Comprehensive Analysis of IoT Security Concerns and Mitigation Strategies Based on the Influence of Current Trends

Bhavani Adikesavan[1], Vijayakumar Ponnusamy[1,*], Suad Suljović[2], Petar Pejić[2] and Nemanja Zdravković[2]

[1]*Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India*

[2]*Faculty of Information Technology, Belgrade Metropolitan University, Tadeuša Košćuška 63, 11000 Belgrade, Serbia*

Abstract

The Internet of Things (IoT) has many disadvantages despite the fact that it has made a vast array of applications possible in many facets of society. Security and privacy are two examples of these issues. IoT devices are more susceptible to security flaws and attacks. There are currently no viable security solutions for IoT devices and apps due to their size, power, memory, and other limitations, which is keeping the world from being securely connected. Going beyond traditional or standard approaches and integrating the IoT device's security features is a feasible way to solve this issue. As cutting-edge technologies like blockchain, fog/edge/cloud computing, machine learning, and quantum computing have been used, IoT networks now have more weak points. The protocols and standards for the next generation of IoT systems are enhanced by the IoT architecture employed in this study. A comparative examination of protocols, standards, and proposed security models is presented in accordance with the IoT security requirements. In order to protect the hardware, software, and data from different threats and attacks, this study emphasises the importance of consistency at the communication and data verification level. This survey work emphasises the need for methods that can be applied to various threat vectors and some mitigating measures. An outline of the key advancements in security research that will help IoT security expand is provided in this article. By incorporating the finest security measures for IoT-based goods, the research findings can benefit the IoT research community.

Keywords

Internet of Things (IoT), Security, Machine Learning, Blockchain

1. Introduction

We are blessed to be alive in such exciting, tumultuous times. Reality appears to be the norm as technology develops, and cognition becomes artificial [1]. Although new and imaginative technologies are always being developed, some of them remain more promising and grounded in actuality than others. IoT is not just one technology; rather, it is a group of interconnected technical developments that offer ways to link the digital and physical realms. Today's wireless technology is a necessary part of our daily lives. Wireless sensor networks (WSNs), WiFi, ZigBee, RFID, actuators, and other wireless sensor technologies are all used in the Internet of Things (IoT). Online real-world product identification is made possible by tagging technologies like NFC, RFID, and 2D barcode, are some examples. These wireless tagging methods are the core components of the Internet of Things [2]. All IoT concepts are built on a layered architecture. IoT architecture explains how each layer interacts with the underlying technology, services, and external objects. Security issues differ according to tier. IoT makes it possible to virtually depict and identify individual goods.

IoT is helping to solve problems that individuals and businesses face every day in a variety of smart

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia

[*] Corresponding author.

bhavania@srmist.edu.in (B. Adikesavan); vijayakp@srmist.edu.in (V. Ponnusamy); suad.suljovic@metropolitan.ac.rs (S. Suljović); petar.pejic@metropolitan.ac.rs (P. Pejić); nemanja.zdravkovic@metropolitan.ac.rs (N. Zdravković)

0000-0003-4312-3003 (B. Adikesavan); 000-0002-3929-8495 (V. Ponnusamy); 0000-0003-1822-3782 (S. Suljović); 0000-0003-4155-8038 (P. Pejić); 0000-0002-2631-6308 (N. Zdravković)

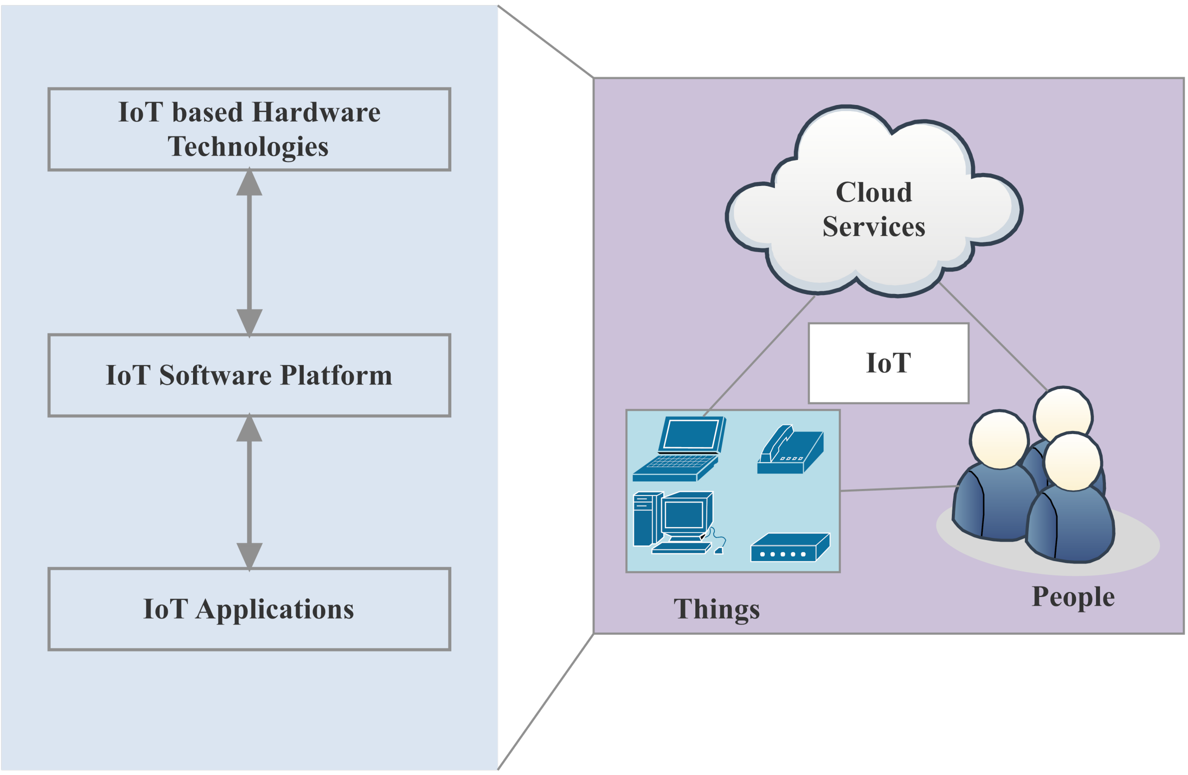

Figure 1: IoT Model with Cloud.

environments and technology sectors. Soon, the number of IoT participants will be greatly outnumbered by the number of participating items [3]. Technology advancement and new applications for corporate expansion have a favorable impact on the Internet of Things. Everyday items are linked to a network in the IoT, enabling a variety of applications in virtually every field, such as smart cities, smart healthcare models, smart agriculture, smart transportation, etc.

IoT has many applications in retail, transportation, medical care, administration, and other industries and is having an impact on almost every aspect of life. IoT will soon grow to be a big business as a result of the integration of people, things, locations, and processes [4]. Resources, energy, QoS, interoperability, interfaces, security, and privacy will all be handled by the IoT applications in the upcoming process. An extensive analysis of the literature on IoT application domains shows that more on-demand data is produced by queries as websites change from static to dynamic websites for social networks. Through short-range communication methods, data is exchanged in this varied environment. Figure 1 depicts the IoT model with the cloud.

The creation of this new technology, which boosts social efficiency, has unintended side effects regarding information security and privacy. This is due to the large amount of private and sensitive data that must be maintained cautiously and enhanced through security measures on the computer system. Important IoT issues include data protection, information security, and user privacy. IoT security issues are examined at the national level by authors in [5] due to the IoT's diverse uses, which include smart services. Establishing access control policies, protecting keys with hardware and software security mechanisms, including essential components in the design, and providing add-on capabilities are just a few of the responsibilities involved in IoT security. IoT, a pretty broad term, refers to the fact that most electronics will be connected in a few years rather than connecting people. In wireless sensor networks where numerous sensor nodes transmit sensitive information, IoT requires exceptional information privacy and security [6]. Only a small percentage of them use the same encryption methods as regular desktop PCs and powerful processors. However, the bulk of them employ low-feature, low-power, and resource-efficient microcontrollers. Therefore, it is crucial to study and create new cryptographic methods.

