential considerations for security professionals and researchers since they represent substantial challenges for corporate and public industries. Increased cybersecurity breaches have demonstrated the risks of IoT systems [1]. Apart from the challenges posed to IoT users, they are equally challenging for IoT engineers in the modern IT world. Consequently, IoT experts must constantly check for new threats that could occur with IoT devices and find solutions [5]. However, it is disappointing that IoT consumers do not typically have the requisite exposure to the security consequences unless a breach has happened, incurring severe loss of critical information. Furthermore, the lack of privacy and security and their potential solutions led to uncertainty about the success of the technology.

Considering these IoT issues, it is mandatory to look out for them, as their satisfactory performance will enhance the acceptance and usage of these devices. Therefore, this paper focuses on reviewing the challenges associated with IoT devices that require emphasis for their successful and optimized performance. The first section of this paper discusses the scope and architecture of IoT devices. The second section describes the major issues in IoT in terms of privacy, cybersecurity, and security, which is further continued by proposing solutions to these challenges.

II. LITERATURE REVIEW

The authors in [7] considered that regardless of the immense advantages of IoT, there are threats associated with it that need attention. The primary indications were related to cybersecurity and privacy. These two threats impose tremendous difficulties for many governments, businesses, and organizations. IoT systems have been exposed to increased cybersecurity risks due to the interconnection of networked systems from unidentified and untrustworthy sources, resulting in privacy and security concerns. Additionally, it's crucial to highlight the principles and core standards of the IoT Cyber Security Framework throughout the development of the IoT security system [8].

Research and services executed in the existing IoT security trends indicate that various services have delivered a few issues and attack avenues to numerous IoT products and their defenders [10]. The IoT security examination conducted by several simulation tools, modelers, and frameworks can validate these security procedures. Rapid progress were observed in the research area related to IoT security, where modelers and simulation tools have improved the study process. If these IoT gadgets fail, then the repercussions will be severe. According to the researchers in [11], several complications have undermined the integrity of the user's information; spoofing attempts, jamming, and other illegitimate access are examples. There are possible solutions to these threats that can assist individuals in implementing various security measures to secure their IoT systems. IoT security is primarily concerned with providing privacy, confidentiality, infrastructure, and services within the IoT system to its end users. Hence, the study of several IoT security issues is achieving the required pace with the support of various simulation software and computing environments [12]. The published reference by [13] describes that because the IoT ecosystem encloses a wide variety of systems that vary from small integrated processor chips to massive servers, these security threats require addressing at distinct layers. The author illustrates this using an IoT security issues taxonomy that covers the different categories of security issues.

The writers in [9] reported that numerous privacy issues have emerged in the current period, which can outrage IoT systems and their associated networks. Monitoring the security of IoT gadgets in various cooperative, government, and institutional sectors isn't easy. To limit the risk of getting infiltrated, these sectors must integrate surveillance and monitoring technologies for every IoT system. For preventing these threats, some common privacy threats described in [14] in the IoT infrastructure need special attention[14].

III. IOT SCOPE AND ARCHITECTURE

There exist diverse viewpoints concerning the total number of layers in the IoT architecture. But the majority of research experts [15–20] believe that the IoT largely relies on three levels, defined as the "Application," "Network," and "Perception" layers.

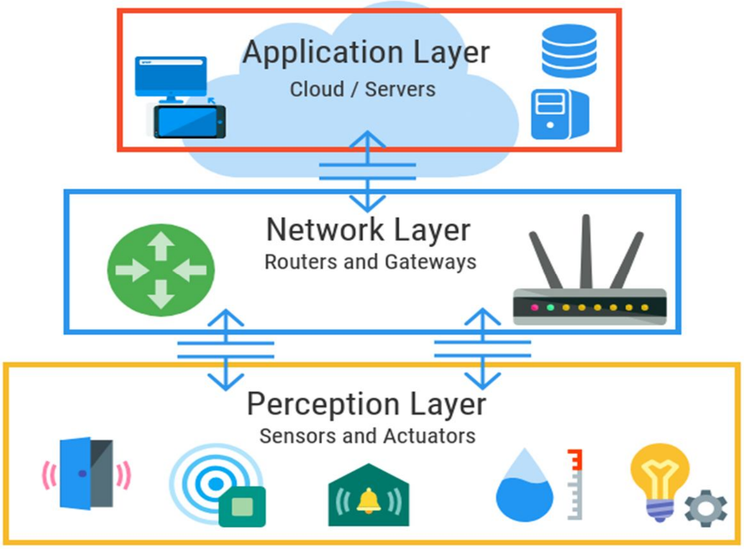

Figure 2: Three-layered IoT architecture.

In the IoT ecosystem, every layer characterizes its operations and the objects that work within them. Figure 2 demonstrates the three basic layered architectural frameworks of IoT systems, consisting of the devices, platforms, and technologies encompassing each tier.

1) *Perception Layer*: The role of the perception layer is to identify the data of every entity in the IoT ecosystem. It is also named the "Sensors Layer" of IoT infrastructure. It comprises cameras, RFID tags, sensors, etc., that recognize any device in the IoT through sensors for detecting and obtaining data on each object. This layer monitors, gathers, processes, and transfers data to the network layer [19].
2) *Network layer:* This layer of the IoT provides data processing and distribution to multiple IoT nodes and systems through the Internet. At this tier, Internet gateways, routing objects, switching devices, cloud computing platforms, etc., function via techniques like Bluetooth, WiFi, LTE, 3G, WiFi, LTE, Zigbee, etc. The network gateways operate as an intermediate for numerous IoT hubs by collecting, filtering, and transferring data between various sensing devices in the IoT infrastructure [20].
3) *Application layer:* It is subject to providing IoT application functionalities to its end users. It represents several application domains, like IoT smart cities, intelligent automobiles, smart homes, healthcare, and intelligent systems, where IoT can be deployed. This layer assures the authenticity, safety, and privacy of users' information [21].

The published study in [13] illustrates a layered IoT architecture with common protocols used within different IoT layers: Applications & Messaging (Application Layer), Routing/Forwarding (Network Layer), physical devices, key management, and authentication (Perception Layer). The figure below demonstrates the different standards and protocols for these layers.

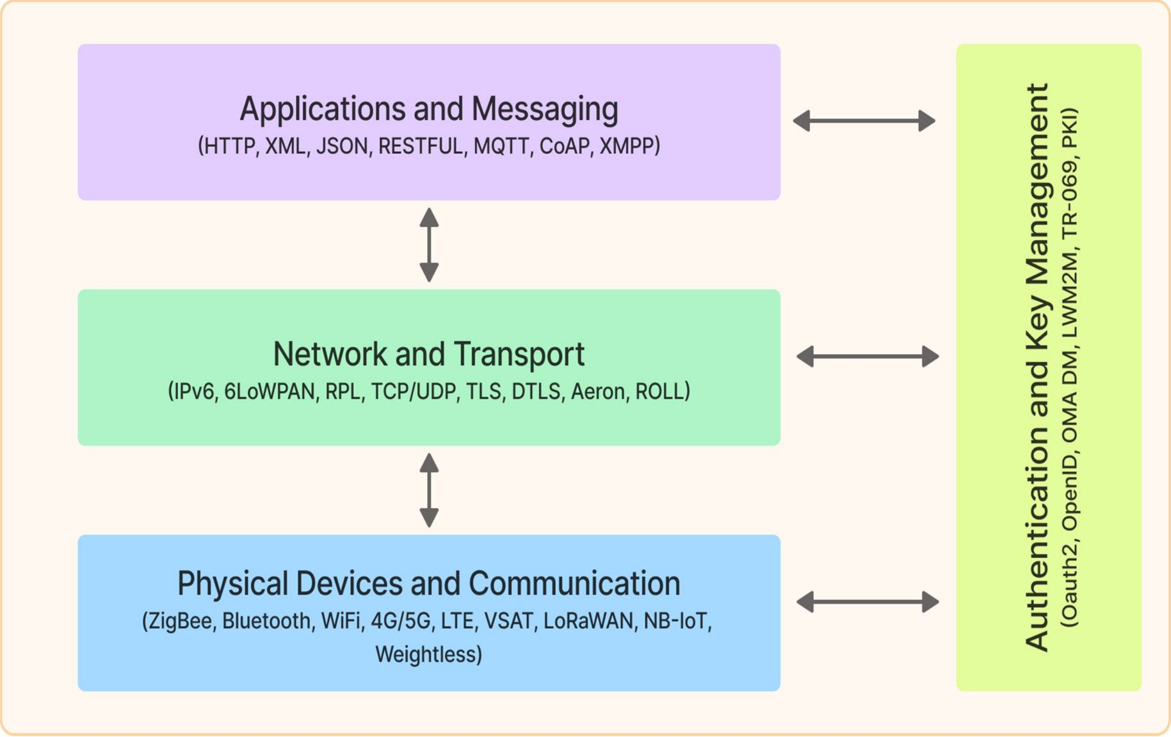
Applications and Messaging
(HTTP, XML, JSON, RESTFUL, MQTT, CoAP, XMPP)
Network and Transport
(IPv6, 6LoWPAN, RPL, TCP/UDP, TLS, DTLS, Aeron, ROLL)
Physical Devices and Communication
(ZigBee, Bluetooth, WiFi, 4G/5G, LTE, VSAT, LoRaWAN, NB-IoT, Weightless)
Authentication and Key Management
(Oauth2, OpenID, OMA DM, LWM2M, TR-069, PKI)

