JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

Communication Technologies, Smart Home Solution and Security Trends in Internet of Things

Navdeep Lata[1], Dr. Raman Kumar[2]

[1]Research Scholor, Department of Computer Scicence & Engineering, I.K.Gujral Punjab Technical University, Kapurthala, Punjab, India. Email-id: ernavdeeplata@gmail.com

[2] Assistant Professor, Department of Computer Scicence & Engineering, I.K.Gujral Punjab Technical University, Kapurthala, Punjab, India. Email-id: er.ramankumar@aol.in

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

Abstract:

Connectivity is the heart of Internet of Things (IoT). Massive growth has been seen in communication technology that has taken the Internet to the masses. These advancements in communication technology and low-power wireless technology form Internet of Things (IoT). Now, IoT is recognized as a global network of devices, networks, things, and machines. Small devices such as RFID, NFC, Bluetooth, sensors act as a backbone of IoT. These connectivity-increasing devices form IoT applications that are becoming part of daily life. The adoption of this technology is transforming the industrial as well as social workflow. Each communication technology plays its own role in terms of range, bandwidth, power consumption, cost, speed and network requirements that will deploy the specific IoT applications. Security is also a major concern. This paper presents communication technologies, namely, RFID, NFC, Bluetooth, ZigBee, cellular and Wi-Fi with their role in IoT applications. Security Challenges faced by these communication technologies are also presented in this paper. Additionally, a smart home solution has been presented in terms of technology and security. Further security trends in IoT are also presented.

Keywords: IoT; Wireless; Security; Communication Technologies; Smart Home.

1 Introduction

Internet of Things (IoT) is enabling opportunities in every field either industrial or domestic by connecting devices through the Internet. IoT is growing rapidly so that it will play a major role in future technology. During this pandemic time of COVID-19, there is a higher demand for IT technology in education, health services, business, etc., where everyone needs Internet connectivity through any type of device everywhere that can be fulfilled by IoT. IoT is also known as a global network of devices. In the future, the industrialist will invest in IoT for redesigning industry workflows and optimizing machinery usage, cost, and to increase revenue. For example, John Deere is already using IoT- enabled tracking system to improve efficiency[53]. Network communication technologies and communication protocols are primarily exploited by IoT. These technologies and protocols support networking operations required in IoT systems. Due to the advancement in micro controller and communication technologies, IoT is growing rapidly with the support of Wireless Sensor Network (WSN). These tiny sensing devices sense the various parameters concerned with specific applications and store these parameters temporarily. Then, this captured information is transferred to electronic devices through communication technology for processing[66]. The major communication enabling technologies of IoT are NFC, RFID, Bluetooth, and Wi-Fi. Each technology has its working capacity in terms of data transfer, storage and security. However, the RFID tag plays an important role in IoT to identify the objects attached to the RFID tag. So, the number of devices connecting to the Internet is increasing day-by-day which leads to various challenges such as object identification, locating device, authentication, management, security, etc. A review of communication technologies contributing to IoT has been also presented by Roselli et al.[82]. This paper represents the communication technologies that enable communication through IoT with their

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452
security challenges. A comparison has also been done between these communication technologies based on some parameters.

2 The Vision of IoT

After Wireless Sensor Network (WSN), IoT is a kind of new generation of Information Technology. In 1991 Kevin Ashton has formed a term Internet of Things (IoT) [87]. IoT's aim is oriented toward connectivity of things and Internet. These things are embedded with RFID and using network technology through Internet. Thus, this connects anywhere anytime at anyplace. This huge network of connectivity form IoT network where anything can consist of Internet and sensors to capture the information. The information is captured by sensors and processes by the concerned devices and actuators perform the action as per the processed information. The vision of such network is to track, locate, identify, trigger and administer the things for a specific application[13]. IoT is enabling resource-constrained devices to accomplish different jobs in many emerging areas. It has enabled the devices to perform computations, communication and intelligent decisions[95] as shown in Fig. 1.