2. Research Contribution

Due to different IoT applications, effort has been induced to examine security vulnerabilities in IoT devices. To understand the security component of IoT, it is first important to understand the infrastructure we are working with. To that end, we've talked about IoT architecture and evaluated the various standards and protocols used in IoT. To establish an IoT security framework, additionally, analysis entails examining all relevant facets of current IoT security research. The thorough analysis of this survey focuses on the most recent security techniques that have been offered for the Internet of Things industry in recent years, as well as the considerable risks that now exist in IoT systems.

The goal is to describe mitigation techniques in terms of the four security needs for IoT: trust management, confidentiality, and integrity [7]. Identifying and comparing popular IoT protocols and standards makes up our third research contribution. We've covered the most recent developments and standardization techniques used in IoT [8], the categorization of security concerns in IoT based on how much the entire ecosystem is impacted, and the appropriate solutions. The results of the study demonstrate that new security design models and existing encryption techniques are used to address IoT security issues. Trust and communication integrity has been identified as the two main security concerns. Additionally, it was discovered that integrating IoT with different network protocols like SDN makes IoT security concerns more difficult [9, 10]. It is also established that there must be uniformity at the assembly level to reveal software and hardware faults [11]. According to inspections, a wide range of threat vectors must be dealt with [12, 13]. The study's findings can benefit the IoT research community by making it possible to deploy the safest security measures in IoT-based goods.

The remainder of this work is organized as follows, Section 3 describes the related works on IoT-based communication and security. Section 4 deliberates the IoT architecture in detail. The various security challenges are listed in Section 5 and their mitigation techniques are presented in Section 6. The comparative analysis is presented in Section 7. The paper is concluded in Section 8 with some ideas for future research.

3. Related works

In this part, we present some of the most recent research on the privacy and security of IoT surveys that have been published. A full analysis of the security-related difficulties and likely sources of attacks in IoT applications was provided by the study in [14]. The report included detailed recommendations for enhancing the IoT framework to enable secure communications. The author also discussed ways to improve IoT security by utilizing cutting-edge technologies like blockchain, edge computing, fog computing, and machine intelligence. Similar concerns regarding IoT security and safety were discussed in [15]. This is achieved by highlighting security flaws that potentially lead to security breaches as well as general risks and attack vectors against IoT devices.

This study also included several security upgrades, risk-reduction techniques, and patches for infected devices. Mishra et al. evaluated the IoT's development, uses, and difficulties [16]. The security flaws related to IoT were demonstrated using a layered approach. To improve IoT security, anomaly detection methods were contrasted with the most recent Intrusion Detection System (IDS). The authors in [17] reviewed the IoT security research trends from 2016 to 2018. This study described modelers, simulation tools, analytical and statistical platforms, and other crucial tools and simulators used by researchers studying IoT security.

Based on the 3-tier IoT model, HaddadPajouh et al. [18] explored IoT security concerns, difficulties, constraints, requirements, and potential solutions. In their discussion of machine learning (ML) and deep learning (DL) techniques, Al-Garadi et al. [19] argued that these techniques can change the nature of the Internet of Things security from "facilitating secure communication between devices to security-based intelligent systems." In this work, the attack vectors and possible vulnerabilities of IoT devices were investigated [20]. To solve the security difficulties based on a layered IoT architecture, Zaman et al. provided a survey on concerns regarding IoT security in addition to AI-based security models. The security advantages that modern innovations like blockchain and software-defined networks (SDN) bring to IoT networks were stressed by Kouicem et al. [21]. Flexibility and scalability are these two systems' two key security advantages.

The problems and security needs for different applications for the Internet were also examined in the report. Security solutions come in two flavors: traditional and modern. Data security, communication, and device security are all included in the taxonomy of security demands that Harbi et al. used to examine IoT security [22]. The essay examined the issues with various IoT applications and offered security solutions. IoT security risks were covered by Hamad et al. [23] along with potential defenses, and identified the key security criteria required to minimize the IoT's resource limitations and heterogeneous nature as security concerns. According to the study, security services including access control, integrity, authentication, anonymity, confidentiality, and privacy are categories under which security solutions are categorized.

In [19], the authors explored portable cryptography techniques for restricted IoT entities. Symmetric and asymmetric lightweight cryptography models are the two main categories. Resource requirement performance measures for hardware and software are introduced. In the paper, lightweight methods that were mentioned in the literature were briefly described. A lightweight algorithm that successfully balances efficiency, expense, and security is the best. According to Hameed and Alomary [24], a variety of attacks on the IoT are reduced by employing simple encryption and authentication mechanisms. Additional research, according to the authors, is necessary to enhance IoT device security. Lu and Xu [25] used the 4layered security-based design for IoT to examine security assaults on the technology and provided the organization of IoT cybersecurity attacks. They discussed its significance in different industries and how to ward off assaults. Although various works on IoT security have been published, as was indicated above, they are only relevant to a small portion of IoT. There is a need for more thorough surveys because some topics have not been addressed, such as security problems associated with incorporating new technologies into IoT and security hardware solutions that can match IoT devices with limited resources. Below is a list of what this work contributed.

1. Analysis of difficulties and potential solutions related to the IoT's integration of developing technologies.
2. Outline cost-effective hardware security options for IoT devices with limited resources.
3. Review the hardware, software, and data-in-transit security risks associated with IoT.
4. Identify and describe common IoT security primitives as well as additional technologies used to defend IoT networks and devices from threats or assaults

4. IoT and its Architecture

The use cases for the Internet of Things range from single-limited node devices to substantial cross-platform executions of implanted technology and real-time cloud systems [26]. As was previously mentioned, IoT activities are made up of three main tasks, such as transmitting, retrieving, and processing data. The IoT is a tool that consists of data interchange across varied devices that transmit information continually to other auxiliary devices.

Figure 2 shows the multi-layer, multi-plane design of the Internet of Things. It consists of the Device Management, Application Interface, and Communication Plane component areas. User Interface (UI) Layer: At this layer of the design, there are embedded interface components that enable devices, including the Arduino and Raspberry Pi development environments, sensors, actuators, and other devices, to interact with the underlying architecture. By identifying the source and destination of the data, the Device Management Plane maintains the device i/o activities. For instance, the central Aggregator component collects the information arriving in from the devices.

The communication layer, an intermediary layer that establishes communication standards and protocols for IoT network traffic, is made up of switches and other comparable network components.