Figure 3: Common IoT standards and protocols.

IV. COMMON ISSUES AND CHALLENGES OF IOT

IoT-focused systems have brought users huge benefits and affected all aspects of human life; however, there are threats associated with them. The various technologies used to communicate data between the networked devices raised complications and led to the emergence of several issues and challenges. Due to advancements in the IT sector, the demand for a superior IoT system is also increasing, which is raising their overall threat.

Cybersecurity, privacy, and security threats are the fundamental considerations of security specialists and researchers, as stated. These challenges are causing substantial difficulties for corporate as well as government sectors. Increased breaches in these systems have indicated the dangers of IoT systems [1]. Apart from the challenges posed to IoT users, they are equally challenging for IoT engineers in the sophisticated IT society.

Consequently, IoT experts constantly need to check for new problems that could arise with IoT devices and provide solutions for them [5].

It is disappointing that IoT consumers rarely see the consequences until an attack has occurred, incurring huge losses like sensitive data theft. Indeed, the lack of a clear understanding of the challenges and their potential solutions led to uncertainty about the success of the technology while intimidating the privacy of its users. This section focuses on explaining a few of the challenges associated with IoT devices that need emphasis for their successful and optimized performance.

A. Cybersecurity

Cybersecurity is considered a crucial aspect concerning the complete adoption of IoT in the real world [13]. The interconnectivity of diversified IoT systems brings several threats and possible challenges. Undoubtedly, safeguarding IoT devices raises the duty of security officials while providing security provisioning facilities to the billions of interconnected IoT devices. The rising number of issues encountered with IoT technologies is causing an urgent need to address cybersecurity threats to improve the future of IoT. As demonstrated by the authors in Figure 4 [8], the challenges associated with IoT devices range from traffic sniffing, spoofing, code injections, manipulation of sensitive information, unauthorized access, etc. As these threats might encounter in varied IoT objects in different locations, it is mandatory to give importance to cybersecurity.

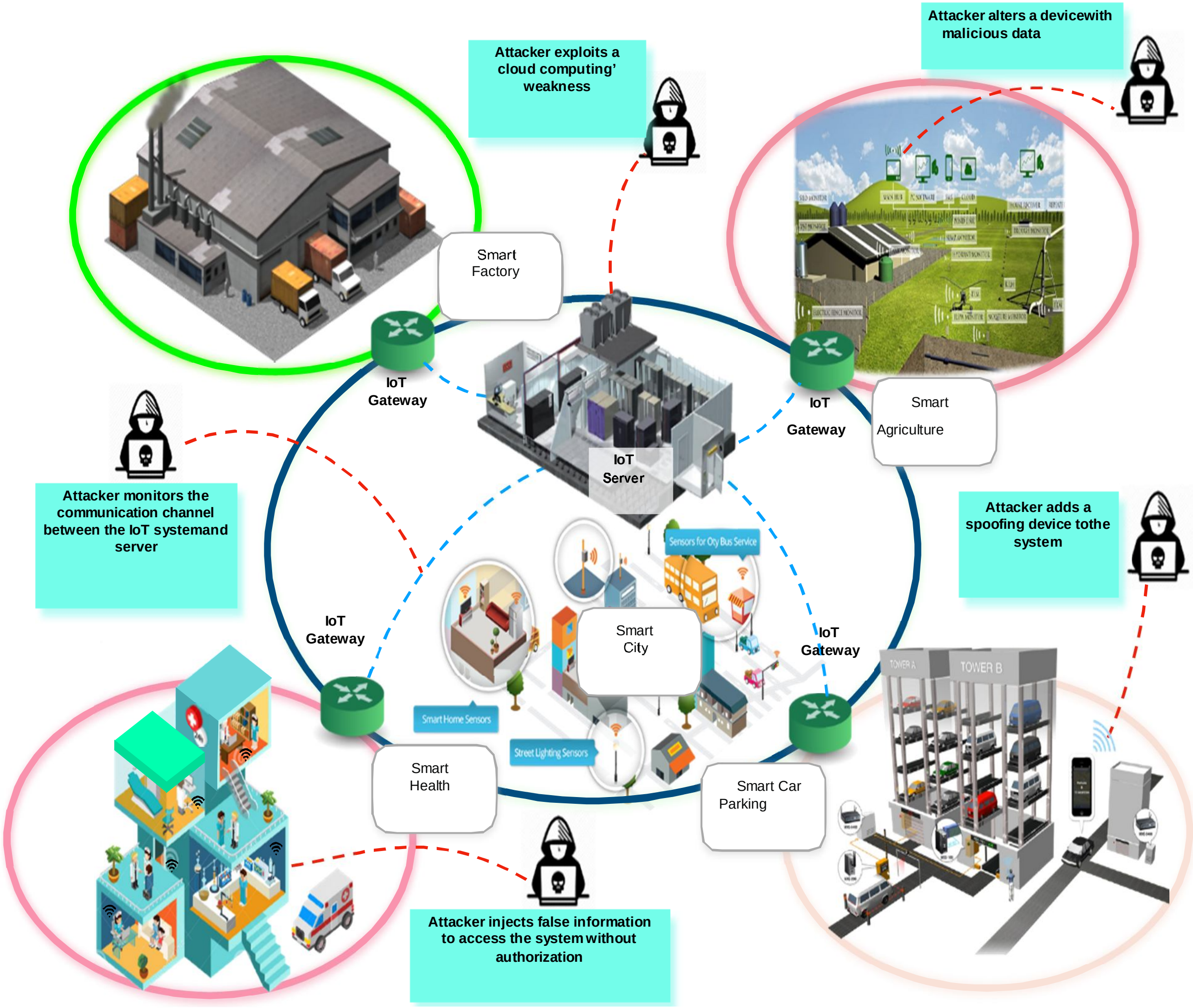
Attacker exploits a cloud computing' weakness
Attacker alters a devicewith malicious data
Smart Factory
IoT Gateway
IoT Gateway
Smart Agriculture
IoT Server
Attacker monitors the communication channel between the IoT systemand server
Attacker adds a spoofing device tothe system
Sensors for City Bus Service
IoT Gateway
Smart City
IoT Gateway
TOWER A
TOWER B
Smart Home Sensors
Street Lighting Sensors
Smart Health
Smart Car Parking
Attacker injects false information to access the system without authorization

Figure 4: Potential security challenges for the IoT ecosystem

The researchers in [10] described that the development and operation of IoT systems should adhere to a unified security and safety features model as they are used to interact with the physical environment to perform vital tasks. IoT cybersecurity is a complex issue inherent to the IoT that is aggravated by the numerous intercommunications of data between IoT systems. Since these objects are exposed vulnerably to the Internet, it exposes them to new threats and unknown vulnerabilities [22]. Further issues prevalent in the IoT platform focus on the lack of awareness about the fundamental components of cybersecurity: security methods, assets, issues, vulnerabilities, security features, etc. Due to a lack of knowledge, users are unaware that different IoT systems need distinct security procedures to prevent breaches in the real and virtual worlds. Alternatively, a corrupted IoT device may be considered an access point to get users' personal data, which leads to the violation of two of the security mechanisms: confidentiality and integrity [8]. Therefore, IoT cybersecurity is crucial, impacting the integration of IoT in multiple sectors.