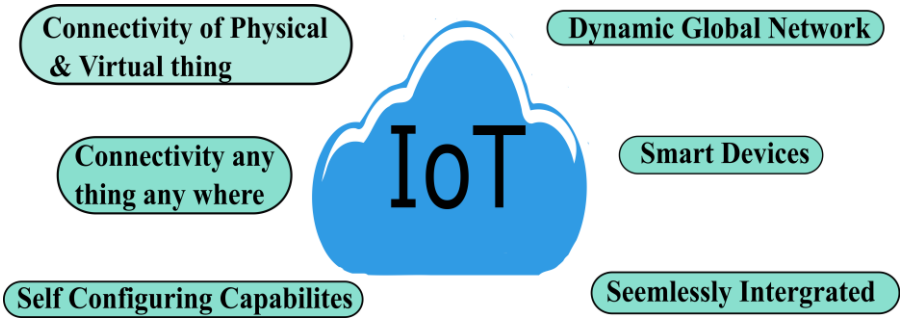

Fig. 1: Vision of IoT

3 IoT Architecture

There is a need for exploratory study to improve aspects such as energy usage, scale, efficiency, and so forth, due to its widespread uses and excellent infrastructure. Furthermore, a framework is required in an IoT context to collect and analyse data for outcome. Since the information obtained global level cannot be managed centralized in all but the most dispersed areas. As a result, cloud solutions have evolved into an indispensable component of IoT systems. Data gathering, transmitting data, method used to transmit information, framework to process and store data, and ultimately decision-making are the five steps of IoT. Just like every section of the community seeks to automate workplaces and replace humans in specific scenarios, work in such IoT stages is fast developing. Sensors, transceivers, actuators, CCTV, radio-frequency identification (RFID), and other devices are commonly used to span objects of interest (known as IoT environment) in a spectrum of uses for a variety of objectives. These devices work at physical layer. Here, devices sense and capture data. IoT may develop enormously by interacting and sharing data with each other without the need for human engagement due to various communication technologies like Bluetooth, Wi-Fi, ZigBee, 5G, etc. These communication technologies enable IoT communication by transmitting data. This layer is known as Transport layer. The devices are internet-connected and can be managed via smartphone apps. Each device in an Iot paradigm is given an IP address in able to connect to the Internet or other networks and be uniquely identifiable. To begin, IoT nodes are attached to a personal area network (LAN) for short-range connectivity (such as ZigBee, Bluetooth, wireless devices, and others). Then, via Wi-Fi, Ethernet, and many other methods, the short-range networks are connected to the local area network. Then data is processed using IoT services. Furthermore, information produced by Iot nodes is transmitted to the cloud over wide-area networks, which may be private or public. In order to analyse and extract knowledge for decision-making, captured data must be kept. This is done at processing layer. This type of information is large, quick, and diverse. A central server can be a cluster, supercomputer, a grid, a cloud, or something else entirely. For diverse reasons, various computing models have

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

been developed. However, because of its dynamic pricing approach and expandable operation characteristic, cloud computing has grabbed corporations and scientific industries. These computing models work at business layer. Cloud computing is such a business model that provides service based resources on a charges basis on use, and it's ideal for IoT environments to quickly build up a virtual computing infrastructure instead of implementing on-premise data warehouses.

IoT has not a universal architecture; rather different researchers have proposed different architectures. During the early stage, three-layer architecture of IoT was proposed then later Said & Masud in 2013 proposed five-layer architecture [83]. These five layers are perception, transport, processing, application, and business layer as shown in Fig. 2.

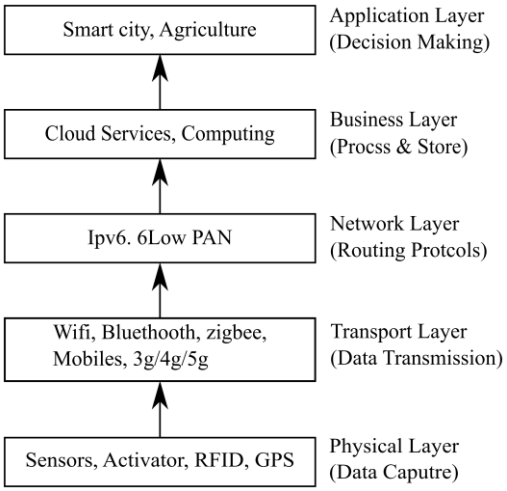

Fig. 2: IoT Architecture

4 COMMUNICATION TECHNOLOGIES

4.1 Radio Frequency Identification (RFID)

This automated technology is used to track, monitor, and identify objects wirelessly. It was first introduced in 1945. It is a prerequisite for IoT communication [44]. This technology includes two components, *i.e.,* tags and readers as shown in Fig. 3.

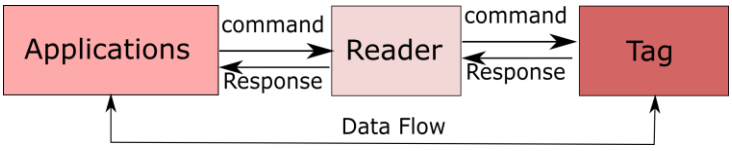

Fig. 3: RFID

Tags:The terminating points of RFID are called tags. Tags are used to store identity information of a device and other information needed for working of tag. These tags are of two types, one is Active tags which contain on-board power and more range. Another is the passive tag which does not have internal power, so it gets active by touching the reader. These tags contain an integrated circuit to store and process the information and to modulate/demodulate the RF signals.

Readers: Readers consist of an antenna to transmit and receive signals to/from the tags. Readers are powered with a battery or plugged using a wall outlet. To activate the passive tags, readers need strong radio frequency signals. A reader controller is connected with the reader to manage the information read by the reader. It can also update a tag if required by the application [80]. The major use of RFID is to tracking objects, observing race timing, and inventory management. It is the so-called IoT. IoT became famous through the Auto-ID Centre

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452
and market-related analysis [44].

1. ***Security Challenges*:** The major security risks are tag isolation, tag cloning, denial of service, malicious code injection, RFID skimming, amplification attack and unauthorized access etc. but still as per market statistics, RFID industry will grow continuously and there is need to develop security measures. Some authors have presented solutions to challenges as shown in Table 1. The cost of commercial RFID reader and reconfiguration is high as RFID tags are not much flexible. Wireless RFID sensors are not pervasive in homely use.

