IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

# Analysis of Lightweight Security Techniques oor IoT Data and Communication

**Prof. Mohan S. Khedkar[1], Prof. Sandip R. Devkate[2], Prof. Shilpa Chaudhari[3]**
Department of Information Technology[1], Department of Electronics and Telecommunication[2]
Department of Computer Technology[3]
Government Polytechnic Nashik, Maharashtra, India[1]
Matoshree College of Engineering And Research Centre, Nashik, Maharashtra, India[2,3]
mohan_khedkar@hotmail.com[1], sandiprdevkate@gmail.com[2], sawaghulde@gmail.com[3]

**Abstract:** *The Internet of Things (IoT) aims to transform everyday physical objects into an interconnected ecosystem with digital data accessible anywhere and anytime. ''Things'' in IoT are embedded with sensing, processing, and actuating capabilities and cooperate in providing smart and innovative services autonomously. The rapid spread of IoT services arises different security vulnerabilities that need to be carefully addressed. Several emerging and promising technologies and techniques are introduced to improve the security of IoT. This paper aims to provide an up-to-date vision of the current research topics related to IoT security. Initially, we introduce common elements and protocols of IoT to demystify the origins of threats in IoT. Then, we propose a taxonomy of IoT attacks and analyse the security vulnerabilities of IoT at different layers. Subsequently, we provide a comparison of recent security schemes based on emerging solutions including fog computing, edge computing, software-defined networking (SDN), blockchain, lightweight cryptography, homomorphic and searchable encryption, and machine learning. Finally, security challenges are discussed and future directions are highlighted for future interested researchers.*

**Keywords:** Blockchain, edge computing, fog computing, IoT, lightweight cryptography, machine learning, SDN

## I. INTRODUCTION

The Internet of Things (IoT) refers to a growing network of everyday physical objects connected to the Internet. The ultimate goal of IoT is the transformation of Internet-enabled devices to an interconnected ecosystem with digital data accessible anywhere and anytime. The IoT devices ranging from small wearable objects to large machines, equipped with sensors and actuators, smartly perceive their surroundings and perform actions autonomously [1], [2]. According to Cisco, 50 billion of devices are currently estimated to be connected to the Inter- net [3]. These devices are inherently resource-constrained, they have limited memory space, low processing capacity, and computation power. Different enabling technologies such as cloud computing evolve as essential components for the emergence of IoT paradigm [4], as shown in Figure 1. In near future, the IoT data will be produced from billions of devices using provided. The formatter will need to create these components, incorporating the applicable criteria that follow. device-to-device (D2D) interactions where devices will be connected to each other and exchange a massive amount of data through the Internet. The number of connected IoT devices is predicted to grow to 1 trillion by 2025. Accord- Ing to this prediction, the IoT will offer potential economic revenue of $11 trillion per year by 2025 [5]. Consequently, this growth will face several security issues that must be addressed. The security of IoT has attracted significant attention in the academic field. A large number of researchers discussed the security of IoT systems [6]–[20]. Most of the existing surveys investigated relevant security aspects such as attacks, require- ments, and challenges in IoT. However, various emerging technologies and techniques have been recently adopted as promising solutions to improve IoT security. The main goal of this paper is to provide an up-to-date review of the current research topics related to IoT security. Specifically, several security schemes based on different emerging technologies and techniques, namely fog computing, edge computing, SDN,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

blockchain, lightweight cryptography, homomorphic and searchable encryption, and machine learning are evaluated. In addition, a comparison of the studied schemes in terms of security and performance is provided. Accordingly, the key contributions of this work arethe following.

- Introduce common elements, protocols, and applications of IoT systems.
- Provide a taxonomy of IoT attacks to identify the security vulnerabilities of IoT systems.
- Present emerging solutions that address the IoT security issues and provide a comparison of recent research works based on these solutions.
- Discuss security challenges and future directions for the IoT systems.

Figure 2 shows the organization of the paper. In Section 2, we explore relevant studies that address IoT security. In Section 3, we present three-layered IoT architecture and introduce common elements, protocols, and applications of IoT. The security threats of each layer of IoT are analyzed in Section 4. Emerging security solutions used in IoT are discussed in Section 5. In Section 6, we report the security challenges and highlight future directions for IoT security. We conclude our study and provide future work in Section 7.

## II. Related Surveys

This section explores recent relevant studies that cover different aspects of IoT security. The main security aspects discussed in the reviewed surveys are summarized in Table 1. Adat and Gupta [6] presented the history, statistics and architecture of IoT. They discussed the security features according to IoT layers and provided a taxonomy of security issues and challenges in IoT systems. Moreover, they analyzed existing defense mechanisms including intrusion detection systems. Kouicem *et al.* [7] pinpointed the security requirements and challenges in different IoT applications such as smart grids, smart cities, healthcare, transportation, and manufacturing. They classified the security solutions into classical and new approaches. The classical approaches cover confidentiality, privacy, and availability, while new solutions include SDN- based and blockchain-based schemes. The authors also focused on context-awareness and safety related to IoT security. Lu and Xu [8] discussed the security issues at four- layered IoT architecture and provided a taxonomy of different attacks. They described the security measures for WSNs and RFIDs and classified the security schemes into three categories: host identity protocol-based schemes, datagram transport layer security-based schemes, and capability-based access control schemes. Noor [9] presented the security attacks and challenges at perception, network, and application layers of IoT. They reviewed a large number of proposed security schemes that address authentication, encryption, trust management, and secure routing. The authors also highlighted the simulation tools involved in the reviewed schemes. Tewari and Gupta [10] addressed the security issues of three-layered IoT architecture. They described the security designs of IoT protocols and discussed the security challenges of enabling technologies such as cloud and RFID. Moreover, the authors presented key factors that must be achieved to provide a trustworthy IoT network and high- lighted the impact of IoT in different fields. Harbi *et al.* [11] analyzed several security attacks that may be launched in IoT systems. They provided a tax- onomy of security requirements including data security, communication security, and device security. Furthermore, the authors described many security schemes proposed for various IoT applications and pinpointed major security challenges. Hassija *et al.* [12] discussed the security issues of various IoT applications and highlighted possible attacks on IoT lay- ers. They reviewed proposed solutions based on blockchain, fog computing, edge computing, and machine learning to secure IoT environments. Meneghello *et al.* [13] classified the security requirements for IoT into three levels, namely information level, access level, and functional level. They reported the vulnerabilities and possible attacks at different IoT layers. They presented the security mechanisms designed to satisfy security in IoT and focused on security designs of popular IoT communication protocols. Neshenko*et al.* [14] focused on IoT vulnerabilities in the context of various dimensions. They provided a compre- hensive taxonomy of IoT vulnerabilities including layers (security of each IoT layer), attacks (performed on exploited vulnerabilities), countermeasures (available techniques to mitigate vulnerabilities), security impact (impact of vulner- abilities on security requirements), and situational aware- ness capabilities (available techniques to capture malicious activities). Hamad *et al.* [15] discussed common security attacks that target IoT systems. They identified the security requirements to overcome such attacks in different IoT applications. They reviewed proposed schemes that address security services

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

such as access control, integrity, authentication, confidentiality, and privacy. Mahbub [16] identified the security concerns of various IoT applications. They introduced threat modeling frame- works that can be used in the security designing of IoT sys- tems. They reported the security attacks at sensing, network, middleware, and application layers. Moreover, the authors presented security techniques using cryptography, fog computing, edge computing, and machine learning to solve IoT attacks. Mrabet *et al.* [17] proposed new IoT architecture that includes five layers; perception, network, transport, application, and cloud layer. They analyzed the security threats at different IoT architectural layers and discussed open challenges to secure IoT systems.