B. Security

The failure of IoT devices can have deteriorating effects on the IoT ecosystem. Accordingly, the research and study on their security issues are significant. The primary objective of IoT device security is to maintain the privacy and confidentiality of the users while ensuring them a secured infrastructure with protected data and guaranteeing access to the facilities existing in an IoT infrastructure [10]. Therefore, research in IoT security has lately received great interest due to the existence of modelers, simulation tools, and computational and analysis tools.

For a secure IoT integration, a published study executed by researchers in [11, 13, 23–29] analyzed various security requirements that summarize in the table below:

Requirements	Explanation	References
Authenticy	Only legally authenticated users should be permitted access to the system or its content. The complexity of IoT authentication methods exists primarily due to the diverse architectures and devices in the IoT infrastructure.	[11, 13, 23]
Authorization	The components of the device and permission of the applications must be restricted so they can use just the assets they require to execute their respective activities.	[11, 24]
Confidentiality	The data transmitted between objects need protection from attackers. As IoT data moves across numerous loops in a system, an appropriate encryption technique is essential to maintaining the confidentiality of information.	[11, 13, 25]
Integrity	The IoT systems exposed to threats may lead a hacker to affect the integrity of data by altering the stored information for harmful objectives. Hence, the associated data should not be tampered.	[11, 13, 26]
Availability of Services	To prevent any possible operational disruptions and failures, the accessibility and durability of security services should be assured. The threats to IoT systems can delay the execution of operations via standardized denial-of-service cyberattacks. Several tactics, including jamming adversaries, sinkhole attempts, or replay attacks, affect IoT systems at multiple stages to damage the quality of service (QoS) delivered to IoT consumers.	[11, 13, 27]
Energy Efficiency	IoT systems are often resource-bound and have low power and storage. The threats to IoT ecosystems can escalate energy usage by overloading the network and exhausting IoT resources with duplicate or fake service requests.	[11, 13]
Single Points of Failure	The constant development of heterogeneous networks in the IoT ecosystem exposes several single points of failure that may worsen the intended operations of the IoT. It requires the establishment of a tamper-proof infrastructure for a significant number of IoT systems as well as the offering of alternative techniques for the installation of a fault-tolerant network.	[11, 13]

Table 1. Security requirements.

As the IoT ecosystem encloses a broad range of systems and devices that vary from small integrated chips to massive servers, security concerns need addressing at multiple stages. The IoT security issue taxonomy demonstrated by the researchers [13] is illustrated in Figure 5. It includes the different levels of security issues with publication references connected to each issue.

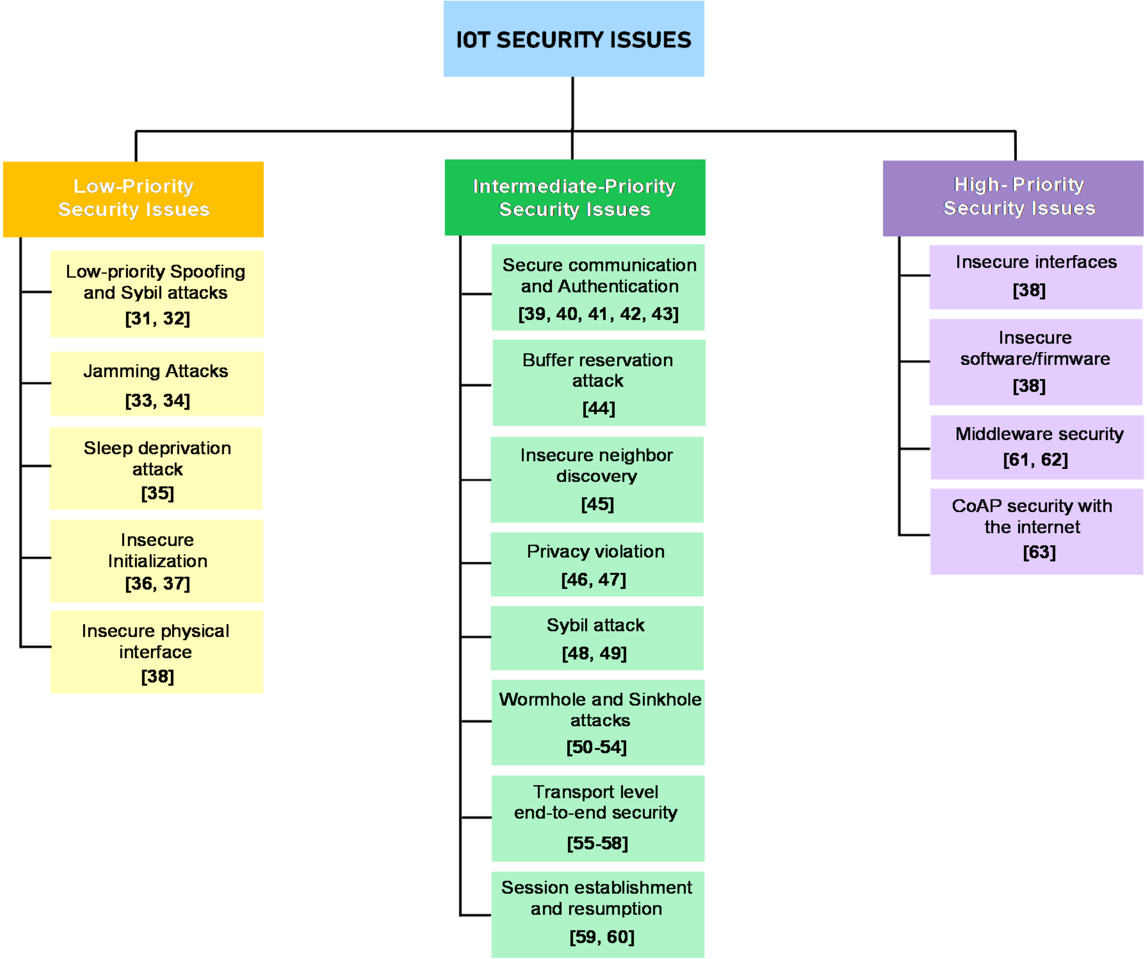
IOT SECURITY ISSUES
Low-Priority Security Issues
Low-priority Spoofing and Sybil attacks [31, 32]
Jamming Attacks [33, 34]
Sleep deprivation attack [35]
Insecure Initialization [36, 37]
Insecure physical interface [38]
Intermediate-Priority Security Issues
Secure communication and Authentication [39, 40, 41, 42, 43]
Buffer reservation attack [44]
Insecure neighbor discovery [45]
Privacy violation [46, 47]
Sybil attack [48, 49]
Wormhole and Sinkhole attacks [50-54]
Transport level end-to-end security [55-58]
Session establishment and resumption [59, 60]
High- Priority Security Issues
Insecure interfaces [38]
Insecure software/firmware [38]
Middleware security [61, 62]
CoAP security with the internet [63]

Figure 5. A taxonomy of IoT security issues along with their publications

The three categories of security threats for the successful adoption of IoT architecture are described below:

1) *Low-priority Security Threats*

The focal point of security is related to the hardware-level security challenges experienced at the data link and physical layers. Each of them is explained below:

a) *Low-priority Spoofing and Sybil Attacks:* The Sybil threats within an IoT ecosystem get triggered by hostile Sybil networks, which create falsified identities to deteriorate the performance of IoT systems. On the physical layer, a Sybil network uses randomly created MAC codes to masquerade as a known node to exhaust the network resources [31, 32]. Hence, the legitimate nodes in the network can be denied access to the available resources.

b) *Jamming Attacks:* The objective of jamming attacks is to disrupt IoT wireless systems by releasing radio frequency signals without maintaining a predefined protocol. This radio congestion substantially affects network functioning and the transmitting and receiving of information by registered networks, leading to malfunction or unexpected system performance [33, 34].

c) *Sleep Deprivation Attack:* Sleep deprivation attack: The energy-bound IoT objects are susceptible to these attacks by inducing the sensors to remain awake all the time, which results in the exhaustion of the battery as numerous tasks are set for execution in the 6LoWPAN environment [35].

d) *Insecure Initialization:* A reliable technique of setting and installing IoT at the physical layer guarantees the proper functioning of the entire system without compromising network and privacy services [36, 37]. The physical communication layer also has to be protected to make it inaccessible to unwanted users.

e) *Insecure Physical Interface:* Various physical elements lead to critical issues for the efficient operation of IoT devices. Software access via physical interfaces, inadequate physical security, and exploitation of testing and debugging tools may disrupt the IoT network [38].