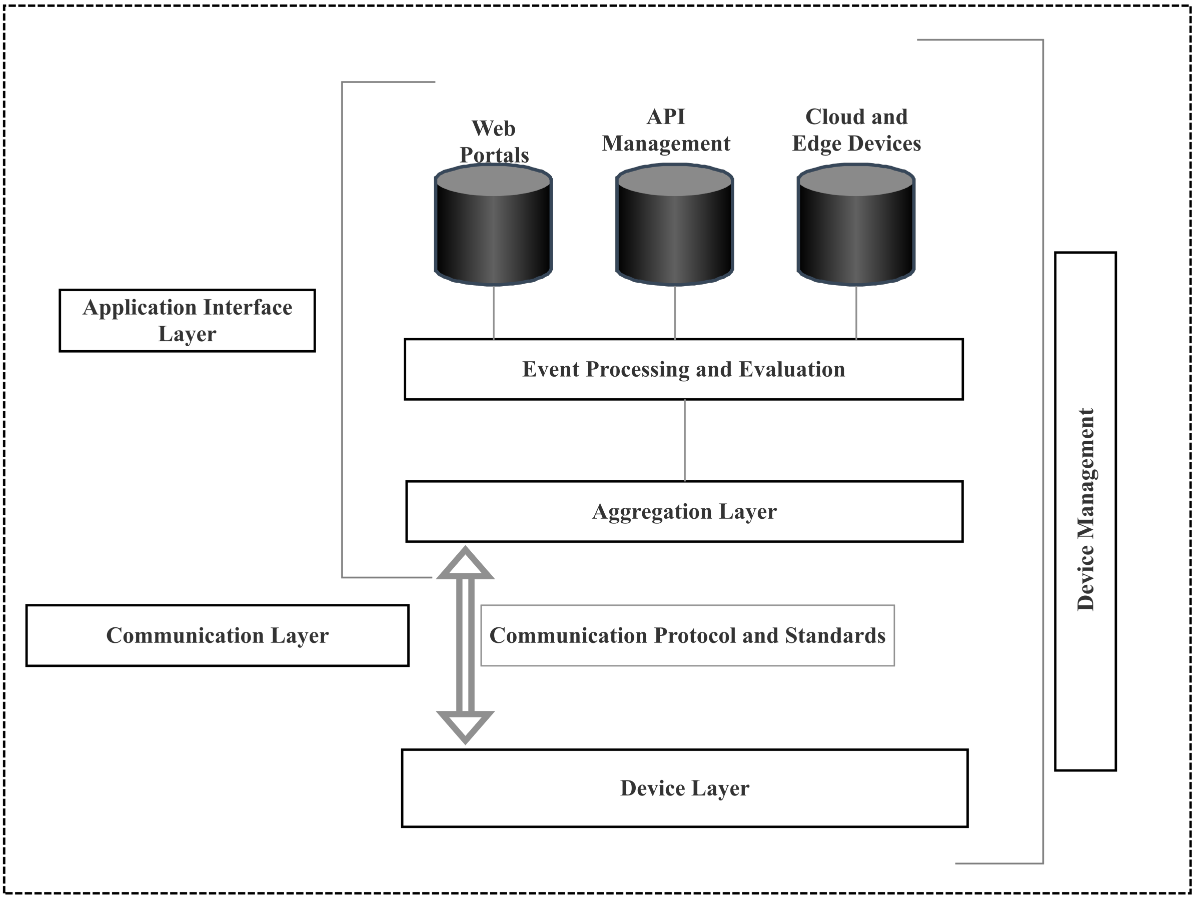

Figure 2: Multi-Layer Architecture of IoT.

This layer, which regulates network traffic across the entire system, is made up of layers of the latest protocols and standards. New, diversified communication protocols are used in embedded IoT contexts that are more energy-efficient, better able to control congestion, and have improved QoS features.

5. Security Inclinations in IoT

IoT is not constrained by scarce resources, as can be seen from the sections above. The IoT's operational perspective has expanded as a result of emerging technologies like 5G [27], blockchain [28], quantum computing, and edge computing being incorporated. Figure 3 illustrates the real-world effects that new technologies have on IoT functionaries. This unstable environment is made up of several physical entities, such as switch nodes, actuators, gateways, and other embedded system parts. The core of the entire notion, the engineering of smart devices, has an enormous effect on the IoT and goes beyond networking concepts.

The most recent IoT breakthrough is self-configuring hardware that uses the M2M communication paradigm. Through the use of algorithms and additional technology, this configuration gives nodes the intelligence necessary to make decisions on their own under any circumstance [29]. It is useful during rescue operations and other emergencies where configuring the network for a specific area is difficult since damaged nodes may not be able to provide much support. However, since machines are not infallible, a reliance on them that is too great leaves it open to risk. Particularly in the present, adversaries make use of poor authentication, vulnerable internet-based credentials, unpatched firmware, and weak authentication.

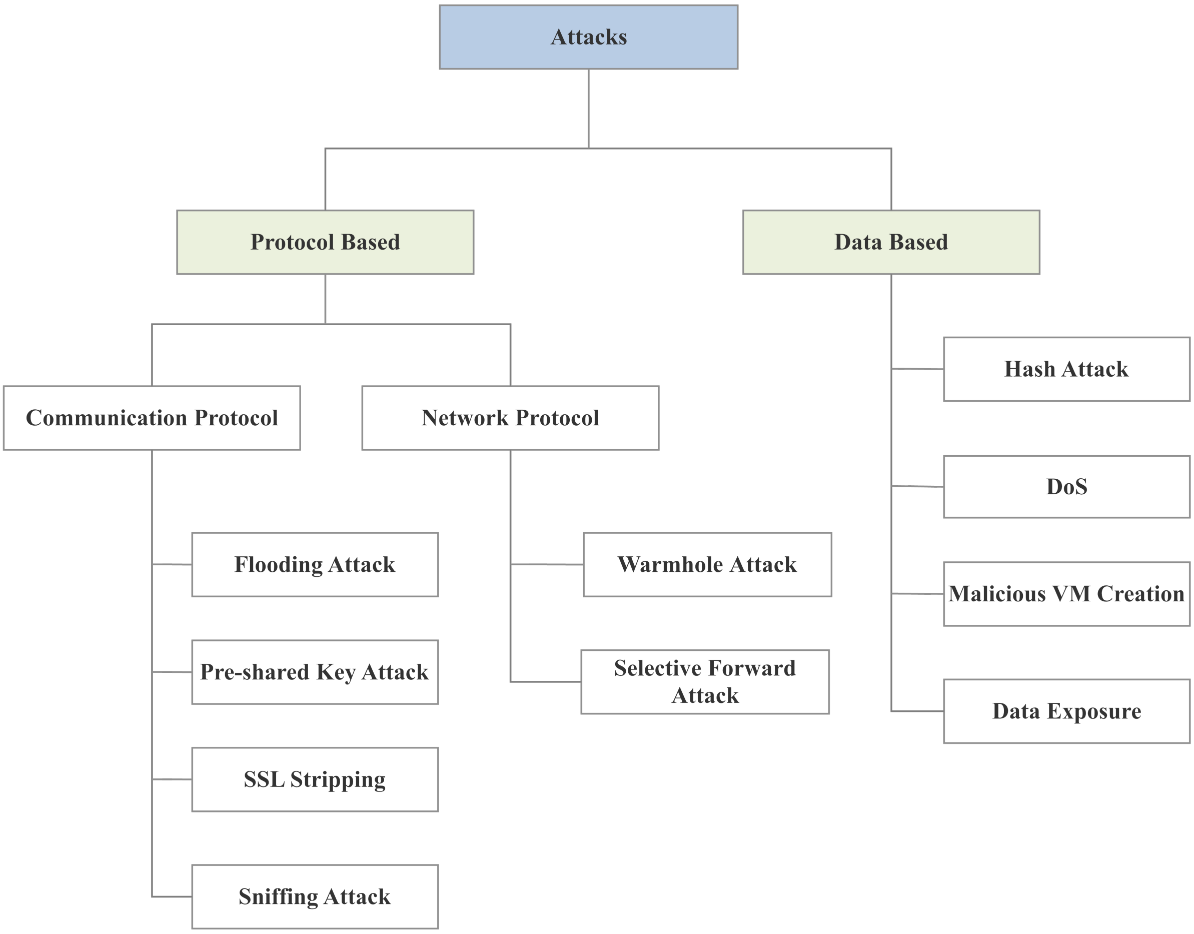

Figure 3: Classification of IoT Attacks.

5.1. Security Challenges

There are several security issues with IoT today that relate to traditional network architecture [30], including:

A. Heterogeneous Device Configuration:

IoT devices use a different method of physical world communication than older traditional network devices. The variety of IoT devices has an impact on how other networking components work. NIST stressed that cybersecurity measures and privacy legislation tailored to the Internet of Things [31] must take into account how IoT devices affect physical components [32], which in turn have an impact on the physical environment. As a result, a form of security problem is represented by heterogeneity's properties [33].

B. Dispersive Network Update Policy:

IoT devices are handled globally through widely dispersed servers, whether they are in a business or a person's workspace. Such IoT devices can be accessed, controlled, or analyzed using a different type of rule engine, and security policy varies depending on the system's devices.