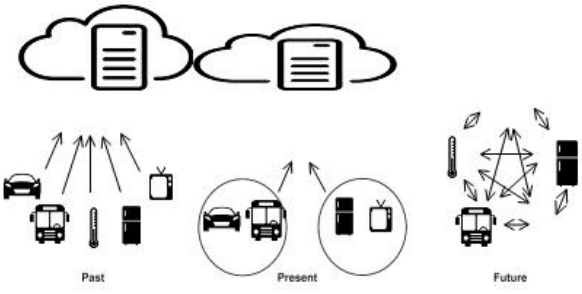


FIGURE 1. Evolution of IoT

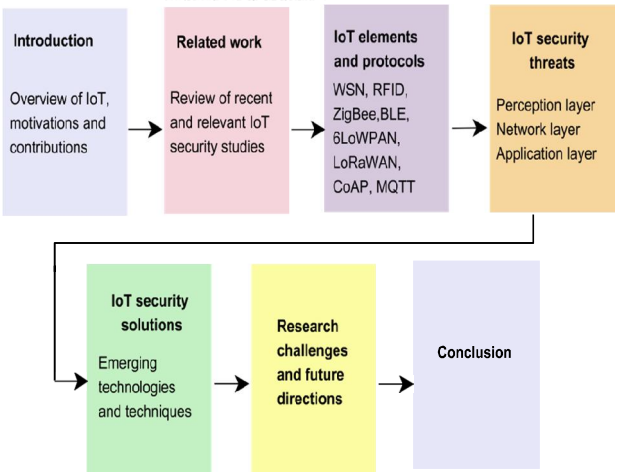


FIGURE 2. Organization of the paper.

Malhotra et al. [18] presented a taxonomy of IoT secu- rity attacks, anomalies, and vulnerabilities. They focused on learning-based techniques to provide intelligent intrusion detection IoT systems. In addition, the authors highlighted critical issues that need to be addressed to secure IoT envi- ronments. Thakor et al. [19] focused on evaluating lightweight cryp- tographic algorithms for constrained IoT devices. They clas- sified the lightweight cryptographic algorithms into two main classes; symmetric and asymmetric, and analyzed the hardware and software performance metrics of symmetric lightweight cryptographic algorithms. Furthermore, they dis- cussed several challenges to provide a trade-off between cost, performance, and security.

Jayalaxmi et al. [20] explored the security issues and attacks at different layers of industrial IoT (IIoT). They presented several frameworks that provide various secu- rity requirements for smart factory systems. Moreover, they investigated intrusion detection techniques proposed for IIoT devices. Table 2 presents the contributions of the aforementioned studies and our survey. According to Table 2, the state-of-the- art surveys covered several research topics in IoT. However, our survey extends the previous researches by introducing emerging solutions that promise to enhance the IoT security. In addition, it provides an objective comparison of recent security schemes based on the emerging solutions by considering relevant key parameters

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

## II. Overview Of IoT

This section provides a brief overview of IoT systems. It aims to present characteristics of IoT elements, protocols, and applications to understand the origins of security risks and set a common ground for the security threats that will be discussed in the next section.

| Related survey | Year | IoT layers | Security aspects |
|---|---|---|---|
| Adat *et al.* [6] | 2017 | Perceptual, network, support, application | Security features of each IoT layer<br>Security issues and challenges<br>IoT intrusion detection systems |
| Kouicem *et al.* [7] | 2018 | - | Security requirements and challenges |
| Lu *et al.* [8] | 2018 | Sensing, network, middleware, application | Security issues of each IoT layer |
| Noor *et al.* [9] | 2018 | Perception, network, application | Security attacks and challenges<br>IoT security schemes |
| Tewari *et al.* [10] | 2018 | Perception, middleware, application | Security issues of each IoT layer<br>Security designs of IoT protocols<br>Security issues of IoT enabling technologies |
| Harbi *et al.* [11] | 2019 | Perception, network, application | Security attacks and requirements<br>Security solutions and challenges |
| Hassija *et al.* [12] | 2019 | Sensing, network, middleware, application | Security issues of IoT applications<br>Security attacks of IoT layers<br>Security solutions and challenges |
| Meneghello *et al.* [13] | 2019 | Edge, access, application | Taxonomy of security requirements and attacks<br>Security mechanisms and threats of IoT protocols |
| Neshenko *et al.* [14] | 2019 | Devices, network subsystems, application | IoT vulnerabilities in context of various domains |
| Hamad *et al.* [15] | 2020 | Physical, information, application | Security attacks and requirements<br>Security solutions and open issues |
| Mahbub [16] | 2020 | Sensing, network, middleware, application | Security concerns of IoT applications<br>Threat modelling frameworks<br>Security attacks at IoT layers<br>Security techniques and challenges |
| Mrabet *et al.* [17] | 2020 | Perception, network, transport, application, cloud | Security threats and solutions<br>Open issues and challenges |
| Malhotra *et al.* [18] | 2021 | Perception, network, support, application | Taxonomy of attacks, anomalies, and vulnerabilities<br>Open issues and challenges |
| Thakor *et al.* [19] | 2021 | - | Lightweight cryptographic algorithms<br>Security challenges |
| Jayalaxmi *et al.* [20] | 2021 | Perception, network, support, application | Security attacks and requirements<br>Intrusion detection techniques |

- : not discussed

TABLE 1. Summary of related surveys

| Contribution | [6] | [7] | [8] | [9] | [10] | [11] | [12] | [13] |
|---|---|---|---|---|---|---|---|---|
| IoT architecture | ✓ | × | ✓ | ✓ | ✓ | × | ✓ | ✓ |
| IoT applications | × | ✓ | ✓ | × | ✓ | × | ✓ | × |
| IoT protocols | ✓ | × | × | × | ✓ | × | × | ✓ |
| IoT attacks | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Security requirements | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| Fog computing | × | × | × | × | × | × | ✓ | × |
| Edge computing | × | × | × | × | × | × | ✓ | × |
| SDN | × | ✓ | × | ✓ | × | × | × | × |
| Blockchain | × | ✓ | × | ✓ | × | × | ✓ | × |
| Lightweight cryptography | × | × | × | × | × | × | × | ✓ |
| Homomorphic encryption | × | × | × | × | × | × | × | × |
| Searchable encryption | × | × | × | × | × | × | × | × |
| Machine learning | × | × | × | × | × | × | ✓ | × |
| Challenges and future directions | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ |

TABLE 2. Contributions of related surveys and our survey.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

### 2.1 IOT Architecture

The architecture of IoT is not standardized; typical IoT architecture has three layers: perception, network, and application [21], as shown in Figure 3.

### A. Perception Layer

The perception layer includes different physical IoT devices; it is responsible for interaction among devices and collection of IoT data. Data collection is performed using smart devices such as radio frequency identification (RFID) tags and sensors. RFID technology is a major element of IoT due to its identification, tracking, and monitoring of objects [22]. An RFID system consists of a radio signal transponder (tag) that storesa unique identity of an object and a tag reader that identifies the object through radio waves. The tag reader transfers the identification number to a computer to track and monitor the object as shown in Figure 4. Wireless sensors play an essential role in IoT by providing sensing and communicating services [23]. A Wireless sensor network (WSN) consists of a large number of intelligent sensors deployed in remote environments to sense and collect

| Contribution | [14] | [15] | [16] | [17] | [18] | [19] | [20] | Our survey |
|---|---|---|---|---|---|---|---|---|
| IoT architecture | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ |
| IoT applications | × | ✓ | ✓ | × | × | × | × | ✓ |
| IoT protocols | ✓ | ✓ | ✓ | ✓ | × | × | × | ✓ |
| IoT attacks | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| Security requirements | × | ✓ | × | ✓ | × | × | ✓ | ✓ |
| Fog computing | × | × | ✓ | × | × | × | × | ✓ |
| Edge computing | × | × | ✓ | × | × | × | × | ✓ |
| SDN | × | × | × | × | × | × | × | ✓ |
| Blockchain | × | ✓ | × | × | × | × | ✓ | ✓ |
| Lightweight cryptography | × | × | ✓ | × | × | ✓ | × | ✓ |
| Homomorphic encryption | × | ✓ | × | × | × | × | × | ✓ |
| Searchable encryption | × | × | × | × | × | × | × | ✓ |
| Machine learning | × | × | ✓ | ✓ | ✓ | × | ✓ | ✓ |
| Challenges and future directions | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

TABLE 3. Cont.