2) *Medium-prioirty Security Issues*

The intermediate-grade security challenges focus on data transmission, routing, and session management at the transport and network layers of the IoT, as mentioned below:

a) *Secure Communication and Authentication:* The components and end-users in the IoT ecosystem must authenticate using key management systems. Any gap in security at the network layer or the broad range of safeguarding transmission may expose the system to dangers [39, 40, 41]. For example, owing to limited resources, the functionality of Datagram Transport Level Security (DTLS) has to be reduced, and the cryptographic methods ensuring a secure IoT data connection must ensure the efficiency and scarcity of other resources [42, 43].

b) *Buffer Reservation Attack:* As a recipient object needs to preserve a buffer memory to recombine incoming data packets, an intruder may harm it by transmitting partial data fragments. This results in denial-of-service as other data packets drop owing to the space consumed by incomplete packets delivered by the attacker [44].

c) *Insecure Neighbour Discovery:* The IoT integration infrastructure requires the unique identification of every object in the system. The message transmission for recognition should be secure to ensure that the transferred information in the end-to-end communication reaches the desired destination. The neighbor discovery phase before data communication executes several actions, like router detection and address determination. The neighbor identification packets' implementation without sufficient validation might have severe consequences in addition to denial-of-service [45].

d) *Privacy Violation:* In the IoT cloud-based system, various attacks may challenge identity, and location privacy may be leaked to the cloud or postpone network-bound IoT [46, 47]. Likewise, a compromised cloud service provider in an IoT-deployed system may retrieve sensitive data transmitted to the preferred destination.

e) *Sybil Attack:* Equivalent to the Sybil attacks on low-prioritized layers, the integrated Sybil networks may damage the system's operation and potentially threaten data privacy. The transmission by Sybil endpoints using false identities may result in phishing attacks, spamming, and the dissemination of malware [48, 49].

f) *Wormhole and Sinkhole Attacks:* With the sinkhole breaches, the attacker endpoint reacts to the navigation requests, thereby causing the fragments to travel via the malicious nodes while creating malicious behavior on the system [50, 51]. The threats within the network may further deteriorate the functionalities of 6LoWPAN owing to wormhole attacks, where a bridge is built through the two endpoints such that packets coming at one endpoint approach other points instantly [52, 53, 54]. These attacks have severe consequences like denial of service, eavesdropping, and privacy violations.

g) *Transport level end-to-end Security:* It aims to deliver a security mechanism where the information from the source node is securely collected by the expected receiver port [55, 56]. It needs a comprehensive authentication mechanism that guarantees safe message communication in an encoded format without compromising privacy while functioning with low overhead [57, 58].

h) *Session Establishment and Resumption:* The session hijacking on the transport layer with falsified messages might cause denial of service [59, 60]. An attacker endpoint may imitate the target endpoint to preserve the session between two networks. The transferring networks might also require the re-transmission of data by modifying the sequence numbers.

3) *High-priority Security Issues*

The high-grade security challenges are mostly linked to the applications running in the IoT environment, as mentioned below.

a) *Insecure Interfaces:* For retrieving IoT functions, the endpoints used via the internet, smartphones, and the cloud are vulnerable to various threats that may adversely impact data privacy [38].

b) *Insecure Software/firmware:* Several risks in IoT include those generated by misconfigured software/firmware [38]. Coding using programming languages such as XML, XSS, JSON, and SQLi demands proper testing. Additionally, the software/firmware upgrades require secure execution.

c) *Middleware Security:* The IoT middleware developed to permit communication between heterogeneous components of the IoT infrastructure must be safe enough to provide services. The interfaces and environments employing middleware require incorporation to offer secure interaction [61, 62].

d) *CoAP Security with the Internet:* The Constrained Application Protocol (CoAP) is a web transport protocol for devices that incorporate DTLS bindings alongside different security configurations to enable end-to-end protection. The CoAP signals adhere to a specific format outlined in RFC-7252 [63], which needs encryption for safe data delivery. Likewise, the multicast capability in CoAP requires adequate key management and authentication techniques.

C. Privacy

As the IoT network grows continuously, adding billions of new sensors and devices to the infrastructure, rendering enormous user data, consisting of their conversations, transactions, locations, pictures, videos, voice notes, connections, shopping records, health records, etc., with or without their permission. This massive amount of data makes privacy maintenance challenging. [64, 70].

Privacy is a concept linked with four primary segments: data, communications, body, and environment. Data privacy is concerned with collecting and processing personal information by an organization, like medical and financial data. Communication privacy is related to protecting information transmitted between two communicating endpoints using any transmission mode. Body privacy focuses on people's physical security alongside external damage, whereas environmental privacy involves developing limits on physical spaces such as workplaces, homes, and public places [65].

In the IoT ecosystem, safeguarding people's privacy has become unattainable due to the information collection process being more passive, pervasive, and less intrusive, leading to less awareness amongst the users of being tracked. The possible risk of losing access to personal data is known as a privacy threat which is considered as the key concern of users and has a significant impact on the adoption level of any new technology [66]. Given below are the common privacy threats existing in the IoT infrastructure:

1) *Profiling:* Profiling is the gathering and processing of users' information based on their performed activities and actions over time for the categorization of some features. This data is usually collected without the user's consent and merged with other data profiles to create a complete data report. Profiling has become common in domains like e-commerce, targeted advertising, credit scoring, etc [68]. The key threat of profiling is that confidential information may be disclosed to other users, as other users using the same system may access those data or view the targeted advertisement. Furthermore, most end-users are concerned by the sheer awareness of being observed and tracked. With the expansion of IoT systems, there is a significant increase in data collection due to the explosion of data sources and interconnected devices. Additionally, data changes exponentially as it is gathered from previously inaccessible parts of users' personal lives, like, information collected by smart watches or other smart systems in the environment [67].
2) *Identification:* The IoT architecture is made ubiquitous in nature to let devices track and gather user information and their interactions with the environment. Usually, these data are processed at service providers, which are located outside of users' control. Identification is the threat of relating an identifier (e.g., name, address) with private data about an individual. In the IoT, new technologies and interconnection of various techniques expand the threat of identification [67]. The use of a surveillance camera, in non-security contexts, is an example of such techniques, where customers' behaviour is studied for analysis and marketing. To address this issue, attribute-based authentication is recommended to minimize the data a device can collect in the IoT and maintain control over the disclosure of data.
3) *Tracking and Localization:* It is the threat of constantly monitoring a user's location through various modes like tracking via cell phone location, GPS data, internet traffic, etc [67]. The immense bulk of data and its wide geographical range has raised interest in using geographic data and performing structural information research. With the advancement of the IoT architecture, various approaches boosted the localization threats like the increase of location tracking applications, enhancement of their accurateness, the ubiquity of information gathering technology, and communication with IoT systems that record the identity, location, and movement of the user.
4) *Linkage:* Linkage risk indicates the inaccessible exposure of users' data by merging various data sources from different systems. Combining different types of user data exposes new facts to the traitor, considered a privacy breach [68]. In the IoT ecosystem, the linkage threat will rise due to the integration of different organizations that establish a more heterogeneous and distributed system which increases the system complexity and makes data collection operation negligibly evident [67].
5) *Life-cycle Transitions:* This kind of privacy risk implies exposure to confidential information where the owner of a product changes during its life cycle. These products bearing personal data of users gathered from various sources like smartphones, cameras, and laptops, under the control of the same owner don't cause many problems. However, as the activities increase and so does the private data, the risk for privacy disclosure due to the changed owner will rise [69].
6) *Inventory Attack:* Inventory attacks refer to the illegal collection of individual data regarding the existence and aspects of things in a targeted place. They usually can be performed with the fingerprint of IoT gadgets, for example, their communication speed, reaction time, etc. If IoT systems accomplish their promise, it unlocks the opportunity for unauthorized individuals to exploit and produce an inventory list of items belonging to a target. This can be used for profiling individuals since owning certain items discloses confidential information about the end user [67].