As a result, updating every device is necessary for regularization, which is a time-consuming and challenging procedure for the business. The pace of updating may not be uniform, new switches may leave some devices behind that aren't updated, or nodes may be improperly configured because it takes time to keep track of millions of nodes. The system's access control may be compromised by outside assistance in the discussed issue. Geographically scattered organizations face time- and cost-intensive problems and need to be updated and safeguarded.

C. Add-Ins Security Policy:

Security controls were never intended to be a part of the Internet of Things. The layered IoT design is improved with more plugins and security controls to produce secure applications. The ability of the IoT architecture to operate with more resources, in contrast to the outdated network paradigm, is therefore essential to the effectiveness of security features. The efficiency of the IoT's security is also influenced by client behaviors, such as how they choose from the various security options.

D. Physical IoT threats:

Network-integrated healthcare systems, industrial units, and corporate sectors all confront real physical security threats with their physical IoT implementations. The two main attack vectors are communication routes and data audit functionaries [34].

At the moment, network entities, participant trust management, and the communication channel's network mode are all security-related concerns. Specific security challenges for data audits demonstrate the vulnerable security points present during massive amounts of data transmission through networks and the collection layer of IoT architecture. The sophisticated network components being unintentionally or purposely damaged is another issue with physical security. IoT hardware, such as robotics, sensors, and hardware devices, might provide physical risks to the physical entities in industrial systems [35].

E. Exposure Threat:

The IoT's end devices, which include IP cameras and sensors placed in public areas, are the threat points that are most accessible to the adversary. As a result, physical-based and proximity assaults pose a threat to the user's integrity and authentication [36]. The largest security challenges in this field are related to the framework modifications that will make to the protocol or communication system to protect such devices from attackers.

5.2. Attack Types in IoT

Designing security solutions requires careful consideration of probable threats to design depending on behavior and target set. In recent years, several commercial businesses have made significant financial investments to secure their IoT-based networks. The two modules of IoT attacks are represented in the figure as follows:

1. Protocol-Based Attacks:
   These attacks take use of the embedded systems' inherent protocol-based architecture to affect the communication channel and forwarding channels. These are further divided into different categories. Two are protocol-based:
   a) Attacks based on communication protocols This exemplifies the various forms of exploitation that happen between nodes during times of transition. These comprise crucial pre-shredding assaults, flooding attacks, and sniffer attacks.
   b) Attacks based on network protocols: This article talks about the exploitation that occurs when connections are made. Attacks include wormhole assaults, targeted forward assaults, and sniffing assaults.
2. Data-Based Attacks:
   These include dangers involving the initial packets of data and messages moving across node sites. Some of its most severely affected security exploitations are data leakage, malicious node VM formation, hash collision, and denial of service.
   Active and passive ways of IoT attack classification Several well-known attacks use active and passive forms. Such attacks are crucial for IoT security because the various network performance consequences of the security mechanisms employed in the context of IoT to avoid active and passive attacks vary. Active attacks must be defended against current, responsive security methods to minimize risk and impact network performance. However, passive attack defenses, which are limited to monitoring techniques, have little effect on the network's effectiveness.
   a) Distributed denial of service (DDoS) [37]: DDoS is a noteworthy IoT concern because it affects the availability of a network security parameter. To conduct a DDoS attack against

sensor nodes or any other physically vulnerable nodes, botnets are developed. Through these entry points, infected packets from multiple sources get access, move down network data paths, and finally jam up the entire link architecture, proving servers useless. Energy transmission industries, military communications, emergency operations, and last but not least, healthcare institutions, are all extremely risky.

b) Traffic sniffing attacks [38]: Active data collection, a threat activity in which crucial system information is obtained and subsequently exploited for assaults like botnet attacks, includes attacks employing traffic sniffing. Such a penetration operation involves the use of sophisticated tools to examine information assets, such as usernames, passwords, unencrypted data information, authentication type, and hardware information. The bulk of Internet of Things (IoT) devices currently available are not fully intelligent enough to mitigate such risks and easily become their targets.

c) Masquerade attack [39]: This attack impersonates a valid access identification procedure to get accessibility to target node information. It does this by using a phony network ID. Devices that have shoddy authorization procedures are highly vulnerable. Through the discovery of logical gaps in programs or the development of workarounds for the current authentication procedure, such attacks make use of hacked passwords and user data. The level of access that can be achieved by a masquerade assault relies on the penetrator's position of authority.

d) Message Replay Attack [40]: A replay attack consists of three steps: monitoring the gateway or secure communication between IoT devices; intercepting the elements that establish connections or acknowledgments; and intentionally delaying or rerouting data using message replay. Forcing network devices to perform tasks for which they were not intended or swaying the outcome in the attacker's favor, hinders them from operating normally. Because the entire message may be replayed after packet seizing to get access to the server, implementation is simpler and doesn't require complex message decryption skills.

e) Port Scanning: The elements of port scanning include SYN requests, target ports, sources, firewalls, packets, open nodes, and monitoring nodes [41]. A common technique is SYN scanning, which involves sending an SYN packet to establish a tenuous link to the target port's host system to gauge its initial response.

6. Mitigation Techniques for IoT

Data at rest (data saved on a device) and data in transit (data sent via a communication channel) should both be encrypted using the best methods possible. This is the accepted procedure for tackling various risks to IoT networks and the Internet of Things. So, to confirm the legitimacy of an entity requesting access to a network, device, or service, the proper authentication methods are required. The following stage is to consider how to implement various security protocols from the standpoint of the tiers of the IoT security architecture. Additionally, we need adequate security measures to safeguard IoT networks and devices against sophisticated threats and attacks that could be application-specific.

6.1. Cryptographic Solutions for Protecting Data

Unfortunately, not all of the cryptographic techniques that can be used to safeguard our private information are appropriate for situations when resources are limited, such as IoT devices. IoT devices deployed in commercial and industrial contexts may be subject to IoT-specific risks [42, 43]. We'll soon see a lot more security catastrophes if we stick with the current IoT device design cycle, where security is treated as an afterthought. To develop a robust cryptographic solution for restricted IoT devices, researchers are looking into lightweight cryptographic methods.

1. Lightweight Cryptography: Data encryption is necessary for the perceptual, network, and application levels to safely protect the data they generate and send. The perceptual layer is the

most limited of all three layers, necessitating a simple cryptographic scheme. A cryptographic algorithm's lightweight is assessed using two criteria [44]. The time and memory complexity of the cipher determines the first demand, which is the weight of the computer program. Memory complexity or time complexity refers to how long it takes the cipher to transform plaintext into ciphertext. The amount of memory required to carry out the ciphering procedure is referred to as "time complexity".

The second criterion is the cipher's size, power consumption, and hardware weight. The size of the cipher is determined by the number of gate equivalencies (GE) employed in implementing it, whereas the power employed by the cipher refers to the energy expended during implementation. To calculate the general efficiency (GE), divide the area of a two-input NAND gate by this area. The algorithm must adhere to lightweight requirements while performing similarly to conventional algorithms in terms of security standards and defense against security assaults. There are two groups of the present cryptographic primitives: Both symmetric key and asymmetric key cryptography are used.

2. Asymmetric Key Cryptography based Solutions: Asymmetric cryptographic algorithms have unfortunately not yet produced findings that are as consistent and fruitful as symmetric cryptographic algorithms, despite the efforts of a small number of lightweight cryptography experts. Since the operation of lightweight asymmetric cryptographic algorithms is complicated, these algorithms frequently do not use little space or power. These techniques are becoming more exposed as attack models progress [45]. Trapdoor functions, such as prime and semiprime factorization and Euler's totient function, are often the foundation of asymmetric algorithms [46]. Key distribution methods and encryption algorithms are two categories of asymmetric algorithms. Rivest-Shamir-Adleman (RSA) is a well-known illustration of an asymmetric encryption technique.