Table 1: RFID Challenges and their Solutions

Security Challenges	Solutions
Tag Cloning	[15], [45], [115]
Privacy	[26], [93]
Malicious code injection	[34], [91]
Unauthorized access/ RFID skimming	[3]
Amplification attack	[20], [29]

2. ***Application Areas of RFID:*** A teaching management application has been developed by Tan et al. [103] which is implemented using WiFi supported RFID (WiRF). It performs automatic student attendance using Quick Response (QR) code. Another RFID based application[26] mainly focuses on protection of medical data using one authentication scheme where tag identity is kept secret. In agriculture, an IoT application has been designed to monitor the growth of sugarcane and to monitor the food quality[19]. Industries are also adopting RFID for inventory tracking, automatic billing, etc. [107], [92]

4.2 Near-Field Communication

NFC is a radio frequency-based communication technology that has enabled contactless transactions. It is useful for short-range communication. It works in a band of 13.56 MHz. It can also read the high-frequency RFID tag. The typical range of NFC is 3 inches. It can also work as a tag or a reader as shown in Fig. 4 [76]. It contains two types of components, namely, Initiator and Target.

- The initiator device initiates the communication and generates an RF field to power the passive target.
- The target device receives the information from the initiator that can be passive or active.

The major use of NFC is to share information between smart phones and for contactless payments. NFC technology enables IoT communication through its following features[106].

- Connect two IoT devices through its tap and go mechanism.
- Due to its short range, it protects against unauthorized access because NFC chips must be close enough to initiate information transfer.
- It provides data confidentiality through its built-in encryption feature.
- Data can be exchanged passively via NFC tags to NFC-enabled devices having no power.
- It plays a major role in IoT applications such as home automation where no need to remind long passwords, just NFC-enabled devices can connect to the home network by simply tapping the feature.

Thus, NFC has significant potential to improve IoT applications.

1. ***Security Challenges:***NFC sensors works with the insecure channel which is vulnerable to various security attacks like eavesdropping, ticket cloning, phishing, spoofing, relay attacks etc. Data can be modified during transmission or denial of service attack can occur. Each smart card chip contains a unique ID, but attacker can misuse the ID as only single id is being used. Such attacks can be handled using some security protocols as shown in Table 2.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

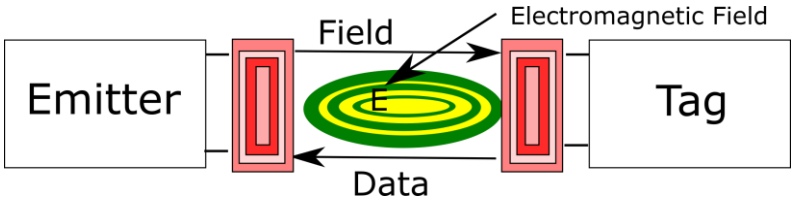

Fig. 4: NFC

Table 2: NFC Challenges and their Solutions

Security Challenges	Solutions
Eavesdropping	[59], [112]
Relay Attack	[18], [111]
Ticket Cloning	[17]
Spoofing/ phishing	[17], [94]
Single ID	[94], [6]

2. ***NFC Applications:*** It plays a major role in IoT applications such as home automation where no need to remind long passwords, just NFC-enabled devices can connect to the home network by simply tapping the feature. Thus, NFC has significant potential to improve IoT applications. NFC applications work in the form of touch and go, touch and confirm, touch and explore etc. Users use NFC applications to shop from home. Payment applications[63], attendance system[58] and other data transfer[69] applications. These applications work in different modes, namely, Card emulation mode, Reader/Writer mode and Peer to Peer mode.

4.3 Bluetooth

Bluetooth is a low-power technology that is native support for IoT communication. It was developed in 1994. It is a short-range wireless technology. It allows devices to transfer data through radios waves by connecting them. Bluetooth acts as a pillar of the IoT that provides connections to devices. Through Bluetooth, any type of file can be transferred such as audio, video, images, and documents[22]. The maximum range of devices having Bluetooth should not exceed 100 m. However, its range varies from Class 1 to Class 3. Class 1 has the maximum range of 100 m and class 3 has the range of 1 m. Although several times Bluetooth technology has been seemed to be dead[22], still it is more suitable for IoT applications [68]. But due to its complex discovery rules, conventional Bluetooth is not well-suitable for IoT[38]. A term BLE (Bluetooth Low-energy) also called Bluetooth Smart has been introduced in 2010. The purpose of BLE is to use Bluetooth for wireless sensor networks as shown in Fig. 5. In BLE, there is more channels and bandwidth as compared to conventional Bluetooth. To discover and establish connections between IP-enabled devices, a protocol named Internet Protocol Support Profile (IPSP) has been introduced by Bluetooth SIG. However, BLE is not able to support multicast communication[52]. Since Bluetooth has more extensive use in smartphones, it is also gaining a place in some IoT applications like home automation[96].