V. SOLUTIONS

A. Cybersecurity Solutions

There are multiple conventional security techniques and mechanisms to minimize specific cybersecurity challenges. Regardless, using IoT devices requires data collection from detectors like network ports, and continuous processing disregards these techniques. These aforesaid possible security challenges have a considerable influence on the IoT ecosystem. To cope with these vulnerabilities, the researchers [8] presented an ontology-based cybersecurity architecture to mitigate their underlying threats. According to the authors, this cybersecurity architecture is crucial for the successful performance of IoT devices in diverse sectors. The framework aims to provide an innovative strategy to enhance IoT cybersecurity in the industry by tracking, analyzing, and characterizing security challenges in a knowledge-based environment while allowing the resulting security service to adjust to the vulnerabilities. This would thereby enhance security features around business operations and technology resources.

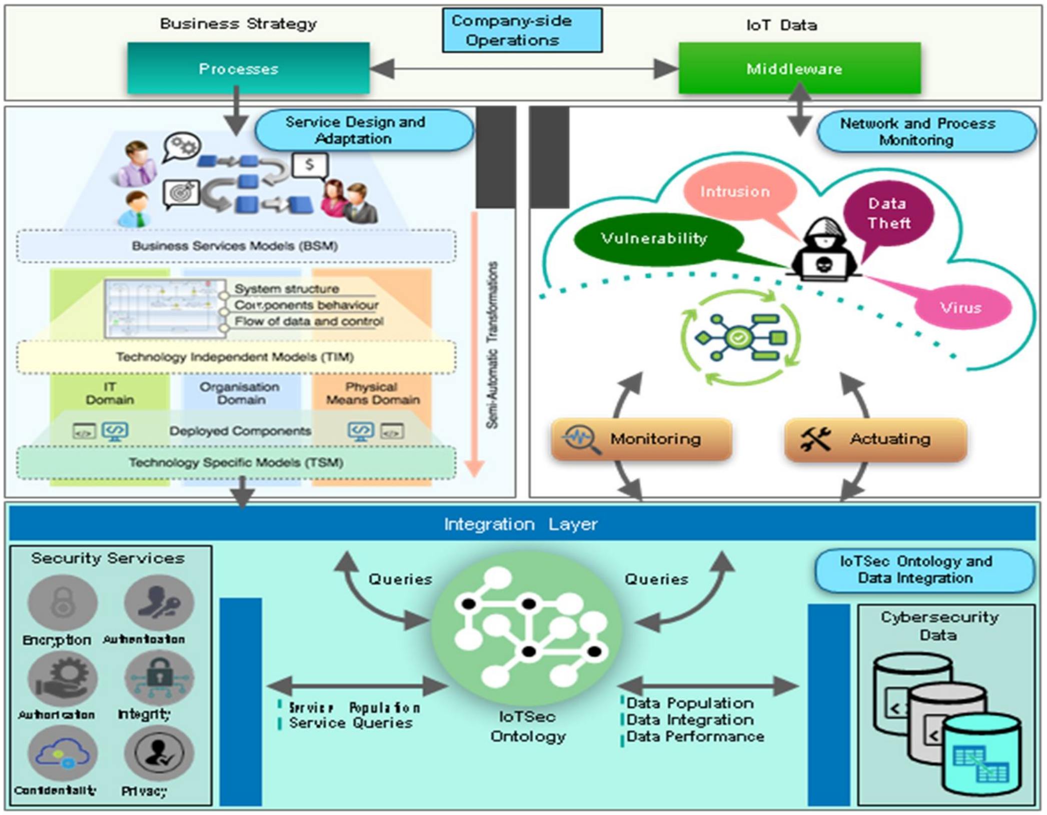

Figure 6. The proposed ontology-based cybersecurity architecture.

For the proper implementation, precise identification of the security-related capabilities of IoT systems is essential for accurate interconnection and intercommunication. For this, the authors separated the framework into three levels: design time, run time, and integration layer (Figure 6). In the design time layer (top-left section of the figure), the method anticipates the implementation of the MSDEA model-driven technique to develop and adjust the current security services partially while using the existing advanced abstraction security service blueprints to build the tech-based elements. In the run-time layer (top-right section of the figure), system and operation tracking techniques gather security warnings from numerous cybersecurity devices, recognizing and organizing them into different categories of importance (e.g., risks and vulnerabilities). Using this knowledge-based standardized by the IoTSec ontology for reasoning mechanisms (integration layer, bottom section of the figure), the taxonomy may recommend appropriate security services that might be stated or not at the design phase for modifying and operating inside IoT networks.

Since industry-based operations involve several enterprise-based processes that depend on data collection and communication between IoT sensors and gadgets, these procedures strive to execute simultaneous activities to fulfill goals set by the organization in its business strategy. The cybersecurity approach combines the IoTSec taxonomy and incorporates information from diverse data locations into a knowledge base. This component offers data incorporation and generation from the taxonomy data and access to numerous security services concerning many business operations and network nodes, including specifications assuring security measures against attacks.

B. Security Solutions

The security challenges imposed in the IoT infrastructure add risk to several components, including network components, applications and interfaces, firmware, software, and hardware objects. In an IoT network, users communicate with these objects through protocols that may detach from security mechanisms. The solutions for security concerns specify the hazards of this communication at various tiers to attain a specific security level. The numerous protocols facilitating the integration of features add to the complexity of these countermeasures.

The overview of the primary security solutions to security threats at different levels is summarized in Table 2. It involves a comparison assessment considering the characteristics of issues, their complexity, involved layers, and potential solutions.

#	Security level	Security Issue	Challenges	Affected Layer	Proposed Solutions	References
1.	Low Priority	Low-level Sybil and spoofing attacks	• Network Disruption • Denial-of-service	Physical layer	❖ Signal strength measurements ❖ Channel estimation	[31, 32, 71, 72, 73]
2.		Jamming Attacks	• Disruption • Denial-of-service		❖ Measuring signal strength ❖ computing packet delivery ratio ❖ modification of frequencies and locations ❖ encoding packets with error fixing scripts	[34, 36, 74]
3.		Insecure Initialization	• Privacy violation • Denial-of-service		❖ Setting data transmission rates b/w nodes ❖ Introducing artificial noise	[36, 37, 75]
4.		Sleep deprivation attack	• Energy consumption	Link layer	❖ Multi-layer-based intrusion detection system	[35]
5.		Insecure physical interface	• Privacy violation • Denial-of-service	Hardware layer	❖ Avoiding software/firmware access to USB ❖ Hardware based TPM modules ❖ Avoiding testing/debugging tools	[38]
6.	Intermediate level	Authentication and secure communication	• Privacy violation	6LoWPAN adaptation layer Transport layer Network layer	❖ Compressed AH and ESP ❖ Header compression and software-based AES, TPM using RSA, SHA1/AES ❖ Hybrid authentication ❖ Authentication with fuzzy extractor	[39, 40, 41, 42, 43, 46, 47, 76, 77, 78, 79, 80, 81]