   Asymmetric key distribution algorithms include Diffie-Hellman and Elliptical Curve Cryptography (ECC). To create a digital signature, ECC and the Digital Signature Algorithm (DSA) cooperate within the structure of public key cryptosystems. Despite the complexity and slowness of key generation, RSA is particularly safe because it makes it exceedingly difficult for an attacker to reverse the process and create the private key from the public key [47].
3. Elliptical Curve Cryptography (ECC): Although ECC is more complicated and challenging to implement than other asymmetric algorithms, it uses comparatively less power. Therefore, ECC is best suited for use in limited devices [48]. DH, or Diffie-Hellman. Although key generation is complex and takes a long time, RSA is highly secure because it makes it difficult for an attacker to reverse the process and produce a secret key from the public key [49]. However, this makes RSA vulnerable to man-in-the-middle attacks.
4. Digital Signature Algorithm (DSA): Compared to other asymmetric techniques, DSA is speedier and more advantageous. Digital signatures are not only hard to share, but they also expire quickly [47]. When compared to other asymmetric techniques, ECC utilizes the least amount of electricity. Recently, this IoT adoption method has become a key research topic, especially from a software perspective. The Contiki OS for IoT contains an open-source ECC that has been developed and tested by [48]. The Berkeley Software Distribution (BSD) license was used for its distribution. When implementing a Zero Knowledge Protocol in an open-source, general programming library called Wiselib, [50] used an ECC approach. In [51], the authors demonstrated how effectively side-channel attacks may be defended against when using an ECC computation. This strategy adhered to lightweight specifications while maintaining a low level of security. A comparison of RSA, Diffie-Hellman, and Elliptical Curve Cryptography with Diffie-Hellman (ECDH) has been shown in [11]. The researchers' conclusions show that ECDH outperforms various other algorithms, related to power and area. As with symmetric key cryptography, the evaluation of public key cryptography's performance is incomplete.
5. Symmetric Key Encryption: Because most operations in symmetric cryptography revolve around bitwise functions like XOR and permutations, these algorithms are less resource-intensive and faster. These algorithms are therefore better suited for IoT applications. The difference between

Table 1
Recent IoT Protocols and Features.

Protocols	Topology	Energy Consumption	Common Threats	Security Solutions
COAP	Random, Chain, Grid, Dumbell, and Cross	Low	DDoS, Malicious Node Creation, Botnet	IPSec, DTLS
DDS	Random	High	Man-in-the-middle, DDoS	DTLS
BLE	Piconet	Low	ID tracking, Man-in-the-middle	GAP
SigFOX	One-hop Star	Low	Weak Payload Encryption Attack	H/w Sec Module

Table 2
Security Requirements Based on Security Demands.

Papers	Model Used	Confidentiality	Integrity	Availability	Trust	Authenticity
[11]	Data Encryption				Yes	Yes
[12]	Fuzzy Logic	Yes			Yes	
[13]	Multi-level Data Encryption	Yes	Yes			
[58]	Mathematical Evaluation			Yes	Yes	
[59]	Blockchain		Yes			Yes
[60]	Cryptographic Data Encryption		Yes			Yes
[61]	Socket Programming	Yes	Yes			Yes

block ciphers, hash functions, and stream ciphers in symmetric algorithms is crucial [52].

6.2. Recent Solutions for IoT Security Issues

In contrast to earlier security, which was tool-centric, the most recent IoT security techniques are more focused on software-centric security solutions [53]. Current solutions focus on three main security issues: verification, trust, and the dependability of the communication route between IoT devices. Even in its current state, IoT fails to support powerful devices and lacks enough adaptability to keep up with the growing number of incompatible entities. Table 1 displays a comparison analysis of IoT protocols. IoT has additional security concerns as it integrates with other emerging technologies like SDN for improved scaling, node management, safety measures, and reliability.

Undoubtedly, the performance factor of these protocols has increased, but this has also highlighted the weak points in the rule flows. The DTLS authentication system is supported by the CoAP protocol, and IPSec offers ad hoc support. Although load-based attacks like a botnet and DDoS attacks are still a security risk, the transient period is still secure [54]. The MQTT protocol provides a Transport layer-based security support layer for secure transient periods. Problems include malicious node subscription attacks and, once more, botnet attacks. EnOcean [55] offers a special rolling code key encryption mechanism that ensures the nodes are in their environment. A hierarchical attack defense model has been proposed and provided a solution for security threats in IoT [56].

Cons include concerns with key secrecy and code synchronization. For the changing IoT setup environment, SigFOX [57] offers protection support through several security solutions. These solutions include a strong firewall, hardware security component, a system for public keys, and on-the-go security deploying security solutions. It is a paradigm for virtual security. Weak Payload encryption is the problem. Nearly every new protocol has low energy consumption standards, which is an encouraging characteristic because it will function greater in a high-density network and thereby improve network performance.

7. Comparative Evaluations on Various Security Models

As was previously noted, a wide range of innovative security measures for IoT contexts have been offered. As demonstrated in Table 2, the effectiveness of each in satisfying the essential security requirements of the IoT network is compared. The technique's parameters and the security standards are noted to be met in this assessment. Confidentiality, reliability, and availability, as well as trust management between nodes and authenticity, are all addressed in this section.

Incorporating the UDS and USD WSN authentication models, the dual authentication model put forth by Xin Zhang and Fengtong Wen [62] is successful in meeting the authorization and trust security requirements but falls short in terms of the CIA requirements, making it vulnerable to tracking, sniffing, and DDoS attacks as well as botnet attacks. The security strategy suggested in [63] satisfies the CT security requirements. Despite this, it is vulnerable to several security problems, including malware, DDoS assaults, and relay attacks.

The authors in [64, 65] give recommendations for security techniques have security elements for Integrity security demands. To prevent Integrity-based attacks, strong cryptographic security solutions have been put out by Priyanka et al. [49]. To satisfy the requirements for secrecy and integrity security, the paper's [65] security proposal presupposes the usage of MFCC security coefficients. The model proposed by the authors [66] satisfies accessibility and trust security criteria through the Hilbert-Huang transformation; however, security parameters can be exploited.

7.1. IoT Applications based Security Solutions

1. Non-Token based
   To send or receive data, this method calls for the user to input credentials. TLS/DTLS (Transport Layer Security/Datagram Transport Layer Security) is a popular protocol for this method. Based on the thing that DTLS is not responsible for packet loss validation, it is used to handle UDP's unreliability. The computational cost of DTLS is high. Figure 4 demonstrates the use of the DTLS handshake for mutual authentication. There are literature-based lightweight DTLS variants for restricted devices.
2. Hardware-based Using the physical characteristics of the hardware, this technique performs authentication. Implicit and explicit strategies can be separated into two groups [67]. Implicit hardware-based solutions carry out the authentication process by utilizing the particular physical traits of the device. Two often employed methods are the True Random Number Generator (TRNG) and Physical Unclonable Functions (PUFs). One of the lightest hardware-based authentication methods that have received the most research is PUFs. Explicit hardware-based techniques perform authentication using keys kept on an IC.
3. Message Authentication
   Data/message integrity in transit is a concern of message authentication. In other words, the communication is not altered while in route, and the recipient can confirm the message's original source. Digital signatures and message authentication codes [68] are two methods for message authentication. The "LightMAC" technique used for Message M authentication is shown in Figure 5.

7.2. Application-based Security Solution

The document [68] summarizes the security risks that several of the popular IoT products on the market today face. The list of popular Internet of Things equipment with remarks on security concerns and security fixes is provided below.

1. IDFA tags:
   Area, electricity, computational power, and storage are the key limitations of RFID tags. The result is the introduction of ultralightweight and lightweight privacy techniques. Security Alternatives: Block ciphers TEA and KATAN, stream ciphers Grain and Trivium, and hash algorithms Keccak and Spongent [69].