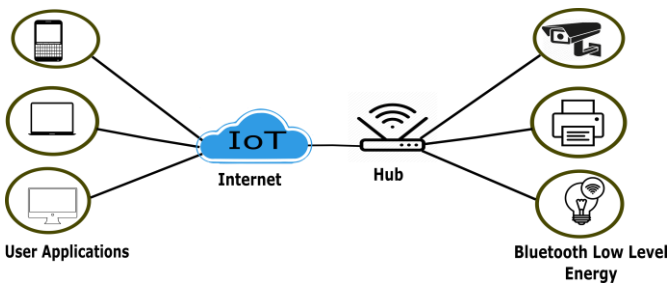

Fig. 5: Bluetooth

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

1. ***Security Challenges:***The initial Bluetooth security settings (connect-ability and discoverability) are done by user that can be silent, private and public. There are so many vulnerabilities such as eavesdropping, weakness in encryption method, PIN code selection, and weak device configuration as shown in Table 3. Man –In –The –Middle (MITM) attack can occur during secure sample pairing. Such type of vulnerabilities can be handled using intrusion detection and prevention system, Fingerprint-based security method etc.

2. ***Bluetooth Applications:***Since Bluetooth has more extensive use in smartphones, it is also gaining a place in some IoT applications like home automation [96]. Radar door system[42], smart agriculture monitoring [81], attendance management system [57], [23] are some Bluetooth-based IoT applications. Bluetooth makes the little things smart by its connectivity feature like pedometer in shoes, smart watches, home automation features etc. It plays a major role in health and fitness applications[78].

Table 3: Bluetooth Challenges and their Solutions

Security Challenges	Solutions
Battery Exhaustion attacks	[65]
Man –In –The –Middle (MITM) attack on SSL	[99], [117]
Relay attacks	[105]
Impersonation attacks (weakness in encryption/ PIN code selection system)	[7]
Eavesdropping, weak device configuration	[105], [36]
Spoofing attacks	[114]

4.4 ZigBee

It is low-power communication and radio wireless technology that is well suited for IoT applications as shown in Fig. 6. However, it is not adopted by the mobile phone industry, so limited to use in public deployment[38]. It is low energy and low-cost technology that is a requirement of IoT. Due to its ultra-low power, ZigBee devices have long-lasting batteries[55]. It is the standard radio protocol used in wireless sensor networks [16]. It supports point-to-point as well as point-to-multipoint networks. It provides a secure data connection using a 128-bit AES encryption algorithm. ZigBee 3.0 supports up to 6500 nodes per network[41]. It enables wireless communication at a low cost with low-power solutions. ZigBee is gaining a place in various IoT applications such as Green House Monitoring[84], Home Automation System [31].

Fig. 6: ZigBee

1. ***Security Challenges:***Like other communication technologies, ZigBee is also vulnerable to different security attacks as shown in Table 4. ZigBee has some built-in security features; still some network attacks can occur. Attacks such as flooding and de-synchronization are vulnerable at transport layer. Network layer is more prone to wormholes and selective forwarding attacks where sender node is attacked by malicious nodes. Sometimes attackers create congestion by neighbour attacks. Attacker sends fake messages to low the node's energy.

2. ***ZigBee Applications:*** ZigBee is an emerging technology in computing that connects devices with Internet and reduces cost, time and human efforts by deploying IoT applications. These technologies have made possible

to identify, locate and track objects. IT has become a communication standard in commercial applications[4]. ZigBee has various automation applications such as smart home[30], attendance system[102], healthcare applications[4] etc.

Table 4: ZigBee Challenges and their Solutions

Security Challenges	Solutions
Network Layer attacks	[27], [49]
Unauthorized access	[49]
Energy Depletion Attack	[14], [64]
Sink attack, LDoS attack	[70], [28]
Wormhole attack	[43]

4.5 6LoWPAN

The 6LoWPAN is a wireless low power personal area network that supports IPv6 protocol network [87], [108]. Its main aim is to apply the Internet Protocol over smallest devices that are limited in computational and processing power. Thus, its target is to connect low-power communication applications using IP networking as shown in Fig. 7. As IPv6 has enough address space to identify all the devices/things in the world. For this, 6LoWPAN group defined the header compression and encapsulation method that allows IPv6 packets to transfer over low power networks. IT provides both secure mode as well as non-secure mode for communication.

1. ***Security Challenges:***6LoWPAN network is vulnerable to various attacks such as direct network damage, stealing the confidential information by unauthorized access etc. As shown in Table 5. At physical layer, there can be jamming attack, tampering attack that exploits nodes to steal the secret information [110]. As 6LoWPAN doesn't provide any authentication scheme so it can result in fragmentation attack. So, attacker can easily join the network[75] It directly connects to the Internet which can lead to Internet side attacks.

Table 5: 6LoWPAN Challenges and their Solutions

Security Challenges	Solutions
Fragmentation attack	[40]
Authentication/Impersonation attack	[71], [73], [104]
Internet side attack	[43], [79]
Replay/Neighbour attack	[110]
Copycat attack	[109]
Denial-of-service attack	[47]