					❖ Encryption of payload dispatch type values with compressed AH ❖ IACAC using the Elliptic Curve Cryptography ❖ Distributed logs ❖ Symmetric homomorphic mapping	
7.		Buffer reservation attack	• Blocking of reassembly buffer	6LoWPAN adaptation layer, and network layer	❖ Split buffer approach requiring complete transmission of fragments	[44]
8.		Insecure neighbour discovery	• IP Spoofing	Network layer	❖ Authentication using Elliptic Curve Cryptography (ECC) based signatures	[45]
10.		Sybil attack	• Privacy violation • Spamming • Byzantine faults • Unreliable broadcast	Network layer	❖ Random walk on social graphs ❖ Analysing user behaviour ❖ Maintaining lists of trusted/un-trusted users	[48, 49, 82, 83, 84, 85]
11.		Sinkhole and wormhole attacks	• Denial-of-service	Network layer	❖ Rank verification through hash chain function ❖ Trust level management ❖ Nodes/communication behaviour analysis ❖ Anomaly detection through IDS ❖ Cryptographic key management ❖ Graph traversals ❖ Measuring signal strength	[50, 51, 52, 53, 54, 86, 87, 88, 89, 90, 91, 92, 93, 94]
12.		Transport level end-to-end security	• Privacy violation	Transport layer, and network layer	❖ DTLS-PSK with nonces ❖ 6LoWPAN Border Router with ECC ❖ DTLS cipher based on AES/SHA algorithms ❖ Compressed IPSEC ❖ DTLS header compression	[55, 56, 57, 58, 76, 95, 96, 97, 98, 99]

					❖ IKEv2 using compressed UDP ❖ AES/CCM based security with identification and authorization	
13.		Session establishment and resumption	• Denial-of-service	Transport layer	❖ Authentication with long-lived secret key ❖ Symmetric key-based encryption	[59, 60, 100]
14.	High-level and Intermediate level	Middleware security	• Privacy violation • Denial-of-service • Network disruption	Application layer, transport layer, and network layer	❖ Secure communication using authentication ❖ Security policies ❖ Key management between devices ❖ Gateways & M2M components ❖ Service layer M2M security ❖ Transparent middleware using authentication/encryption mechanisms	[61, 62, 101, 102, 103]
15.		Insecure software/firmware	• Privacy violation • Denial-of-service • Network disruption	Application layer, transport layer, and network layer	❖ Regular secure updates of software/firmware ❖ Use of file signatures ❖ Encryption with validation	[38]
16.		CoAP security with the Internet	• Network bottleneck • Denial-of-service	Application layer, and network layer	❖ TLS/DTLS and HTTP/CoAP mapping ❖ Mirror Proxy (MP) and Resource Directory ❖ TLS-DTLS tunnel and message filtration using 6LBR	[104, 105, 106, 107]
17.	High Level	Insecure interfaces	• Privacy violation • Denial-of-service • Network disruption	Application layer	❖ Disallowing weak passwords ❖ Testing the interface against the vulnerabilities of software tools (SQLi and XSS) ❖ Using https along with firewalls	[38]

Table 2. Security solutions to security threats at different levels

C. Privacy Solutions

Maintaining the privacy of IoT systems is crucial for their successful development and functioning. Hence, several approaches have been suggested by researchers in [70, 108-110] to maintain their privacy. Listed below are a few techniques for handling privacy threats in the IoT ecosystem:

#	Technique	Explanation	References
1	Data Anonymization	The deletion of unique identifiers like phone numbers, driving license numbers, etc., from databases to remove the person's identity.	[70]
2	Cryptographic Techniques	Using appropriate cryptography techniques to encrypt information in IoT devices with minimal storage and processing resources [45].	[108]
3	Data Minimization	Integrating data minimization by IoT service providers to limit the collection of personal data to only when necessary for service [44].	[109]
4	Access Control	Establishing a reliable access control mechanism for the IoT infrastructure to allow IoT devices to provide the best solutions.	[70]
5	Privacy Awareness	The lack of public awareness is one of the key problems with privacy violations. IoT customers need to know the different types of privacy threats to stay protected [43].	[110]

Table 3. Techniques for handling privacy threats

VI. CONCLUSION

IoT devices can connect and interact with practically all real-world entities over the Internet to increase information exchange. These IoT-based systems have brought users huge benefits and affected all aspects of human life. In addition to being considered the most emerging technology, it has drawn significant developers and researchers from various parts of the world, making significant contributions to resolve multiple critical IoT issues. Yet, this field still needs attention, as threats like cybersecurity, security, and privacy still require a more advanced survey and evaluation. This paper has covered a complete insight into different challenges associated with IoT systems concerning cybersecurity, security, and privacy, along with their necessary solutions.

The survey on cybersecurity involves a parametric study of cyberattacks in IoT and the potential solution with the cybersecurity framework. The research on security issues categorizes them based on priority from low to high and includes techniques for maintaining IoT security at different levels. Analyzed potential solutions are provided in relation to the implications of these security attacks. Finally, the paper explores typical privacy issues in IoT systems and the solutions for safeguarding privacy. The paper identifies and mentions open research concerns that need the attention of researchers to offer safe, robust, and accessible IoT systems to end users.

REFERENCES

[1] Tawalbeh, Loai & Muheidat, Fadi & Tawalbeh, Mais & Quwaider, Muhannad. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences. 10. 4102. 10.3390/app10124102.

[2] Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.

[3] Presser M, Krco Sa. IOT-I: Internet of Things Initiative: Public Deliverables – D2.1: Initial report on IoT applications of strategic interest 2010.

[4] Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks 2010; 54(15):2787 – 2805, doi: 10.1016/j.comnet.2010.05.010.

[5] Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019). https://doi.org/10.1186/s40537-019-0268-2

[6] Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges." Security and Communication Networks 7.12 (2014): 2728-2742.

[7] Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe,W. A security framework for the Internet of things in the future internet architecture. Future Internet 2017, 9, 27. https://www.mdpi.com/1999-5903/9/3/27

[8] Mozzaquatro, Bruno & Agostinho, Carlos & Goncalves, Diogo & Martins, João & Jardim-Goncalves, Ricardo. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors. 18. 3053. 10.3390/s18093053.

[9] Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.

[10] Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.

[11] Leloglu, E.A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136. https://www.scirp.org/journal/paperinformation.aspx?paperid=73675

[12] Izzat, A.; Chuck, E.; Lo'ai, T. The NICE Cyber Security Framework, Cyber Security Management; Springer: Basel, Switzerland, 2020; ISBN 978-3-030-41987-5.

[13] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765?via%3Dihub

[14] Atlam, Hany & Wills, Gary. (2019). IoT Security, Privacy, Safety and Ethics. 10.1007/978-3-030-18732-3_8.

[15] Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of Internet of things. In Proceedings of the 3rd IEEE international conference on advanced computer theory and engineering, China.

[16] Chowdhury, S. N., Kuhikar, S. M., & Dhawan, S. (2015). IoT architecture: A survey. Journal of Industrial Electronics and Electrical Engineering, 3(5), 88–92.

[17] Sethi, P., & Sarang, S. R. (2017). Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 17, 1–25.

[18] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[19] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[20] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[21] Mahmoud, Rwan & Yousuf, Tasneem & Aloul, Fadi & Zualkernan, Imran. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. 336-341. 10.1109/ICITST.2015.7412116.

[22] Wolf, M.; Serpanos, D. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. Proc. IEEE 2018, 106, 9–20. https://ieeexplore.ieee.org/document/8232537

[23] Huang, X., Craig, P., Lin, H. and Yan, Z. (2015) SecIoT: A Security Framework for the Internet of Things. Security and Communication Networks, 9, 3083-3094. https://doi.org/10.1002/sec.1259

[24] Wind River Systems (2015) Security in the Internet of Things. http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[25] Suo, H., Wan, J., Zou, C. and Liu, J. (2012) Security in the Internet of Things: A Review. IEEE International Conference on Computer Science and Electronics Engineering, Hangzhou, 23-25 March 2012, 648-651. https://doi.org/10.1109/ICCSEE.2012.373

[26] Nguyen, K.T., Laurent, M. and Oualha, N. (2015) Survey on Secure Communication Protocols for the Internet of Things. Ad Hoc Networks, 32, 17-31. https://doi.org/10.1016/j.adhoc.2015.01.006

[27] European Commission. IoT Privacy, Data Protection, Information Security. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

[28] Farooq, M.U., Waseem, M., Khairi, A. and Mazhar, S. (2015) A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111, 1-6. https://doi.org/10.5120/19547-1280

[29] Chen, M., Wan, J.F. and Li, F. (2012) Machine-to-Machine Communications: Architectures, Standards and Applications. KSII Transactions on Internet and Information Systems, 6, 480-497.