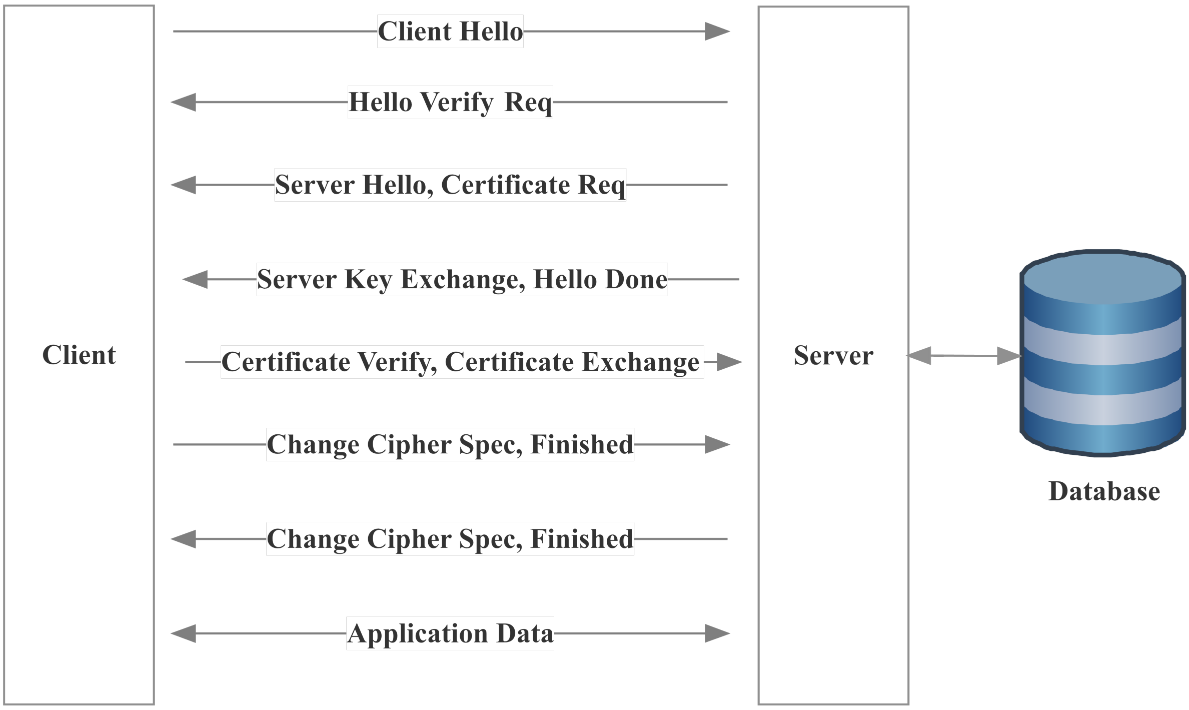
Client
Client Hello
Hello Verify Req
Server Hello, Certificate Req
Server Key Exchange, Hello Done
Certificate Verify, Certificate Exchange
Change Cipher Spec, Finished
Change Cipher Spec, Finished
Application Data
Server
Database

Figure 4: DTLS Handshake Model.

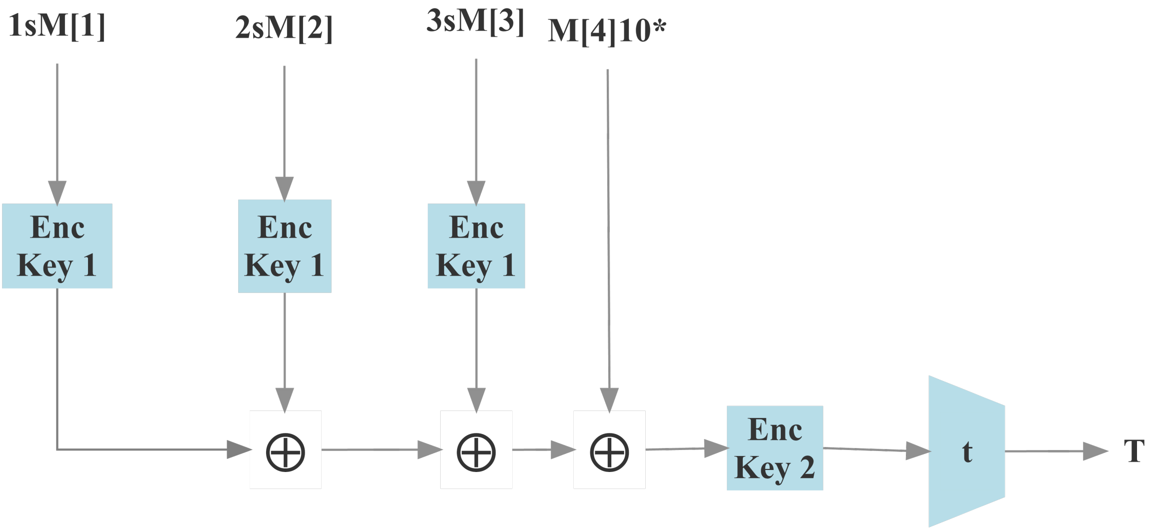

Figure 5: LightMAC Model.

2. Smart Watches:
   Smartphone contains sensitive data, and hackers employ security risks to get access to it. Pairing-Based Cryptography, SHA 1, SHA 2, RSA 1024, RSA 2048 E, and RSA 2048 D are security measures [70].
3. Devices that support Universal Plug and Play (UPnP):
   A malicious program may be able to completely avoid the firewall thanks to UPnP. Disabling UPnP on routers until absolutely necessary is a security fix.
4. Minivan or small car:
   Modern automobiles come with gadgets that can communicate via Bluetooth, radio frequency,

and the internet. The gadgets' heterogeneous implementation of security leaves the car open to outside remote attacks.

5. Toys for kids:
   In the case that a hacker gains access to the device, any personal data kept on it needs to be encrypted. Security fixes: Toys must adhere to pertinent security requirements set forth by organizations like GDPR, COPPA, and PECR. For authenticated sessions, use Transport Layer Security [71].
6. IoT Camera:
   Many of the vulnerable devices lack both the encryption of all communications between the camera, applications, and servers, as well as the authentication of the streaming video protocols. Use Transport Layer Security (TLS) for data encryption and HTTPS for account authentication. Additionally, data ought to be encrypted at rest using a recognized technique (like AES) [72].
7. IoT Medical Devices:
   There haven't been any reported cases of IoT medical devices being used maliciously. However, there are tales of successful hacks. AES-256 encryption is used to protect data sent to and from devices, data is cryptographically signed to prevent tampering, and the private key is kept on a Trusted Platform Module (TPM). Use multi-factor authentication for user access. Utilizing Hardware Security Modules (HSMs) with server-side applications [73] prevents unauthorized access.
8. IoT Thermostat:
   The safe operation of this gadget could mean the difference between life and death because there are locations with subfreezing winter temperatures and scorching summer temperatures.
9. Security measure:
   To connect to the Wi-Fi network, Google Nest uses two-factor authentication, Wi-Fi Protected Access II (WPA2), and WPA3 security, with TLS to protect communication [74].
10. Smart Lock:
    A smart lock does not increase the security of a lock over a standard mechanical lock. The smart lock from August is a security measure. Security measures include two-factor authentication, Bluetooth Low Energy (BLE) two-layer encryption, and a lost phone function that enables the consumer to eliminate all virtual keys kept on the software loaded in the phone [75].
11. Air Quality Sensor:
    These devices function as standalone wireless sensor nodes. Security procedures are needed to protect them from security concerns that could jeopardize data integrity. Security measures Wi-Fi should be secured using WPA2 or WPA3, and end-to-end encryption should be performed using HTTPS. Flash encryption is used to safeguard sensitive data on flash memory [76].
12. Industrial IoT Devices:
    An "egg shell" network paradigm must never be used for implementing security measures in a SCADA system. Security measures Symmetric keys can be protected via hash algorithms (SHA2 to SHA5) and hash-based Message Authentication Codes (HMAC). For asymmetric keys, use the Elliptic Curve Digital Signature Algorithm (ECDSA). A hardware root of trust (HRoT) model, including a hardware security module (HSM), a TPM, and secure mutual authentication is discussed in [77].
13. Voice Activated Services:
    Many works have proved that a hacker can command a device audibly with or without having physical access to it. Multi-factor authentication methods are security fixes. To encrypt data, WPA2 or WPA3 can be used [78].