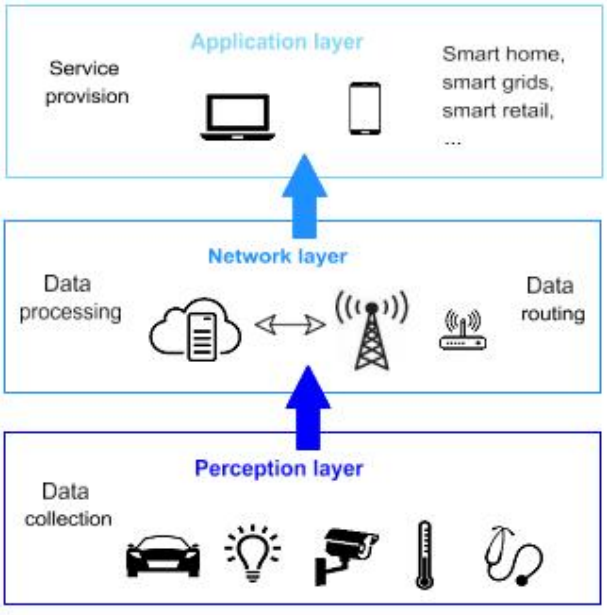


FIGURE 3. Three-layered IoT architecture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252


FIGURE 4. RFID system.

data such as temperature, humidity, vibration, etc. Sensed data are transmitted through one or multi-hop to a gate-way/base station as depicted in Figure 5.

B. Network Layer

The network layer processes the collected data provided by the perception layer and stores or sends the data to the appli- cation layer. It is the most important layer of IoT architecture because it integrates various communication technologies that enable the connectivity of IoT devices. The widely used

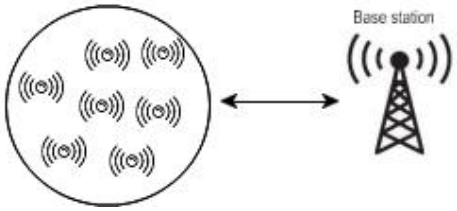


FIGURE 5. WSN architecture.

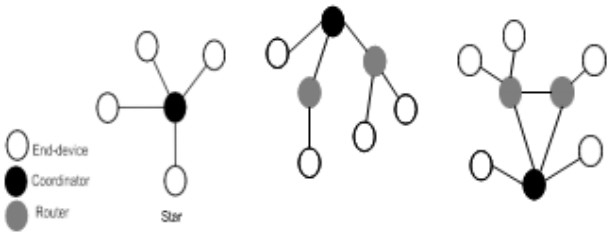


FIGURE 6. ZigBee topologies.

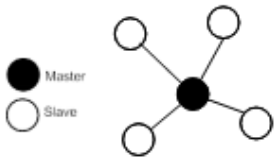


FIGURE 7. BLE topology.

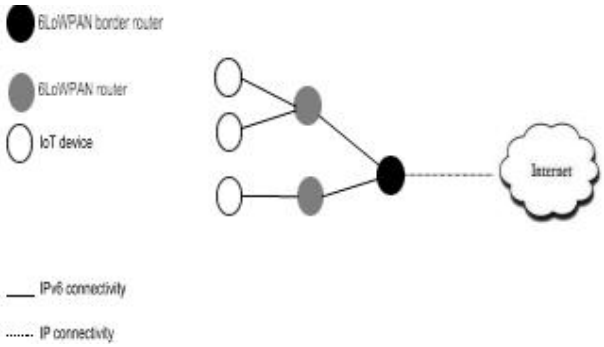


FIGURE 8. 6LoWPAN architecture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

### C. Application Layer

The application layer receives the data from the network layer and provides the required services to IoT users. It supports a large variety of applications such as smart home, smart retail, smart grids, etc. The most common application protocols are constrained application protocol (CoAP) and message queuing telemetry transport (MQTT).

Since IoT devices are resource-constrained, HTTP proto- col is not suitable for low-power devices due to its complexity. CoAP was designed to include features of HTTP dedicated to IoT devices. As demonstrated in Figure 10, CoAP is a messaging protocol based on representational state transfer (REST) architecture [32]. It has four message types: confirmable, non-confirmable, acknowledgment and reset. It provides features that are not available on HTTP such as push notification (i.e., the server sends a notification to the device) and resource discovery (i.e., the server can store the list of devices). MQTT is a lightweight messaging protocol that provides the connectivity of networks and users with applications. It is based on publish/subscribe architecture where the system consists of three main components: publishers, subscribers, and a broker as presented in Figure 11. In the context of IoT, publishers are embedded devices that send data to the broker and subscribers are applications servers. A comparison of IoT application layer protocols is provided in Table 5.

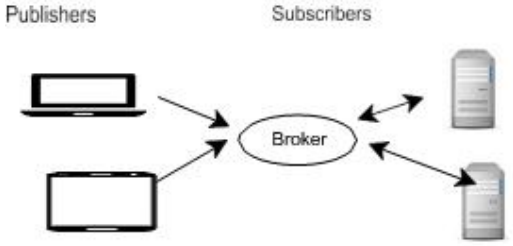


FIGURE 11. MQTT architecture.

### 2.2 IOT Applications

The IoT provides a large number of applications to enhance people's daily lives and activities. Figure 12 shows potential examples of IoT applications

| Wireless technology | ZigBee | BLE | 6LoWPAN | LoRaWAN |
|---|---|---|---|---|
| Topology | star, tree, mesh | Star | Star, mesh | star, star-of-star |
| Range | 10-20m | <100m | 10-20m | 3-5km |
| Application | smart home<br>smart meters<br>smart healthcare | smart vehicule | smart home<br>smart agriculture<br>smart industry | smart city |
| Interoperability | No | No | Yes | Yes |
| Security | Yes | Yes | No | Yes |
| Scalability | Yes | No | Yes | Yes |

TABLE 4. Comparison of IoT wireless technologies.

| Application protocol | CoAP | MQTT |
|---|---|---|
| Transport layer | UDP | TCP |
| REST | Yes | No |
| Request/response | Yes | No |
| Publish/Subscribe | Yes | Yes |
| Security | DTLS | SSL |

TABLE 5. Comparison of IoT application protocols

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252


FIGURE 12. IoT applications.