[30] Mardiana binti Mohamad Noor, Wan Haslina Hassan, Current research on Internet of Things (IoT) security: A survey, Computer Networks, Volume 148, 2019, Pages 283-294, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2018.11.025

[31] L. Xiao, L. J. Greenstein, N. B. Mandayam, W. Trappe, Channel-based detection of sybil attacks in wireless networks, IEEE Transactions on Information Forensics and Security 4 (3) (2009) 492–503.

[32] Y. Chen, W. Trappe, R. P. Martin, Detecting and localizing wireless spoofing attacks, in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007, pp.193–202.

[33] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. doi:10.1145/1062689.1062697. URL http://doi.acm.org/10.1145/1062689.1062697

[34] G. Noubir, G. Lin, Low-power dos attacks in data wireless lans and countermeasures, SIGMOBILEMob. Comput. Commun. Rev. 7 (3) (2003) 29–30.

[35] T. Bhattasali, R. Chaki, A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280.

[36] S. H. Chae, W. Choi, J. H. Lee, T. Q. S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. For. Sec. 9 (10) (2014) 1617–1628. doi:10.1109/TIFS.2014.2341453. URL http://dx.doi.org/10.1109/TIFS.2014.2341453

[37] Y.-W. P. Hong, P.-C. Lan, C.-C. J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Processing Magazine 30 (5) (2013) 29–40.

[38] OWASP, Top iot vulnerabilities (May 2016). URL https://www.owasp.org/index.php/ Top IoT Vulnerabilities

[39] J. Granjal, E. Monteiro, J. S. Silva, Network-layer security for the Internet of things using tinyos and blip, International Journal of Communication Systems 27 (10) (2014) 1938–1963. doi:10.1002/dac.2444. URL http://dx.doi.org/10.1002/dac.2444

[40] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6lowpan with compressed ipsec, in: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–8. doi:10.1109/DCOSS.2011.5982177.

[41] J. Granjal, E. Monteiro, J. S. Silva, Enabling network-layer security on ipv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6. doi:10.1109/GLOCOM.2010.5684293.

[42] P. N.Mahalle, B. Anggorojati, N. R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the Internet of things, Journal of Cyber Security and Mobility 1 (4) (2013) 309–348.

[43] D. U. Sinthan, M.-S. Balamurugan, Identity authentication and capability based access control (iacac) for the Internet of things, Journal of Cyber Security and Mobility 1 (4) (2013) 309–348.

[44] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6lowpan fragmentation attacks and mitigation mechanisms, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, ACM, New York, NY, USA, 2013, pp. 55–66. doi:10.1145/2462096.2462107. URL http://doi.acm.org/10.1145/2462096.2462107

[45] R. Riaz, K.-H. Kim, H. F. Ahmed, Security analysis survey and framework design for ip connected lowpans, in: 2009 International Symposium on Autonomous Decentralized Systems, 2009, pp. 1–6. doi:10.1109/ISADS.2009.5207373.

[46] J. Zhou, Z. Cao, X. Dong, A. V. Vasilakos, Security and privacy for cloud-based iot: Challenges, IEEE Communications Magazine 55 (1) (2017) 26–33. doi:10.1109/MCOM.2017.1600363CM.

[47] [M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, K. Wehrle, Distributed configuration, authorization and management in the cloud-based Internet of things, in: 2017 IEEE Trustcom/BigDataSE/ICESS, 2017, pp. 185–192doi:10.1109/Trustcom/BigDataSE/ICESS.2017.236

[48] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the Internet of things, IEEE Internet of Things Journal 1 (5) (2014) 372–383. doi:10.1109/JIOT.2014.2344013.

[49] G.Wang, M. Mohanlal, C.Wilson, X.Wang, M. Metzger, H. Zheng, B. Y. Zhao, Social turing tests: Crowdsourcing sybil detection, in: In Symposium on Network and Distributed System Security (NDSS), 2013.

[50] K. Weekly, K. Pister, aluating sinkhole defense techniques in rpl networks, in: Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP), ICNP '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 1–6. doi:10.1109/ICNP.2012.6459948. URL http://dx.doi.org/10.1109/ICNP.2012.6459948

[51] F. Ahmed, Y.-B. Ko, Mitigation of black hole attacks in routing protocol for low power and lossy networks, Security and Communication Networks 9 (18) (2016) 5143–5154, sCN-16-0443.R1.

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

[53] W. Wang, J. Kong, B. Bhargava, M. Gerla, Visualisation of wormholes in underwater sensor networks&#58; a distributed approach, Int. J. Secur. Netw. 3 (1) (2008) 10–23.

[54] M. Wazid, A. K. Das, S. Kumari, M. K. Khan, Design of sinkhole node detection mechanism for hierarchical wireless sensor networks, Sec. and Commun. Netw. 9 (17) (2016) 4596–4614. doi:10.1002/sec.1652. URL https://doi.org/10.1002/sec.1652

[55] M. Brachmann, O. Garcia-Morchon, M. Kirsche, Security for practical coap applications: Issues and solution approaches, in: 10th GI/ITG KuVS Fachgespraech Sensornetze (FGSN 2011), 2011.

[56] 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.

[57] G. Peretti, V. Lakkundi, M. Zorzi, Blinktoscoap: An end-to-end security framework for the Internet of things, in: 2015 7th International Conference on Communication Systems and Networks (COMSNETS), 2015, pp. 1–6. doi:10.1109/COMSNETS.2015.7098708.

[58] 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.

[59] N. Park, N. Kang, Mutual authentication scheme in secure Internet of things technology for comfortable lifestyle, Sensors 6 (1) (2016) 20–20.

[60] M. H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, International Journal of Network Security 18 (6) (2016) 1089–1101.

[61] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M. A. Spirito, The virtus middleware: An xmpp based architecture for secure iot communications, in: 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–6. doi:10.1109/ICCCN.2012.6289309.

[62] C. H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in internet-of-things sensory environments, Ad Hoc Networks 18 (Supplement C) (2014) 85 – 101. doi: https://doi.org/10.1016/j.adhoc.2013.02.008 URL http://www.sciencedirect.com/science/article/pii/S1570870513000280

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

[64] Atlam, H.F., Walters, R.J., Wills, G.B.: Internet of nano things : security issues and applications. In: 2018 2nd International Conference on Cloud and Big Data Computing, no. October, pp. 71–77 (2018)

[65] Padilla-López, J.R., Chaaraoui, A.A., Flórez-Revuelta, F.: Visual privacy protection methods: A survey. Expert Syst. Appl. 42(9), 4177–4195 (2015)

[66] Atlam, H.F.,Alenezi,A., Alassafi, M.O.,Walters,R.J.,Wills, G.B.:XACMLfor building access control policies in Internet of things. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), pp. 253–260. (2018)

[67] Ziegeldorf, J.H., Morchon, O.G., Wehrle, K.: Privacy in the internet of things: Threats and challenges. Secur. Commun. Netwo. 7(12), 2728–2742 (2014)

[68] Toch,E.,Wang,Y.,Cranor,L.F.: Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Model. User-Adapted Interact. 22(1–2), 203–220 (2012)

[69] Aleisa,N., Renaud, K.: Privacy of the Internet of things: a systematic literature review(Extended Discussion). ArXiv e-prints, pp. 1–10 (2016)

[70] Atlam, Hany & Wills, Gary. (2019). IoT Security, Privacy, Safety and Ethics. 10.1007/978-3-030-18732-3_8

[71] M. Demirbas, Y. Song, An rssi-based scheme for sybil attack detection in wireless sensor networks, in: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06, IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. doi:10.1109/WOWMOM.2006.27 URL http://dx.doi.org/10.1109/WOWMOM.2006.27

[72] Q. Li, W. Trappe, Light-weight detection of spoofing attacks in wireless networks, in: 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2006, pp. 845–851.

[73] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Fingerprints in the ether: Using the physical layer for wireless authentication, in: 2007 IEEE International Conference on Communications, 2007, pp. 4646–4651 doi:10.1109/ICC.2007.767.