8. Conclusion and Future Work

This research highlighted the most current security advancements in the IoT model industry by reviewing the recently proposed architectures, protocols, and encryption approaches necessary to safeguard the

IoT network. The study's findings on IoT security risks highlight the growth of IoT threats' attack surfaces and flaws in data- and protocol-based attacks, demonstrating how outdated traditional defenses against dynamic attacks like malicious nodes, DDoS attacks, and botnet attacks that are common in heterogeneous IoT are no longer effective. The employment of various encryption approaches has been demonstrated to be effective in protecting channels that transmit information attack surfaces in the Internet of Things while promoting lower energy usage, according to studies of current research models. By combining technologies like deep learning, fuzzy logic based on AI, elliptical cryptographic procedures, and blockchain, the security of IoT networks has increased. On the downside, it has made the system's overall complexity higher. The degree of openness in the purpose of security provisions has reduced as a result of the extensive degree of abstraction of such complicated solutions. The tireless efforts performed by scientific researchers around the world in previously discussed issues have been attempted to deal with the evolution of current communication methods, protocols, and globally recognized standards in this work. Nevertheless, there is always room for exploration.

Acknowledgment

This paper was supported by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Belgrade, Serbia.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] S. S. M. Al-Dabbagh, I. F. T. Al Shaikhli, K. A. Al-Enezi, M. J. Alyaqoup, Enhancing lightweight block cipher algorithm olbca through decreasing cost factor, in: 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), IEEE, 2015, pp. 159–164.

[2] R. Ankele, S. Banik, A. Chakraborti, E. List, F. Mendel, S. M. Sim, G. Wang, Related-key impossible-differential attack on reduced-round s kinny, in: Applied Cryptography and Network Security: 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings 15, Springer, 2017, pp. 208–228.

[3] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, Camellia: A 128-bit block cipher suitable for multiple platforms—design andanalysis, in: Selected Areas in Cryptography: 7th Annual International Workshop, SAC 2000 Waterloo, Ontario, Canada, August 14–15, 2000 Proceedings 7, Springer, 2001, pp. 39–56.

[4] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, F. Regazzoni, Midori: A block cipher for low energy, in: Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21, Springer, 2015, pp. 411–436.

[5] S. N. Basha, S. Jilani, M. S. Arun, An intelligent door system using raspberry pi and amazon web services iot, International Journal of Engineering Trends and Technology (IJETT) 33 (2016) 84–89.

[6] M. Bellare, T. Kohno, A theoretical treatment of related-key attacks: Rka-prps, rka-prfs, and applications, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2003, pp. 491–506.

[7] S. Jaiswal, D. Gupta, Security requirements for internet of things (iot), in: Proceedings of International Conference on Communication and Networks: ComNet 2016, Springer, 2017, pp. 419–427.

[8] P. Radanliev, D. C. De Roure, J. R. Nurse, R. Mantilla Montalvo, S. Cannady, O. Santos, L. Maddox, P. Burnap, C. Maple, Future developments in standardisation of cyber risk in the internet of things (iot), SN Applied Sciences 2 (2020) 1–16.

[9] K. Sood, S. Yu, Y. Xiang, Software-defined wireless networking opportunities and challenges for internet-of-things: A review, IEEE Internet of Things Journal 3 (2015) 453–463.

[10] Y. Li, M. Chen, Software-defined network function virtualization: A survey, IEEE Access 3 (2015) 2542–2553.

[11] A. Bhattacharjya, X. Zhong, J. Wang, X. Li, Security challenges and concerns of internet of things (iot), Cyber-Physical Systems: architecture, security and application (2019) 153–185.

[12] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, G. Wang, Security and attack vector analysis of iot devices, in: Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10, Springer, 2017, pp. 593–606.

[13] P.-A. Vervier, Y. Shen, Before toasters rise up: A view into the emerging iot threat landscape, in: Research in Attacks, Intrusions, and Defenses: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings 21, Springer, 2018, pp. 556–576.

[14] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on iot security: application areas, security threats, and solution architectures, IEEe Access 7 (2019) 82721–82743.

[15] A. Jurcut, T. Niculcea, P. Ranaweera, N.-A. Le-Khac, Security considerations for internet of things: A survey, SN Computer Science 1 (2020) 1–19.

[16] N. Mishra, S. Pandya, Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review, IEEE Access 9 (2021) 59353–59377.

[17] W. H. Hassan, et al., Current research on internet of things (iot) security: A survey, Computer networks 148 (2019) 283–294.

[18] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for internet of things (iot) security, IEEE communications surveys & tutorials 22 (2020) 1646–1685.

[19] V. A. Thakor, M. A. Razzaque, M. R. Khandaker, Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities, IEEE Access 9 (2021) 28177–28193.

[20] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, M. Mahmud, Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey, Ieee Access 9 (2021) 94668–94690.

[21] D. E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: A top-down survey, Computer Networks 141 (2018) 199–221.

[22] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, A. Refoufi, A review of security in internet of things, Wireless Personal Communications 108 (2019) 325–344.

[23] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, S. Nepal, Realizing an internet of secure things: A survey on issues and enabling technologies, IEEE Communications Surveys & Tutorials 22 (2020) 1372–1391.

[24] A. Hameed, A. Alomary, Security issues in iot: A survey, in: 2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT), IEEE, 2019, pp. 1–5.

[25] Y. Lu, L. Da Xu, Internet of things (iot) cybersecurity research: A review of current research topics, IEEE Internet of Things Journal 6 (2018) 2103–2115.

[26] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions, Future generation computer systems 29 (2013) 1645–1660.

[27] S. Li, L. Da Xu, S. Zhao, 5g internet of things: A survey, Journal of Industrial Information Integration 10 (2018) 1–9.

[28] S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, A. Khanna, An efficient lightweight integrated blockchain (elib) model for iot security and privacy, Future Generation Computer Systems 102 (2020) 1027–1037.

[29] T. Leppänen, J. Riekki, M. Liu, E. Harjula, T. Ojala, Mobile agents-based smart objects for the internet of things, Internet of Things based on Smart Objects: Technology, Middleware and Applications (2014) 29–48.

[30] M. Ahmad, T. Younis, M. A. Habib, R. Ashraf, S. H. Ahmed, A review of current security issues in

internet of things, Recent trends and advances in wireless and IoT-enabled networks (2019) 11–23.

[31] A. Rayes, S. Salam, Internet of things security and privacy, in: Internet of Things From Hype to Reality: The Road to Digitization, Springer, 2022, pp. 213–246.

[32] A. Soni, R. Upadhyay, A. Jain, Internet of things and wireless physical layer security: A survey, in: Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016, Springer, 2017, pp. 115–123.

[33] G. Yıldırım, Y. Tatar, On wsn heterogeneity in iot and cpss, in: 2017 International Conference on Computer Science and Engineering (UBMK), IEEE, 2017, pp. 1020–1024.

[34] J. Hou, L. Qu, W. Shi, A survey on internet of things security from data perspectives, Computer Networks 148 (2019) 295–306.

[35] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, A survey on hardware-based security mechanisms for internet of things, ArXiv. org (2019).

[36] H. Xu, D. Sgandurra, K. Mayes, P. Li, R. Wang, Analysing the resilience of the internet of things against physical and proximity attacks, in: Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10, Springer, 2017, pp. 291–301.