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

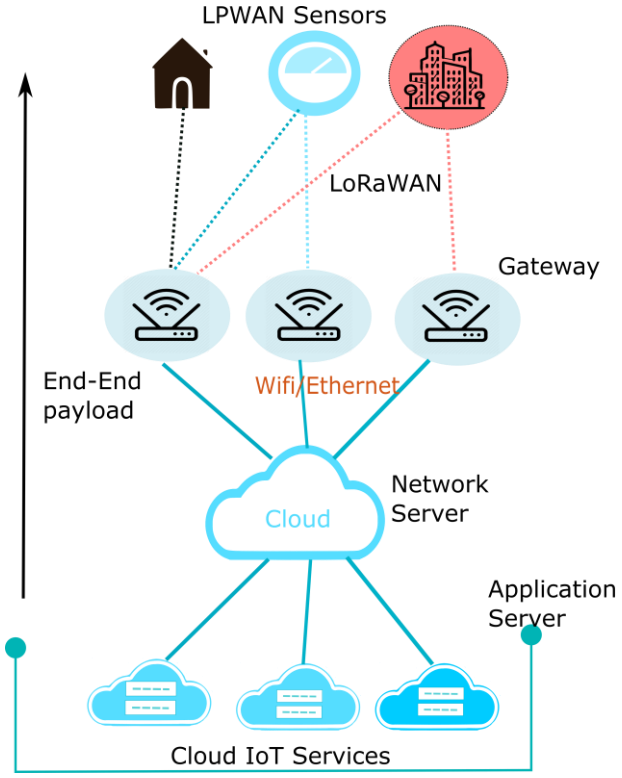

Fig. 7: 6LoWPAN

2. ***6LoWPAN Applications:*** 6LoWPAN provides wireless connectivity to Internet at low data rates. It has so many application areas. It provides so many opportunities in various areas of automation such as healthcare [37] , smart grid [89], smart home [104], [51], industries [86], smart lighting [39], etc. These applications decrease human efforts a lot.

4.6 Wi-Fi

Wireless Fidelity (Wi-Fi) is a widespread network. It connects a broad network of computers to form a local area network as shown in Fig. 8. It has higher range than ZigBee, Bluetooth, and other protocols. It operates on the frequency of 2.4 GHz and 5GHz [96]. It can address a variety of profiles. Its main role in IoT is to perform internetworking with other specialized communication technologies. Thus, Wi-Fi supports narrowband as well as broadband IoT applications. Some IoT applications like vehicular systems and security cameras system need higher bandwidth, so implemented with the support of Wi-Fi.

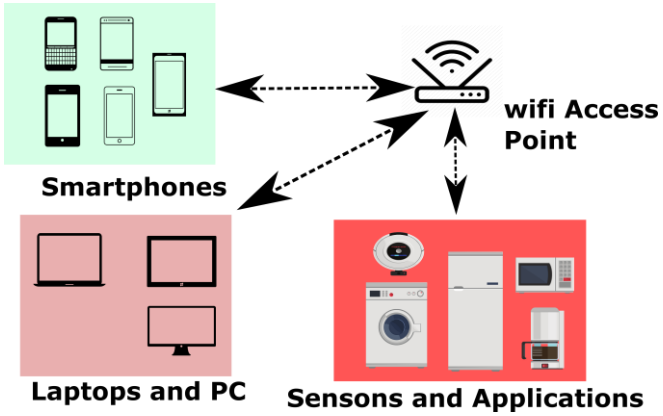

Fig. 8: WiFi

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

1. ***Security Challenges:***There are also various encryption levels of Wi-Fi such as WEP 64/128-bit encryption, WPA and WPA2. But still, it's difficult to detect attacks in Wi-Fi networks. Usually, attacker attacks the Wi-Fi network when a device searches for a wireless signal. The other major attack is eavesdropping on wireless network. Wi-Fi network is also vulnerable to various attacks such as network access, data stealing etc. as shown in Table 6.

Table 6: Wi-Fi Challenges and their Solutions

Security Challenges	**Solutions**
Data stealing	[9]
Authentication	[54], [60]
WiFi Cracking/Spoofing/ DoS/ Port scanning attack	[24]
Devices prone to attack	[90]

2. ***Wi-Fi Applications:*** Wi-Fi addresses the many different profiles due to its family of standards. Thus, it supports application areas in most IoT networks. IoT applications like security cameras[97], vehicular system[67] need wireless broadband network's bandwidth that enable low latency. It supports broadband as well as narrow band IoT applications.

4.7 Cellular Technology (3G/4G/5G)

3G networks support more security features than 2G, but still have some bearers such as circuit data as well as circuit voice. Cellular technology[61] is raising the mobile communication that supports audio-video calls effectively. But it needs high power requirements and operational cost. However, it is not much suitable for battery-operated IoT sensor networks. Next-generation high-speed 5G [33] cellular technology is expected to be future of IoT applications. 5G has ultra-low latency. It supports communication to the devices like smart phones, GPS trackers, and wireless devices like mouse, keyboard, cell phones and many more.

1. **Security Challenges:** As the technology is advancing, with the same speed vulnerabilities are also increasing. There are various security challenges that need to consider while deploying IoT applications. Due to wide architecture of these networks, such networks are vulnerable to various attacks such as Denial of Service, Unauthorized access, Channel jamming, Energy depletion, Message forgery, replay attack, Man-in-middle attack etc. as shown in Table 7.