[74] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: Defenses against wireless denial of service, in: Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe '04, ACM, New York, NY, USA, 2004, pp. 80–89. doi:10.1145/1023646.1023661. URL http://doi.acm.org/10.1145/1023646.1023661

[75] T. Pecorella, L. Brilli, L. Muchhi, The role of physical layer security in iot: A novel perspective, Information 7 (3).

[76] S. Raza, T. Chung, S. Duquennoy, D. Yazar, T. Voigt, U. Roedig, Securing internet of things with lightweight ipsec, Tech. rep., Lncaster University, UK (February 2011). URL http://soda.swedishict.se/4052/2/reportRevised.pdf

[77] S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt, Secure communication for the Internet of things a comparison of link-layer security and ipsec for 6lowpan, Security and Communication Networks 7 (12) (2014) 2654–2668. doi:10.1002/sec.406.

[78] [96] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, A dtls based end-to-end security architecture for the Internet of things with two-way authentication,

in: 37th Annual IEEE Conference on Local Computer Networks -Workshops, 2012, pp. 956–963. doi:10.1109/LCNW.2012.6424088.

[79] X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu, Robust multi-factor authentication for fragile communications, IEEE Transactions on Dependable and Secure Computing 11 (6) (2014) 568–581. doi:10.1109/TDSC.2013.2297110.

[80] J. M. Bohli, A. Skarmeta, M. V. Moreno, D. Garca, P. Langendrfer, Smartie project: Secure iot data management for smart cities, in: 2015 International Conference on Recent Advances in Internet of Things (RIoT), 2015, pp. 1–6. doi:10.1109/RIOT.2015.7104906.

[81] I. Stojmenovic, S. Wen, X. Huang, H. Luan, An overview of fog computing and its security issues, Concurrency and Computation: Practice and Experience 28 (10) (2016) 2991–3005. doi:10.1002/cpe.3485. URL http://dx.doi.org/10.1002/cpe.3485

[82] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, A. Panconesi, Sok: The evolution of sybil defense via social networks, in: Proceedings of the 2013 IEEE Symposium on Security and Privacy, SP '13, IEEE Computer Society, Washington, DC, USA, 2013, pp. 382–396. doi:10.1109/SP.2013.33. URL http://dx.doi.org/10.1109/SP.2013.33

[83] Q. Cao, X. Yang, Sybilfence: Improving social-graph-based sybil defenses with user negative feedback, Tech. rep., Duke University, USA (March 2012). URL https://users.cs.duke.edu/ qiangcao/

[84] A. Mohaisen, N. Hopper, Y. Kim, Keep your friends close: Incorporating trust into social network-based sybil defenses, in: 2011 Proceedings IEEE INFOCOM, 2011, pp. 1943–1951. doi:10.1109/INFCOM.2011.5934998.

[85] D. Quercia, S. Hailes, Sybil attacks against mobile users: Friends and foes to the rescue, in: Proceedings of the 29th Conference on Information Communications, INFOCOM'10, IEEE Press, Piscataway, NJ, USA, 2010, pp. 336–340. URL http://dl.acm.org/citation.cfm?id=1833515.1833583

[86] Y.-C. Hu, A. Perrig, D. B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, Wireless Networks 11 (1) (2005) 21–38.

[87] I. Krontiris, T. Dimitriou, T. Giannetsos, M. Mpasoukos, Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 150–161.

[88] I. Raju, P. Parwekar, Detection of Sinkhole Attack in Wireless Sensor Network, Springer India, New Delhi, 2016, pp. 629–636.

[89] E. C. H. Ngai, J. Liu,M. R. Lyu, On the intruder detection for sinkhole attack in wireless sensor networks, in: 2006 IEEE International Conference on Communications, Vol. 8, 2006, pp. 3383–3389. doi:10.1109/ICC.2006.255595.

[90] R. Poovendran, L. Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks, Wirel. Netw. 13 (1) (2007) 27–59. doi:10.1007/s11276-006-3723-x. URL http://dx.doi.org/10.1007/s11276-006-3723-x

[91] S. A. Salehi, M. A. Razzaque, P. Naraei, A. Farrokhtala, Detection of sinkhole attack in wireless sensor networks, in: 2013 IEEE International Conference on Space Science and Communication (IconSpace), 2013, pp. 361–365. doi:10.1109/IconSpace.2013.6599496

[92] C. Tumrongwittayapak, R. Varakulsiripunth, Detecting sinkhole attacks in wireless sensor networks, in: 2009 ICCAS-SICE, 2009, pp. 1966–1971.

[93] J. Jang, T. Kwon, J. Song, A time-based key management protocol for wireless sensor networks, in: Proceedings of the 3rd International Conference on Information Security Practice and Experience, ISPEC'07, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 314–328.

[94] S. Sharmila, G. Umamaheswari, Detection of sinkhole attack in wireless sensor networks using message digest algorithms, in: 2011 International Conference on Process Automation, Control and Computing, 2011, pp. 1–6. doi:10.1109/PACC.2011.5978973

[95] S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt, Secure communication for the Internet of thingsa comparison of link-layer security and ipsec for 6lowpan, Security and Communication Networks 7 (12) (2014) 2654–2668. doi:10.1002/sec.406. URL http://dx.doi.org/10.1002/sec.406

[96] A. A. Chavan, M. K. Nighot, Secure coap using enhanced dtls for Internet of things, International Journal of Innovative Research in Computer and Communication Engineering 2 (12) (2014) 7601–7608.

[97] S. Raza, D. Trabalza, T. Voigt, 6lowpan compressed dtls for coap, in: 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, 2012, pp. 287–289. doi:10.1109/DCOSS.2012.55.

[98] H. C. Phls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. D. Rodriguez, T. Mouroutis, Rerum: Building a reliable iot upon privacy- and security- enabled smart objects, in: 2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2014, pp. 122–127. doi:10.1109/WCNCW.2014.6934872.

[99] BUTLER-Consortium, Butler smartlife – uBiquitous, secUre inTernet-of-things with Location and contExtawaReness (October 2014).

[100] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, K. Wehrle, Tailoring end-to-end ip security protocols to the Internet of things, in: 2013 21st IEEE International Conference on Network Protocols (ICNP), 2013, pp. 1–10. doi:10.1109/ICNP.2013.6733571.

[101] A. Gmez-Goiri, P. Ordua, J. Diego, D. L. de Ipia, Otsopack: Lightweight semantic framework for interoperable ambient intelligence applications, Computers in Human Behavior 30 (Supplement C) (2014) 460 – 467. doi:https://doi.org/10.1016/j.chb.2013.06.022. URL http://www.sciencedirect.com/science/article/pii/S0747563213002148

[102] OneM2M, Security solutions – OneM2M Technical Specification (August 2017). URL http://onem2m.org/technical/latest-drafts

[103] H. G. C. Ferreira, R. T. de Sousa, F. E. G. de Deus, E. D. Canedo, Proposal of a secure, deployable and transparent middleware for Internet of things, in: 2014 9th Iberian Conference on Information Systems and Technologies (CISTI), 2014, pp. 1–4. doi:10.1109/CISTI.2014.6877069.

[104] M. Brachmann, S. L. Keoh, O. G. Morchon, S. S. Kumar, End-to-end transport security in the ip-based Internet of things, in: 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–5. doi:10.1109/ICCCN.2012.6289292.

[105] J. Granjal, E. Monteiro, J. S. Silva, Application-layer security for the wot: extending coap to support end-to-end message security for internet-integrated sensing applications, in: International Conference onWired/Wireless Internet Communication, Springer Berlin Heidelberg, 2013, pp. 140–153.

[106] M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepy smart object networks, in: 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 964–972. doi:10.1109/LCNW.2012.6424089.

[107] 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, in: 2012 Workshop on Smart Object Security, in conjunction with IETF83, 2012, pp. 1–3.

[108] Atlam, H.F., Alenezi, A., Walters, R., Wills, G.B.: An overview of risk estimation techniques in risk-based access control for the Internet of things. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), pp. 254–260 (2017)

[109] Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D.: Twenty security considerations for cloud-supported Internet of things. IEEE Internet Things J. 3(3), 269–284 (2016)

[110] Atlam, H.F., Attiya, G., El-Fishawy, N.: Comparative study on CBIR based on color feature. Int. J. Comput. Appl. 78(16), 975–8887 (2013)