[37] M. M. Salim, S. Rathore, J. H. Park, Distributed denial of service attacks and its defenses in iot: a survey, The Journal of Supercomputing 76 (2020) 5320–5363.

[38] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, R. Budiarto, Investigating brute force attack patterns in iot network, Journal of Electrical and Computer Engineering 2019 (2019) 4568368.

[39] H. Shen, J. Shen, M. K. Khan, J.-H. Lee, Efficient rfid authentication using elliptic curve cryptography for the internet of things, Wireless personal communications 96 (2017) 5253–5266.

[40] S. Na, D. Hwang, W. Shin, K.-H. Kim, Scenario and countermeasure for replay attack using join request messages in lorawan, in: 2017 international conference on information networking (ICOIN), IEEE, 2017, pp. 718–720.

[41] C. Om Kumar, P. R. Sathia Bhama, Detecting and confronting flash attacks from iot botnets, The Journal of Supercomputing 75 (2019) 8312–8338.

[42] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, Y. Jin, Security analysis on consumer and industrial iot devices, in: 2016 21st Asia and South Pacific design automation conference (ASP-DAC), IEEE, 2016, pp. 519–524.

[43] P. Sudhakaran, C. Malathy, Authorisation, attack detection and avoidance framework for iot devices, IET Networks 9 (2020) 209–214.

[44] W. J. Okello, Q. Liu, F. A. Siddiqui, C. Zhang, A survey of the current state of lightweight cryptography for the internet of things, in: 2017 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2017, pp. 292–296.

[45] C. A. Lara-Nino, A. Diaz-Perez, M. Morales-Sandoval, Elliptic curve lightweight cryptography: A survey, IEEE Access 6 (2018) 72514–72550.

[46] N. Krzyworzeka, Asymmetric cryptography and trapdoor one-way functions, Automatyka/Automatics 20 (2016).

[47] S. Chandra, S. Paira, S. S. Alam, G. Sanyal, A comparative survey of symmetric and asymmetric key cryptography, in: 2014 international conference on electronics, communication and computational engineering (ICECCE), IEEE, 2014, pp. 83–93.

[48] O. P. Pinol, S. Raza, J. Eriksson, T. Voigt, Bsd-based elliptic curve cryptography for the open internet of things, in: 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2015, pp. 1–5.

[49] P. A. Urla, G. Mohan, S. Tyagi, S. N. Pai, A novel approach for security of data in iot environment, in: Computing and Network Sustainability: Proceedings of IRSCNS 2018, Springer, 2019, pp. 251–259.

[50] I. Chatzigiannakis, A. Pyrgelis, P. G. Spirakis, Y. C. Stamatiou, Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices, in: 2011 IEEE eighth international conference on mobile ad-hoc and sensor systems, IEEE, 2011, pp. 715–720.

[51] T. Backenstrass, M. Blot, S. Pontie, R. Leveugle, Protection of ecc computations against side-channel attacks for lightweight implementations, in: 2016 1st IEEE International Verification and Security Workshop (IVSW), IEEE, 2016, pp. 1–6.

[52] P. Sudhakaran, M. Kaliyaperumal, V. Sindhu, Secured authentication and key sharing using encrypted negative password in iot devices, ECS Transactions 107 (2022) 12713.

[53] O. Flauzac, C. Gonzalez, F. Nolot, Developing a distributed software defined networking testbed for iot, Procedia Computer Science 83 (2016) 680–684.

[54] K. Sonar, H. Upadhyay, A survey: Ddos attack on internet of things, International Journal of Engineering Research and Development 10 (2014) 58–63.

[55] F. Khursheeed, M. Sami-Ud-Din, I. A. Sumra, M. Safder, A review of security machanism in internet of things (iot), in: 2020 3rd International Conference on Advancements in Computational Sciences (ICACS), IEEE, 2020, pp. 1–9.

[56] P. Sudhakaran, M. Kaliyaperumal, T. Senthilkumar, R. Jeya, B. Sowmiya, Hierarchical and on-demand attack defence framework for iot devices, Wireless Communications and Mobile Computing 2022 (2022) 4335871.

[57] F. L. Coman, K. M. Malarski, M. N. Petersen, S. Ruepp, Security issues in internet of things: Vulnerability analysis of lorawan, sigfox and nb-iot, in: 2019 Global IoT Summit (GIoTS), IEEE, 2019, pp. 1–6.

[58] Statista, Internet of things (iot) connected devices installed base worldwide from 2014 to 2024, 2024. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[59] K.-H. Wang, C.-M. Chen, W. Fang, T.-Y. Wu, On the security of a new ultra-lightweight authentication protocol in iot environment for rfid tags, The Journal of Supercomputing 74 (2018) 65–70.

[60] S. Grooby, T. Dargahi, A. Dehghantanha, A bibliometric analysis of authentication and access control in iot devices, Handbook of big data and IoT security (2019) 25–51.

[61] H. F. Atlam, G. B. Wills, Iot security, privacy, safety and ethics, Digital twin technologies and smart cities (2020) 123–149.

[62] X. Zhang, F. Wen, An novel anonymous user wsn authentication for internet of things, Soft Computing 23 (2019) 5683–5691.

[63] M. D. Alshehri, F. K. Hussain, A fuzzy security protocol for trust management in the internet of things (fuzzy-iot), Computing 101 (2019) 791–818.

[64] M. Mukhandi, D. Portugal, S. Pereira, M. S. Couceiro, A novel solution for securing robot communications based on the mqtt protocol and ros, in: 2019 IEEE/SICE International Symposium on System Integration (SII), IEEE, 2019, pp. 608–613.

[65] P. Singh, V. Khanna, A mfcc based novel approach of user authentication in iot, in: 2nd International Conference on Emerging Trends in Engineering and Applied Science, ISSN, 2019, pp. 2454–4248.

[66] H. Chen, C. Meng, Z. Shan, Z. Fu, B. K. Bhargava, A novel low-rate denial of service attack detection approach in zigbee wireless sensor network by combining hilbert-huang transformation and trust evaluation, IEEE Access 7 (2019) 32853–32866.

[67] M. El-Hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, A survey of internet of things (iot) authentication schemes, Sensors 19 (2019) 1141.

[68] P. Williams, P. Rojas, M. Bayoumi, Security taxonomy in iot–a survey, in: 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), IEEE, 2019, pp. 560–565.

[69] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, M. M. Dessouky, Slim: A lightweight block cipher for internet of health things, IEEE Access 8 (2020) 203747–203757.

[70] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, Y. Koucheryavy, Feasibility characterization of cryptographic primitives for constrained (wearable) iot devices, in: 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), IEEE, 2016, pp. 1–6.

[71] A. K. Jadoon, L. Wang, T. Li, M. A. Zia, Lightweight cryptographic techniques for automotive cybersecurity, Wireless Communications and Mobile Computing 2018 (2018) 1640167.

[72] G. Chu, N. Apthorpe, N. Feamster, Security and privacy analyses of internet of things children's

toys, IEEE Internet of Things Journal 6 (2018) 978–985.

[73] Federal Trade Commission, Using IP cameras safely, 2020. URL: https://www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely.

[74] Device Authority, Securing a Connected/IoT Medical Device: a guide for device manufacturers and medical professionals, 2018. URL: https://www.deviceauthority.com/sites/deviceauthority/files/medical_device_insight_guide_2018.pdf.

[75] Google Nest, Google Nest Wifi security features, 2020. URL: https://support.google.com/googlenest/answer/9547625?hl=en.

[76] August, August Smart Lock, 2020. URL: https://august.com/products/august-smart-lock-3rd-generation.

[77] L. Luo, Y. Zhang, B. Pearson, Z. Ling, H. Yu, X. Fu, On the security and data integrity of low-cost sensor networks for air quality monitoring, Sensors 18 (2018) 4451.

[78] T. Gebremichael, L. P. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, J. Akerberg, Security and privacy in the industrial internet of things: Current standards and future challenges, IEEE Access 8 (2020) 152351–152366.