- **SMART HOME:** Encompasses a collection of smart devices (e.g., smart lock, baby monitor, fire detector) deployed at home and locally communicate over wireless channels. Home devices can be remotely accessed through a home gateway.
- **SMART HEALTHCARE:** Enables collection, transmission, and storage of patients' physiological information. For instance, a patient's heart rate can be collected by medical sensors and transmitted to a hospital server for diagnosis and tracking purposes.
- **SMART TRANSPORTATION:** Includes a large number of smart vehicles which can communicate with each other (vehicle-to-vehicle), to the outside station (vehicle-to-infrastructure), and to pedestrians (vehicle- to-pedestrian) over wireless networks. A smart vehicle can detect current traffic status, manage speed, and exchange data to provide efficient and safe driving.
- **SMART AGRICULTURE:** Allows remote control of temperature, humidity, irrigation, soil moisture, and micro-climate conditions to provide high production/quality and prevent financial losses. In an intelligent farming system, sensors can be attached to animals to track livestock behaviors and health conditions.
- **SMART INDUSTRY:** Known as industrial IoT (IIoT) uses machine-to- machine technology to automate the process of manufacturing with insignificant human intervention. The IIoT aims to better control the production process, data, and issues to provide efficient and reliable final products.
- **SMART RETAIL:** Permits the tracking of products in warehouses or during traveling. Sensors can be attached to a retail item to track the product status. Various smart shopping systems were developed to provide intelligent services for customers and thus gain more clients.
- **SMART GRID:** Is a common application of IoT that measures, monitors, and manages electricity consumption. It enables efficient and reliable electricity management, provides energy-saving, and reduces powers grids issues/failures.

### 2.3 Lessons Learned

IoT systems are empowered with diverse elements and proto- cols which allow to continually expand possible attacks and introduce several vulnerabilities. IoT integrates the Internet with the physical world to provide various intelligent applications, from smart homes to smart grids. Consequently, the IoT devices can be targeted by adversaries to launch potential attacks. Therefore, it is very necessary to analyze the attack surfaces of IoT systems to satisfy the desired level of security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

## III. Security Threats Of IoT

In this section, we provide a taxonomy of IoT attacks based on levels, purposes, and countermeasures as shown in Figure 13. Then, we focus on the security vulnerabilities of IoT at the three layers. Levels: Examine the security issues of IoT at the three layers. Perception layer threats address the security attacks within major elements of IoT such as WSNs and RFID. Net- work layer threats analyze vulnerabilities of the aforementioned communication protocols. Application layer threats include attacks related to IoT software and end-user devices. Purposes: Evaluate the impacts of security attacks on IoT systems. The main purposes of IoT attacks are the following:

- Access to communication.
- Reveal or alter data.
- Disable required services.
- Drain device resources.

Countermeasures: Consist of the security requirements to mitigate the identified purposes of IoT attacks. This class includes communication security, data security, and device security. IoT communications can be secured by providing authentication, access control, and non-repudiation. To protect data, relevant security requirements such as confidentiality, privacy, and integrity must be considered. Other fundamental requirements including trust and availability of IoT devices are needed in different environments. For more details about these security requirements, the reader is referred to our previous survey [11].

### 3.1 Perception Layer Threats

The limited resources and heterogeneous nature of IoT devices make them vulnerable to various security attacks. WSNs are generally deployed in harsh and unattended environments, and thus, they are prone to several attacks. Common security attacks of WSNs are sinkhole, blackhole, wormhole, sybil, denial of service (DoS), node capture, and node injection attack [11]. Brief descriptions of these security attacks are provided in Table 6. Similar to the WSN, the RFID networks are susceptible to different types of attacks including spoofing, cloning, and sniffing attacks (See Table 6). The IoT inherits the security threats of WSNs and RFID because they are vital elements of IoT networks.

### A. Network Layer Threats

ZigBee protocol implements security mechanisms includ- ing advanced encryption standards with cipher block chaining message authentication code (AES- CCM) and message integrity code (MIC) to provide confidentiality, authentication, and integrity. The ZigBee security is based on three keys: a link key (for unicast communications), a network key (for broadcast communications), and a master key (for link key and network key generation). As mentioned in [33], the mas-ter key is installed in the device during the manufacturing process. The link key can be generated using key transport or key establishment methods, while the network key can be acquired using the key transport method. As the master key is stored on the device, an attacker can read it from the memory after the node capture attack's success. Another possible attack presented in [34] that aims to drain the energy of ZigBee nodes. The authors in [35] evaluated the vulnerability of the ZigBee network against sinkhole attack. In [36], the authors showed that three ZigBee- based smart light systems are susceptible to several types of attacks such as denial of service (DoS), network key extraction, and code injection attacks. BLE protocol provides confidentiality and authentication using the 128- bits AES-CCM algorithm as ZigBee. The symmetric key is generated using the pairing procedure. First, the IoT devices exchange necessary information for authentication. Second, they generate and exchange temporary keys based on a pairing method. Finally, the device may exchange and store common keys to be used for further communications. The pairing methods have several security issues including eavesdropping, man-in-the- middle (MTM), and brute force attacks as presented in [37] and [38]. Latter, a new pairing procedure has been designed based on elliptic curve diffiehellman (ECDH).

However, the authors in [39], [40] demonstrated that it has similar problems. In [41], the authors presented other types of attack such as data leakage and DoS attack that can be performed in a BLE-based smart door lock system. 6LoWPAN protocol enables resource-constrained device to connect to the Internet using IPv6 addresses. It uses IPv6 header

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

compression and packet fragmentation to reduce transmission overhead. However, it does not provide confidentiality, authentication, or integrity preservation. An adversary can inject fake fragments with the header of a legitimate fragment; the receiver node uses the injected fragment in packet reassembly causing the construction of a corrupted packet. Consequently, the buffer space of the receiver node will be reserved and not be able to receive further fragments [42]. Consecutive repetitions of fragment injection attack lead to a DoS attack [43]. RPL defines three security modes: unsecured, preinstalled, and authenticated in the packet header. The unsecured mode is adopted when security is provided by the MAC layer. In preinstalled mode, preinstalled keys are used to join the RPL network. The authenticated mode is not fully defined by the specification of RPL. If security is not provided at any layer, an attacker can perform different types of attacks in the RPL network. A sinkhole, blackhole, flooding, Sybil, and DoS attacks against RPL networks are presented in [43]–[45]. The security of 6LoWPAN relies on securing communications at the MAC layer or APP layer. The security of the MAC layer is provided using AES-CCM and MIC. However, the specification of IEEE 802.15.4 does not define the key management procedure. LoRaWAN protocol adopts 128-bits AES algorithm and MIC to guarantee data confidentiality and integrity. When an IoT device is allowed to join the LoRaWAN network, the network server sends two session keys, namely network session key and application session key, to the end device. These keys are used for data encryption/decryption and MIC. The main security weakness of the LoRaWAN protocol is related to key management; an intruder can access session keys using a side channels attack since they are stored on the end device. Moreover, the end devices share the same session keys to secure multicast communications. This enables the intruder to read the keys from one node and thus reveal communications of other devices [46]. The authors in [47] demonstrated that the LoRaWAN network is vulnerable to DoS and MTM attacks. Table 7 summarizes the security threats of IoT communi-cation protocols.

### B. Application Layer Threats

CoAP is the application layer protocol that enables resource-constrained devices to achieve RESTful interactions. Since CoAP is built on UDP transport protocol, data- gram TLS (DTLS) was proposed to provide confidentiality, authentication, and integrity preservation in CoAP proto- col [48]. However, the limitations of DTLS can be considered as security threats of CoAP protocol [49]. Secure socket layer (SSL) was introduced to secure data transfer using the MQTT protocol. SSL uses an asymmetric cryptographic technique to encrypt/decrypt the data. How- ever, it is stills prone to MTM attack [50]. An extension of MQTT called secure MQTT (SMQTT) was proposed to provide security during data transfer [51]. The publishers and subscribers register to the broker and get a secret key. This key is used for data encryption and decryption performed by publishers and subscribers, respectively. However, the key generation and encryption algorithms are not standardized. In IoT, software vulnerabilities and users devices can be exploited by attackers. An adversary can impersonate or manipulate legal users to gain access to IoT systems by injecting malicious software. The lack of user authentication has led to several IoT attacks such as Bashlite and Mirai attacks [52].