Table 7: Cellular Technology Challenges and their Solutions

Security Challenges	**Solutions**
DoS/Spoofing/ Routing attack	[34], [50]
Sniffing attack/ Identification attack	[88]
Replay attack	[2]
Energy Depletion Attack	[48], [74]
Privacy attack	[8], [12]

2. **Applications:** Rise in bandwidth of 3G/4G networks give rise to several IoT applications such as Video on demand, Global roaming, Tele-marketing, Tele-medicine, Mobile Television, Video conferencing, Location-based applications[25], Antenna designing [21], Agriculture [101] etc.

5 Comparative Evaluation

The trend to support a variety of connections under the umbrella of IoT is increasing day by day. In IoT, the number of machine-to-machine (M2M) connections is more, and the majority of these connections are wireless. These connections are enabled by various communications technologies that vary in some capacity's metrics mentioned below:

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

- Power - Moderate power/ low power/ Ultra-low-power
- Range – Long range/ local range/ short range/ very short range
- Data Rate – Moderate data rate/ Low data rate
- Latency – Low latency/ Ultra-low latency
- Availability – Standard availability/ Critical availability
- Topology – Point-to- point/ multi-point

As per these factors, some of the communication technologies that enable IoT are compared in Table 8. As the number of devices connecting to IoT is increasing day-by-day, so there is need to update the communication technologies in terms of wide spectrum, multi-functional chips with ultra-low power and unified protocol. Standardization of these technologies is also necessary to ensure security, efficiency and reliability.

Table 8: Comparison of Communication Technologies

Communication Technologies **Features**	**RFID**[10]	**NFC** [106]	**Bluetooth** [113]	**ZigBee**[41]	**6LoWPAN** [108]	**WiFi 5 and 6**[72]	**Cellular Technology** (3G/4G/5G) [61]
Power	Low power based on (Active or Passive)	Need device power	Very low	Very low (Long battery life)	Very low	Moderate	Ultra-low (5G) High (3G/4G)
Range	10cm/1m/ 100m/2m	Short range 3inch	Short 40-400m	Short 10-100m	800m	Moderate 20 m/ 150 m	10 Miles (4G)
Data Rate	Low to moderate (band wise)	Low 424 Kbps	Low 2Mbps (BLE)5.0	Low 250 Kbps	250 Kbps	High bandwidth 100Mbps	20 Mbps (4G)
Frequency	120kHz/13.56 MHz/ 10GHz (band wise)	13.56 MHz	2.402 GHz to 2.48 GHz	2.4 GHz, 900 MHz, 868 MHz	2.4 GHz	2.4 / 5/ 6 GHz	2-8 GHz (4G)
Latency	--	--	Low	Low	--	Low	Ultra-low (5G)
Topology	Point-to-point	Point-to-point	Point-to-point	Mesh	Mesh, Star	Any	Star
Role in IoT	Identify and track objects	communication	BLE is suited for communication in IoT devices	Well suited for IoT applications	Connect smallest devices	Internetworking/ communication	Global Mobility, Seamless Switching
Security	--	--	Key Pairing	AES	Secure and non-secure mode	AES/RC4	Device-based Authentication
Applications	Smart mirrors, tracking applications,	Contactless payment, Smart tag	Content delivery, in-store navigation	Home automation, Energy management, smart lighting	Smart agriculture, smart city	Industrial automation applications, Smart home	Traffic routing, Fleet tracking, time-sensitive industrial application

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

Selection of communication Technologies: While selecting a communication technology for any IoT application, there is needed to consider range, throughput, and availability of technology in that area, power consumption and battery life. Actually, some technologies have large range, but consume more network resources like power and battery life. In IoT, devices work using sensors and these sensors are powered with battery. So, there are various factors that need to be considered such as:

1. Nature of IoT application
2. Type of network
3. Configuration of network resources
4. Module or chip or sensors used in network
5. Availability of communication technology
6. Spectrum

6 A Smart home automation solution

With a one App, this application provides a full Connected Home automated process. You can operate your electronic objects from wherever, whether it's outside, inside, or on the go. It provides intelligent, safe, and trustworthy cloud-based approach for controlling many devices with a single button press. Air conditioners, fans, plugs, and light bulbs may all be managed through a single app. Alexa, Google Home, and a half-dozen more Voice - enabled can control your Smart Home gadgets. It provides management and control of devices in realtime. With this app, devices can be shared and grouped.

6.1 Connectivity

In a smart home each type of appliance is connected with the IoT. This connectivity needs some communication technology to enable IoT. Here, WiFi connectivity has been used to implement smart home solution. Each device is connected with WiFi. Internet connectivity is must for this communication. Firstly, the app is installed and then account is created for security. Then, switch on the scan mode. It will start searching for smart devices. After searching the devices, we can switch on/off the appliances. For secure communication it is necessary to add the devices so that unauthorized device will unable to connect.

6.2 Security

In a smart home, two types of security is required, namely, physical security and digital security.

Physical Security: It means to ensure that no unauthorized user can enter in the house. For this following solutions are there:

1. Alarm Sensors: For security, security alarms can be installed which sound when there is any suspicious activity or entry.
2. Door-Lock Sensor: One digital lock can be equipped inside door to entry only of authorized users.
3. Camera: Cameras are required to monitor the suspicious activity.