### C. Lessons Learned

IoT devices are inherently resource-constrained and generally deployed in unattended environments. In addition, they usu- ally communicate with each other through wireless channels. Consequently, an intruder can remotely control the interconnected objects or intercept private information from the communications. Therefore, there is a need to explore the security vulnerabilities of IoT systems to increase awareness about the consequences of potential threats and possible attacks.

## IV. Emerging Security Solutions

In this section, we discuss the emerging computing technologies and techniques proposed in the literature to increase the level of security in IoT. We also provide a comparison of recent research works based on these technologies and techniques in terms of attack level (i.e., IoT layer targeted by the adversary), countermeasures (i.e., data security, communication security, and device security), and performance (i.e., computation cost, communication cost, and storage cost). The selected comparison parameters are usually considered to design security mechanisms suitable for IoT systems. A summary of the proposed security schemes for IoT.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

### 4.1 Fog Computing-Based Solutions

Fog computing has been introduced as a new paradigm to extend (not to replace) the computational resources of Cloud computing. It provides storage, computation, and networking/communication at the edge of the network [108]. Fog computing architecture consists of fog nodes deployed close to IoT devices and connected to the cloud server as shown in Figure 14. The fog architecture helps to reduce the amount of data exchanged between the IoT devices and the cloud infrastructure. Fog computing supports mobility, location awareness, low latency, heterogeneity, scalability and thus can be perfectly adopted into real-time or latency-sensitive IoT applications. Since IoT devices have limited resources, fog nodes can provide various security requirements to secure IoT environments. To achieve authentication, Alrawais et al. [53] focused on securing communications in fog-assisted IoT environments using ciphertext-policy attribute-based encryption (CP-ABE). They analyzed the security of the proposed scheme against different attacks and provided a comparison with a certificate-based method. Gope [54], the authors pro- posed three lightweight authentication schemes for device- to-device communications that can be used in various IoT applications. The proposed schemes ensure mutual authentication and key agreement and they are efficient in terms of computation cost.

To ensure privacy-preserving, Hu et al. [55] presented a face identification and resolution framework based on fog computing for IoT. The framework is mainly comprised of user devices, fog nodes, and cloud servers. The authors adopted several cryptographic techniques to preserve the personal information of users. Lu et al. [56] addressed privacy-preserving of data aggregation in heterogeneous IoT environments. The aggregated data is filtered by fog nodes, and thus the scheme can resist false data injection attack. Moreover, the proposed scheme can also resist differential attacks. Yang et al. [57] proposed privacy-preserving scheme for IoT location-awareness applications. The authors used bilinear pairing and asymmetric scalar-product preserving encryption to secure the location of mobile devices. Guan et al. [58] employed pseudonym certificates to pre- serve the privacy of sensitive data during data aggregation in fog- enhanced IoT systems. The data aggregation is per- formed by fog nodes, while the pseudonym certificates are generated and updated by two certification authorities. The authors evaluated the proposed scheme in terms of computation complexity and communication overhead. To guarantee confidentiality, Boakye-Boateng et al. [59] adopted one-time pad (OTP) and random number genera- tors (RNG) to encrypt the collected data in WSN in the context of IoT. The security of OTP is based on the strength of RNG. The proposed scheme is computationally efficient because it requires lightweight operations to perform the data encryption. In [109], the authors enhanced the security of medical data in healthcare IoT applications using fog.

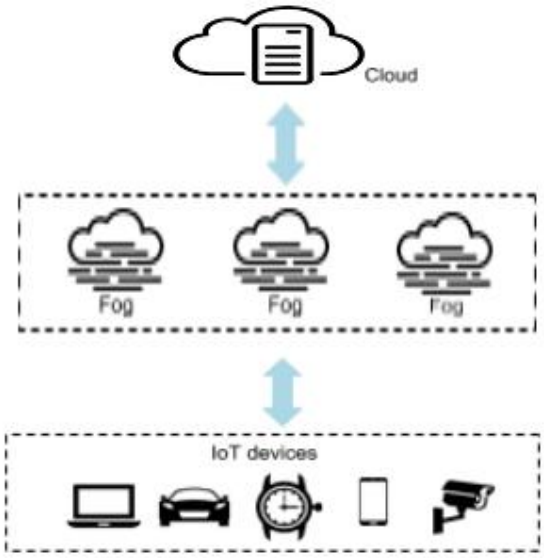


FIGURE 14. Fog computing architecture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

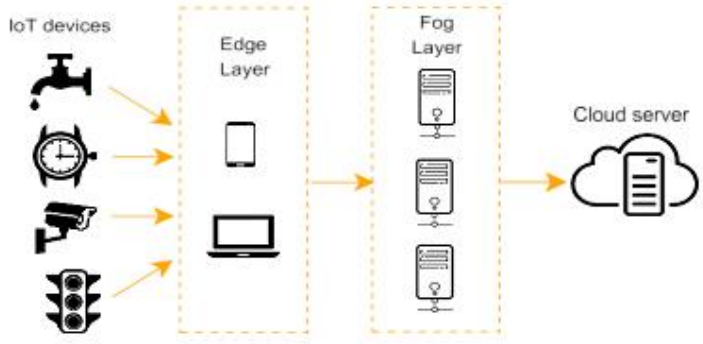


FIGURE 15. Edge computing architecture.

computing. The proposed architecture allows patients' data to be analyzed and secured by fog-based gateways, it also supports the MQTT protocol and M2M communications. The authors provided a comparison to cloud-based architecture to highlight the benefits of fog computing. How- ever, they did not define the encryption technique used for medical data security. Zhang [60] proposed a key management scheme based on contributory broadcast encryption where fog nodes negotiate a public key with an end-user device. This latter sends an encrypted session key to the fog nodes to achieve confidentiality of further communications. The authors in [61] investigated the IoT data encryption using the CP- ABE technique that involves four algorithms, namely, setup, key generation, encryption, and decryption. They defined a formal security model using game theory and analyzed their proposed scheme based on this model. Table 9 compares the IoT security schemes based on fog computing. It is observed that fog computing can improve the security of IoT systems at perception and network layers. The fog-based security schemes satisfy major requirements such as authentication (i.e., communication security), privacy, and confidentiality (i.e., data security). Moreover, they have acceptable computation cost and communication overhead. However, most of the surveyed articles did not consider the storage cost which is an important parameter fore source-constrained IoT devices.

### 4.2 Edge Computing-Based Solutions

Edge computing is another extension of Cloud computing that provides promising services to edge IoT devices including sensors, actuators, and RFID tags. Both fog computing and edge computing offer the same functionalities to carry out computation tasks closer to IoT devices. The main difference between cloud, fog, and edge computing is the location of computational resources [110]. Edge computing architecture consists of smart IoT devices, edge devices, fog nodes, and cloud server as presented in Figure 15. In an edge-enabled IoT application, the data is pro- cessed within the device itself without being transferred to fog nodes or cloud server [111]. This enhances the performance of the network in terms of communication overhead, decreases the latency of data processing, and improves the security of the IoT application. Mobile edge computing (MEC) is a type of edge computing that extends the capabilities of cloud computing to deploy processing and storage services close to IoT mobile users [112]. Several researchers adopted the edge layer to increase the security of IoT systems by providing crucial security require- ments such as access control, authentication, and privacy- preserving [113]. Cui et al. [62] introduced edge computing to achieve an effective access control for IoT networks. They proposed a proxy- aided CP-ABE scheme where partial decryption computations are maintained by edge devices. The proposed scheme significantly reduces the computational cost com- pared to CP-ABE schemes. Hsu et al. [63] designed an efficient framework to strengthen the security of resource-limited IoT devices using edge computing. The proposed framework is based on an edge device called a security agent which is responsible for performing cryptographic computations to secure communications among IoT devices. Wazid et al. [64] focused on device authentication and key management for securing communication in an edge-based IoT environment. The proposed scheme is based on a lightweight cryptographic hash function and thus, it is efficient in terms of computation cost. In addition, it resists known security attacks. Razaque et al. [65] addressed the detection of digital crimes in industry 4.0 and identification of criminals and evidence of crimes. The proposed scheme is based on edge-cloud computing and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

consists of a detection model and validation model to increase the efficiency and security of industrial forensics.

| Scheme | Attack level | Countermeasure | Performance |
|---|---|---|---|
| [53] | Network layer | Communication security | - Medium computation cost<br>- Low communication cost<br>- Storage cost is not considered |
| [54] | Perception layer | Communication security | - Low computation cost<br>- Medium communication cost<br>- Storage cost is not considered |
| [55] | Network layer | Data security | - Medium computation cost<br>- Medium communication cost<br>- Storage cost is not considered |
| [56] | Network layer | Data security | - Low computation cost<br>- Medium communication cost<br>- Storage cost is not considered |
| [57] | Perception layer | Data security | - High computation cost<br>- High communication cost<br>- Storage cost is not considered |
| [58] | Network layer | Data security | - High computation cost<br>- Medium communication cost<br>- Storage cost is not considered |
| [59] | Network layer | Data security | - Low computation cost<br>- Low communication cost<br>- Storage cost is not considered |
| [60] | Network layer | Data security | - Medium computation cost<br>- Low communication cost |

TABLE 9. Comparison of IoT security schemes based on fog computing

Li et al. [66] investigated the integration of IoT, mobile edge computing, and cloud computing technologies to guarantee data privacy. Their system architecture includes user devices, edge servers, and a public cloud center. The edge servers are located at the edge of the network (i.e., IoT user devices) and perform data aggregation to provide privacy preservation. Table 10 compares the IoT security schemes based on edge computing. The integration of edge computing and IoT technologies enhances the performance of IoT systems in terms of communication overhead by providing data processing and aggregation at the edge layer. Consequently, the security of IoT collected data is improved.

**4.3 Software Defined Networking Based Solutions**

Software-defined networking (SDN) is an emerging computing concept that facilitates network management by separating routing decisions of network elements (e.g., routers, switches, and gateways) and forwarding process. In SDN architecture, the network control operations like forwarding tables and ACL rules are handled by a centralized component called SDN controller, while data forwarding is managed by the network elements as depicted in Figure 16 [7]. The SDN can be an effective solution for achieving several security requirements in IoT systems. In [67], the authors proposed a role-based SDN architecture for IoT environments. Their network model includes three controllers, and thus the communication traffic is distributed. The proposed distributed architecture provides different security properties. Wang et al. [68] proposed an identity-based SDN network to overcome the IoT security threats. The generated identity of the IoT device is based on its IPv6 address and secured using data encryption operation. To provide authentication in heterogeneous IoT networks, Salman et al. [69] presented an identity-based authentication scheme. The proposed scheme has three main components; things, gateway, and SDN controller that is responsible for security management. The formal security verification showed that it is secure against masquerade, man-in- the- middle, and replay attacks.

The authors in [70] introduced the SDN in IIoT to secure real-time data transmission. The proposed encryption method requires lightweight operations such as substitution and per-mutation to provide data confidentiality.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

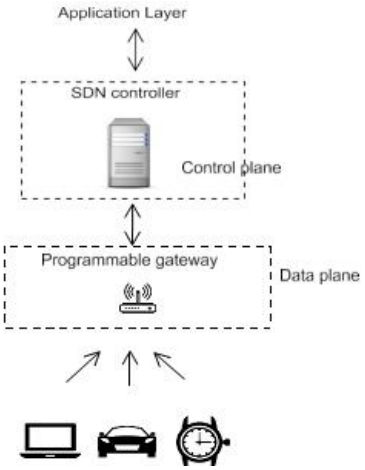


FIGURE 16. Software-defined networking architecture.

| Scheme | Attack level | Countermeasure | Performance |
|---|---|---|---|
| [62] | Perception layer | Communication security | - Low computation cost<br>- Communication cost is not considered<br>- Storage cost is not considered |
| [63] | Perception layer | Communication security | - Medium computation cost<br>- Low communication cost<br>- Storage cost is not considered |
| [64] | Perception and network layer | Communication security | - Low computation cost<br>- Low communication cost<br>- Storage cost is not considered |
| [65] | Network and application layer | Communication security | - Low computation cost<br>- Communication cost is not considered<br>- Storage cost is not considered |
| [66] | Network and application layer | Data security | - Medium computation cost<br>- Low communication cost<br>- Storage cost is not considered |

TABLE 10. Comparison of IoT security schemes based on edge computing

To protect the IoT devices from malicious attacks and mitigate the damage upon an attack, the authors in [71] focused on monitoring anomalous behaviors of IoT devices using SDN gateway with an associated controller. The use of SDN improves the accuracy of attacks detection and enhance the resilience of mitigation action. Bhunia and Gurusamy [72] proposed SDN-based framework. The SDN controller analyzes the communication traffic and determines if it is normal or not. If an attack is detected, it applies rate limiting to reduce the impact of a suspicious attack. The authors considered three different attack scenarios to evaluate the performance of the proposed scheme. Table 11 compares the IoT security schemes based on SDN. It is noticed that SDN technology can provide security for the IoT environments because security mechanisms can be implemented easily by exploiting the SDN con- troller capabilities. However, the additional functions of the SDN controller can decrease the network efficiency due to the high communication overhead caused by the control traffic between the SDN controller and the IoT devices.

### 4.4 Blockchain-Based Solutions

Blockchain is a disruptive technology that has revolutionized the world of cryptocurrency. It is a distributed ledger/database that contains transactions of nodes in a peer-to-peer (P2P) network. A set of transactions are grouped into a single block and validated in a distributed way using a consensus algorithm.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

The consensus process is executed by some nodes in the network called miners. Common consensus algorithms include proof of work (PoW), proof of stake (PoS), and practical byzantine fault tolerance (PBFT).

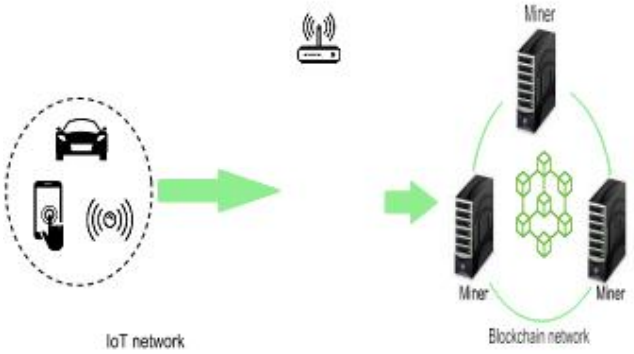


FIGURE 17. Blockchain architecture.

There are two main types of blockchain, namely public (permissionless) and private (permissioned) [114]. Fig- ure 17 demonstrates the architecture of blockchain in IoT.