Digital Security: It means to access the home network through devices securely.For this following solutions are there:

1. Account: There should be one account for accessing the home automation network. Email –id can be used for authorized access.
2. Secure communication technology: Communication technology such as Wi-Fi should be password enabled so that unauthorized user cannot access the network.
3. New Device Access: First time, new device should be added with an authentication protocol to maintain the security.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

Fig. 9: Communication technologies enabling IoT

6.3 Implementation:

By creating an app, it's very easy to implement secure smart home automation network. After installing app and creating account, there is need to just connect smart devices through communication technology such as Wi-Fi. Then, user can operate smart devices anytime anywhere. Some vendors also provide such apps to make smart home such as Digitap by Havells India Ltd as shown in Fig. 9. This app can be installed on the mobile and then connect the smart devices and smart home can be formed easily.

Steps for implementation:

1. Switch on the Wi-Fi and smart devices.
2. Install the app on the mobile.
3. Create the account for secure access.
4. Scan the smart devices on the app.
5. Then, automatically selected devices will be added.
6. Then, devices can be operated from the app.

7 Security Trends in IoT

IoT network aims to secure in terms of privacy, integrity, authentication and availability. If any of these security factor losses then system is being compromised. Thus, it is necessity of IoT provide security services to users so that data is securely available to authorized users consistently. There is need to follow security standards while connecting electronics devices. Usually, the devices from unauthorized vendors are not secure and don't follow security standards. IoT architecture has three basic layers: Perception, Network and Application layers.

RFID, sensors, actuators and other hardware devices work at perception layer. These devices don't have their own security so these devices must be secure through some security applications in the network. Further these are connected with network layer. Security techniques are implemented on these connections to control unauthorized access. Some access control and device-based authentication techniques are implemented at this layer. Usually, data captured by devices at perception layer is encrypted by cryptography algorithms so that any data theft during transmission cannot read by unauthorized user. Network layer provides communication between perception and application layer. On the network layer devices can be connected through Wi-Fi, BLE, LoRa, and ZigBee, 2G/3G /4G/5G, NFC or any other communication technology. These technologies have different data rate, security mechanism, frequency and range. This layer is more vulnerable to threats due to exposure to different types of networks. These technologies have some built-in security techniques in terms of cryptography algorithms. Intrusion detection systems, virtual private networks, hop-count filtering, timeliness of data messages, synchronization of cookies are the security solutions at network layer. Application layer receives data through network layer. IoT applications are deployed at this layer using different platforms such as cloud computing, fog computing, web interfaces etc. At this layer, data needs protection from

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452
unauthorized access and misuse. Applications at this layer need access control, authentication mechanisms. Thus, following security mechanisms are available to secure IoT network:

- Cryptography algorithms – Both symmetric and asymmetric algorithms[1]
- Access Control techniques[5]
- Authentication techniques[6]
- Security tools at application level[62]
- Anti-virus[2]
- Faraday cage[35]
- Message timer[28]
- Physical security[105]
- Virtual private networks[46]
- Fault detection methods[116]
- Intrusion detection system[73]
- Security upgrade services[77]
- Hop-count Filter[100]
- Data Forensics[98]
- Anomaly detection tools[11]
- Audit system[85]
- Dynamic security tools[56]
- Security Protocols[32]

Each security method has a specific goal to achieve security in terms of confidentiality, privacy, access control, authentication, eavesdropping, non-repudiation etc. Like anti-malware techniques provide only security from data stealing or some other attacks but not provide privacy which is achieved by only cryptography techniques. So, there us need to develop a complete security package that fulfills each type of security goals over an IoT network.

8 Challenges and Research Directions

IoT has a special goal for communication, *i.e.*, connecting anything anywhere anytime. Thus, communication technologies face different challenges to enable IoT communication as shown in Fig. 10. These challenges and research directions are:

1. **Resource Management:** In IoT, communication technologies have to connect any type of device. IoT devices are limited in memory, power, and computation. Thus, technologies need to tackle resource-constrained devices.
2. **Data Modeling:** Due to heterogeneous applications, devices, there is urgent need to manage and structure the data. Thus, efficient data modeling techniques are required.
3. **Dynamic Topology:** Any device that can connect to another network or device that can affect the network topology or any routing tables. Communication technologies should be efficient enough to handle a dynamic network.
4. **Security:** IoT communication needs security in terms of authentication, integrity, confidentiality, anonymity, and non-repudiation. IoT devices are resource-constrained, so devices are not suitable for traditional security algorithms. Communication technologies should use lightweight security algorithms that need fewer resources.
5. **Internetworking:** IoT devices use a variety of wireless networks and use non-IP protocol as well as IP protocol at the same time while communicating with their service provider. Communication technologies should support multi-protocol networking with different communication mediums.
6. **Availability:** Communication technologies should be available for authorized devices each time.
7. **Identity Management:** Each time when a device connects to an IoT network, unique identification is

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p.42-61
https://publishoa.com
ISSN: 1309-3452

necessary for each device. This identity management is dynamic.

8. **Scalability:** The number of devices connecting to IoT networks is increasing day by day. So, communication technologies need to support scalability dynamically.