Due to its prominent features such as decentralization, immutability, transparency, blockchain technology can be applied in several IoT applications. To achieve authentication, Hammi et al. [73] proposed a decentralized mechanism called bubbles of trust based on a public blockchain that implements smart contracts. They considered a network with a large number of heterogeneous smart things where each device can communicate only with devices of its zone (i.e., the bubble). Lin et al. [74] designed an anonymous authentication scheme using blockchain technology and group signature. The proposed scheme enables users to remotely access smart home devices through a gateway node. To verify a transaction, the gateway node executes a smart contract and all valid transactions are added to the blockchain by con- sensus nodes. Hong [75] proposed a decentralized authentication system for sensor networks in the context of IoT. The network architecture consists of two main components; sink node and sensor node, and is organized into levels. Each sensor node should prove its legitimacy to top-level root using the blockchain's Merkle tree. Khalid et al. [76] adopted the public blockchain to provide a secure environ- ment for IoT smart city scenarios. The proposed mechanism

| Scheme | Attack level | Countermeasure | Performance |
|---|---|---|---|
| [67] | Perception and network layer | Data, communication and device security | - Low computation cost<br>- High communication cost<br>- Low storage cost |
| [68] | Perception layer | Device security | - High computation cost<br>- High communication cost<br>- Storage cost is not considered |
| [69] | Network layer | Communication security | - Low computation cost<br>- Medium communication cost<br>- Low storage cost |
| [70] | Network layer | Data security | - Low computation cost<br>- Communication cost is not considered<br>- Storage cost is not considered |
| [71] | Perception layer | Communication security | - High computation cost<br>- Communication cost is not considered<br>- Storage cost is not considered |
| [72] | Network layer | Communication security | - High computation cost<br>- Communication cost is not considered<br>- Storage cost is not considered |

TABLE 11. Comparison of IoT security schemes based on SDN.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

consists of three main phases that include, the initializa- tion phase, device authentication phase, and device-to-device communication phase. In the latter phase, two devices either from the same group or different, communicate with each other after the mutual authentication. Cui et al. [77] pre- sented a hybrid blockchain-based authentication mechanism for remote users in WSN-enabled IoT. The proposed scheme includes a base station, cluster head node, ordinary node, and end-user device. It relies on private blockchain for ordinary node authentication and public blockchain for cluster head node authentication and remote user authentication. The user is identified using its certificate distributed by a certificate authority (CA). To provide secure access control to IoT devices and data, Dorri et al. [78] proposed a blockchain-based architecture for IoT smart home systems. They employed a local blockchain that stores all transactions and is managed by reviewed papers have high communication overhead because they employed local blockchains that are not distributed caus- ing in providing high network traffic between the blockchain and the IoT nodes. Therefore, they should be improved to meet the decentralization property of blockchain technology.

### 4.5 Lightweight Cryptography-Based Solutions

Cryptography is an effective tool to guarantee confidentiality, integrity, and authentication. However, most IoT devices have challenging characteristics such as processing, memory, and battery power. Thus, traditional cryptographic algorithms are not suitable for resource- constrained IoT devices. Recently, lightweight cryptographic primitives were proposed to secure IoT systems. As presented in Figure 18, lightweight crypto- graphic algorithms can be classified into four main classes: block ciphers, stream ciphers, hash functions and elliptic curve cryptography (ECC) [115]. In block ciphers, a block of plaintext is encrypted at a time, while stream ciphers encrypt/decrypt a single bit or byte of plaintext/ciphertext. Hash functions are used to provide data integrity by generating a fixed-length message from an arbitrary-length message. ECC is a lightweight asymmetric cryptographic technique that provides the same level of security as rivest- shamir-adleman (RSA) algorithm with a smaller key size. Several recent research works [81]–[94] adopt lightweight cryptographic techniques to achieve key security require- ments including confidentiality, privacy, integrity, and authentication. Usman et al. [81] presented a lightweight encryption scheme for the IoT. It is a symmetric key block cipher algorithm based on substitution-permutation and feistel networks. The substitution-permutation architecture satisfies Shannon's confusion and diffusion properties. In the feistel architecture, encryption and decryption operations are almost the same. The proposed scheme guarantees data confidentiality and integrity.

## V. Security Challenges And Future Directions

The home miner. To establish a secure trusted system in IoT, the Athough the studied emerging technologies have been intro-authors in [79] investigated the use of blockchain with a reputation mechanism. They introduced a credit-based blockchain to build trust between a service provider and service consumers. The proposed system allows users to consume services by pro- viding obligations as specified by the service provider. These obligations are stored on the blockchain and verified based on the users' reputation information. In [80], the authors evaluated the trustworthiness of sensor data using blockchain technology. Their network architecture consists of a large number of sensors and multiple gateways that maintain the blockchain. The transactions of data including its collection and communication are stored on the blockchain. The block validation is based on a reputation model. duced to provide improved security in different IoT systems, they impose several security challenges that are not properly solved. Table 16 summarizes the main security purposes and challenges of the studied emerging solutions. Most IoT devices are resource-constrained, thus security-enhancing solutions must be computationally efficient. Unfortunately, some emerging technologies and approaches such as blockchain, homomorphic encryption, searchable encryption, and machine learning algorithms require high processing and storage capabilities. Therefore, it is challenging to trade-off between security and performance in IoT infrastructure. The IoT takes advantage of fog computing to achieve different security requirements. Fog nodes cooperate to provide real-time and latency-sensitive services to IoT users. However, a fog node does not have any information about other nodes; it is challenging to ensure that all joining fog nodes are trusted. In fact, users have several fog nodes available to cooperate for guaranteeing IoT services. Thus, it is imperative to select trustworthy fog nodes. The integration of edge computing and IoT technology improves the performance and security of different IoT applications. However, the edge layer is highly sus- ceptible to attacks and can be easily compromised by adversaries. Common edge

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

computing threats include location-based attack and battery draining attack since edge devices are typically resource-constrained. More- over, the deployment of edge nodes at the edge of the network (i.e., at a local level) makes recovery mechanisms challenging. The IoT is rapidly spreading in different domains. Consequently, physical objects of daily life are progressively integrated into various environments, and thus, the scalability of systems needs to be ensured. However, central- ized SDN architecture cannot deal with a large number of IoT devices. In addition, SDN-based solutions are not efficient in high dynamic IoT environments such as vehicular networks. Hence, it is necessary to enforce the scalability property in SDN networks. As IoT devices are tremendously increasing, a massive amount of data including sensitive data are generated and exchanged via the Internet. Blockchain technology efficiently tackles the scalability issue due to its distributed architecture. However, it does not ensure the privacy of transactions and it is prone to data leakage. In fog computing-based architecture, fog nodes are responsible for forwarding data to the cloud. If fog nodes are not trustworthy or compromised by an adversary, they can disclose personal information. Furthermore, various threats can be launched against machine learning algorithms during the training process, and thus exposing sensitive data used by the classifiers. The security of data transmission can be achieved using encryption techniques. The encryption of trans- mitted data prevents intruders from revealing the con- tent of messages. This approach can be applied when the communication parties share encryption/decryption keys. In symmetric encryption (i.e., block ciphers, stream ciphers, and hash functions), the key must be pre-distributed or securely communicated. How- ever, in scalable IoT environments, key management including distribution, agreement, update, and revocation remains a meaningful task.

## VI. Conclusion

In this paper, we provided a new taxonomy of IoT security attacks based on levels, purposes, and countermeasures. Then, we discussed emerging security solutions for IoT based on different technologies and techniques including fog computing, edge computing, SDN, blockchain, lightweight cryptography, homomorphic and searchable encryption, and machine learning. Furthermore, a comparative study of security schemes based on these emerging technologies and techniques in terms of security and performance was provided. Finally, we presented the security challenges related to these emerging solutions and highlighted future directions to enhance the security of IoT. This paper will help researchers to have an idea about the current state-of-the-art of security in IoT to address their respective interests.

## References

**[1].** J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

**[2].** S. Hammoudi, Z. Aliouat, and S. Harous, "Challenges and research directions for Internet of Things," Telecommun. Syst., vol. 67, no. 2,pp. 367–385, 2018.

**[3].** D. Evans, "The Internet of Things: How the next evolution of the internet is changing everything," CISCO White Paper, vol. 1, pp. 1–11, Apr. 2011.

**[4].** R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Comput. Netw., vol. 57, no. 10, pp. 2266–2279, 2013.

**[5].** J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "Unlocking the potential of the Internet of Things," McKinsey Global Inst., Tech. Rep., 2015, vol. 1.

**[6].** V. Adat and B. B. Gupta, "Security in Internet of Things: Issues, chal- lenges, taxonomy, and architecture," Telecommun. Syst., vol. 67, no. 3, pp. 423–441, 2017.

**[7].** D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," Comput. Netw., vol. 141, pp. 199–221, Aug. 2018.

**[8].** Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet Things J., vol. 6, no. 2,pp. 2103–2115, Apr. 2019.

**[9].** M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Comput. Netw., vol. 148, pp. 283– 294,Jan. 2018.

**[10].** A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Future Gener. Comput. Syst., vol. 108, pp. 909–920, Jul. 2018.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

**[11].** Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, ‘‘A review of security in Internet of Things,’’ Wirel. Pers. Commun., vol. 108, no. 1,pp. 325–344, Sep. 2019.

**[12].** V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, ‘‘A survey on IoT security: Application areas, security threats, and solu- tion architectures,’’ IEEE Access, vol. 7, pp. 82721–82743, 2019.

**[13].** F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, ‘‘IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8182– 8201,Oct. 2019.

**[14].** N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, ‘‘Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2702– 2733, 3rd Quart., 2019.

**[15].** S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, ‘‘Realizing an internet of secure things: A survey on issues and enabling technolo- gies,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1372– 1391,2nd Quart., 2020.

**[16].** M. Mahbub, ‘‘Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and pre- emptive architectonics,’’ J. Netw. Comput. Appl., vol. 168, Oct. 2020, Art. no. 102761.

**[17].** H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, ‘‘A survey of IoT security based on a layered architecture of sensing and data analysis,’’ Sensors, vol. 20, no. 13, p. 3625, Jun. 2020.

**[18].** P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, ‘‘Internet of Things: Evolution, concerns and security chal-lenges,’’ Sensors, vol. 21, no. 5, p. 1809, Mar. 2021.

**[19].** V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, ‘‘Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities,’’ IEEE Access, vol. 9,pp. 28177–28193, 2021.

**[20].** P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, ‘‘A taxonomy of security issues in industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges,’’ IEEE Access, vol. 9, pp. 25344–25359, 2021. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ‘‘A sur- vey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

**[21].** X. Jia, Q. Feng, T. Fan, and Q. Lei, ‘‘RFID technology and its applications in Internet of Things (IoT),’’ in Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Apr. 2012, pp. 1282– 1285.

**[22].** M. Kocakulak and I. Butun, ‘‘An overview of wireless sensor networks towards Internet of Things,’’ in Proc. IEEE 7th Annu. Comput. Commun.Workshop Conf. (CCWC), Jan. 2017, pp. 1–6.

**[23].** Zigbee Document 053474r13, Z. Specification, ZgBee Standards Org., USA, 2006.

**[24].** Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks, I. W. Group, IEEE Standard802.15.4, vol. 802, no. 4, 2003, p. 2003.

**[25].** J. Li, X. Zhu, N. Tang, and J. Sui, ‘‘Study on ZigBee network architecture and routing algorithm,’’ in Proc. 2nd Int. Conf. Signal Process. Syst.,vol. 2, Jul. 2010, pp. V2-389–V2-393.

**[26].** Bluetooth Core Specification Version 4.0, Specification Bluetooth Syst., USA, vol. 1, 2010, p. 7.

**[27].** G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, ‘‘Transmission of IPv6 packets over IEEE 802.15. 4 networks,’’ Internet Proposed StandardRFC, vol. 4944, p. 130, Sep. 2007.

**[28].** G. Mulligan, ‘‘The 6LoWPAN architecture,’’ in Proc. 4th Workshop Embedded Networked Sensors (EmNets), 2007, pp. 78–82.

**[29].** T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. K. Alexander, RPL: IPv6 Routing Pro- tocol for Low-Power and Lossy Networks, document RFC 6550, 2012, pp. 1–157.

**[30].** Lorawan 1.1 Specification, Tech. Specification, L. Alliance, USA, 2017.

**[31].** Z. Shelby, K. Hartke, and C. Bormann, The Constrained Application Protocol (COAP), document RFC 7252, 2014.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

**[32].** T. Zillner and F. Eichelberger, ‘‘ZigBee smart homes: A hacker’s open house,’’ in Proc. CRESTCon Conf., 2016.

**[33].** X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, ‘‘Ghost- in-ZigBee: Energy depletion attack on ZigBee-based wireless networks,’’ IEEE Internet Things J., vol. 3, no. 5, pp. 816–829, Oct. 2016.

**[34].** L. Coppolino, V. D’Alessandro, S. D’Antonio, L. Levy, and L. Romano, ‘‘My smart home is under attack,’’ in Proc. IEEE 18th Int. Conf. Comput.Sci. Eng., Oct. 2015, pp. 145–151.

**[35].** P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, ‘‘Insecure to the touch: Attacking ZigBee 3.0 via touchlink commission- ing,’’ in Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw., Jul. 2017, pp. 230–240.

**[36].** M. Ryan, ‘‘Bluetooth: With low energy comes low security,’’ in Proc. 7thUSENIX Workshop Offensive Technol. (WOOT), 2013, pp. 1–7.

**[37].** A. Y. Lindell, ‘‘Attacks on the pairing protocol of Bluetooth v2. 1,’’ BlackHat USA, Las Vegas, NV, USA, Tech. Rep., 2008.

**[38].** W. K. Zegeye, ‘‘Exploiting Bluetooth low energy pairing vulnerability intelemedicine,’’ Int. Found. Telemetering, USA, Tech. Rep., 2015.

**[39].** T. Rosa, ‘‘Bypassing passkey authentication in Bluetooth low energy,’’ IACR Cryptol. ePrint Arch., vol. 2013, p. 309, May 2013.

**[40].** M. Ye, N. Jiang, H. Yang, and Q. Yan, ‘‘Security analysis of Internet- of- Things: A case study of August smart lock,’’ in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), May 2017, pp. 499–504.

**[41].** R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, ‘‘6LoWPAN fragmentation attacks and mitigation mechanisms,’’ in Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw., 2013, pp. 55–66.

**[42].** A. Rghiout, A. Khannous, and M. Bouhorma, ‘‘Denial-of-service attacks on 6LoWPAN-RPL networks: Issues and practical solutions,’’ J. Adv. Comput. Sci. Technol., vol. 3, no. 2, pp. 143–153, 2014.

**[43].** P. Pongle and G. Chavan, ‘‘A survey: Attacks on RPL and 6LoWPAN in IoT,’’ in Proc. Int. Conf. Pervas. Comput. (ICPC), Jan. 2015, pp. 1– 6.

**[44].** A. Mayzaud, R. Badonnel, I. Chrisment, and I. G. Est-Nancy, ‘‘A tax- onomy of attacks in RPL-based Internet of Things,’’ Int. J. Netw. Secur.,vol. 18, no. 3, pp. 459–473, 2016.

**[45].** R. Miller, ‘‘LoRa security: Building a secure LoRa solution,’’ MWR Labs,White Paper, 2016.

**[46].** X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, ‘‘Security vulner- abilities in LoRaWAN,’’ in Proc. IEEE/ACM 3rd Int. Conf. Internet-of- Things Design Implement. (IoTDI), Apr. 2018, pp. 129– 140.

**[47].** J. Granjal, E. Monteiro, and J. S. Silva, ‘‘Security for the Internet of Things: A survey of existing protocols and open research issues,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, Aug. 2015.