Fig. 10: Challenges & Research Directions Conclusions

9 Conclusion

As IoT applications are wide and manifold, so there is need for various wireless communication technologies that enable IoT. However, each technology has its working capacity in terms of bandwidth, speed, range, etc. No single technology is enough for low-power communication rather collectively these communication technologies enable connectivity at a large scale. Each application has different requirements with a different configuration of the device that may appear under the umbrella of IoT. By analyzing the presented communication technologies, BLE, Wi-Fi, and ZigBee are suitable for IoT communication. Additionally, a smart home solution can be easily implemented by considering security tools. Further different security techniques has been presented, these techniques provide specific type of security. There is need to develop an efficient security package that works on each layer of network and resistant to each type of threat. However, many challenges are still to handle for which new communication technologies are in need.

Acknowledgment

The authors wish to thank many anonymous referees for their suggestions to improve the paper. Lata, N. would like to thank I.K. Gujral Punjab Technical University for offering the Ph.D. course in Computer Science & Engineering and providing support to access the resources for research.

References

[1] Abood, Omar G. and Elsadd, Mahmoud A. and Guirguis, Shawkat K. Investigation of cryptography algorithms used for security and privacy protection in smart grid. *2017 Nineteenth International Middle East Power Systems Conference (MEPCON)*, pages 644–649, Cairo, 2017. IEEE.

[2] Ahvanooey, Milad Taleby and Li, Qianmu and Rabbani, Mahdi and Rajput, Ahmed Raza. A survey on smartphones security: software vulnerabilities, malware, and attacks. *arXiv preprint arXiv:2001.09406*, 2020.

[3] Alamr, Amjad Ali and Kausar, Firdous and Kim, Jongsung and Seo, Changho. A secure ECC-based RFID mutual authentication protocol for internet of things. *J Supercomput*, 74(9):4281–4294, 2018.

[4] Alharbe, Nawaf and Atkins, Anthony S. and Akbari, Akbar Sheikh. Application of ZigBee and RFID Technologies in Healthcare in Conjunction with the Internet of Things. *Proceedings of International Conference on Advances in Mobile Computing & Multimedia - MoMM '13*, pages 191–195, Vienna, Austria, 2013. ACM Press.

[5] Ali, Inayat and Sabir, Sonia and Ullah, Zahid. Internet of things security, device authentication and access control: a review. *arXiv preprint arXiv:1901.07309*, 2019.

[6] Alshammari, Munefah and Nashwan, Shadi. Fully Authentication Services Scheme for NFC Mobile Payment Systems. *Intelligent Automation & Soft Computing*, 32(1):401–428, 2022.

[7] Antonioli, Daniele and Tippenhauer, Nils Ole and Rasmussen, Kasper. BIAS: Bluetooth Impersonation AttackS. *2020 IEEE Symposium on Security and Privacy (SP)*, pages 549–562, San Francisco, CA, USA, 2020. IEEE.

[8] Atukuri, Veera RaghavaRao and Mathe, MP Rama Krishna and Pamidipati, Mrunalini. Network evolution in 3g/4g: Applications and security issues. *International Journal of Computer Science and Information Technologies*, 2(6):2835–2837, 2011. Publisher: Citeseer.

[9] Belghazi, Zakariae and Benamar, Nabil and Addaim, Adnane and Kerrache, Chaker Abdelaziz. Secure WiFi-Direct Using Key Exchange for IoT Device-to-Device Communications in a Smart Environment. *Future Internet*, 11(12):251, 2019.

[10] 49ersBelongInSanFrancisco. Radio-frequency identification. 2021. Page Version ID: 1022557688.

[11] Bhatia, M. P. S. and Sangwan, Saurabh Raj. Soft computing for anomaly detection and prediction to mitigate IoT-based real-time abuse. *Pers Ubiquit Comput*, 2021.

[12] Borgaonkar, Ravishankar and Hirschi, Lucca and Park, Shinjo and Shaik, Altaf. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *Proceedings on Privacy Enhancing Technologies*, 2019(3):108–127, 2019.

[13] Burhan, Muhammad and Rehman, Rana and Khan, Bilal and Kim, Byung-Seo. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, 18(9):2796, 2018.

[14] Cayre, Romain and Galtier, Florent and Auriol, Guillaume and Nicomette, Vincent and Kaaniche, Mohamed and Marconato, Geraldine. WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips. *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 376–387, Taipei, Taiwan, 2021. IEEE.

[15] Chahid, Yassine and Benabdellah, Mohamed and Azizi, Abdelmalek. Internet of things security. *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, pages 1–6, Fez, Morocco, 2017. IEEE.

[16] Chang, Hong-Yi. A connectivity-increasing mechanism of ZigBee-based IoT devices for wireless multimedia sensor networks. *Multimed Tools Appl*, 78(5):5137–5154, 2019.

[17] Chattha, Naveed Ashraf. NFC — Vulnerabilities and defense. *2014 Conference on Information Assurance and Cyber Security (CIACS)*, pages 35–38, Rawalpindi, Pakistan, 2014. IEEE.

[18] Chen, Cheng Hao and Lin, Iuon Chang and Yang, Chou Chen. NFC Attacks Analysis and Survey. *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 458–462, Birmingham, United Kingdom, 2014. IEEE.

[19] Chi, Tao and Chen, Ming. A frequency hopping method for spatial RFID/WiFi/Bluetooth scheduling in agricultural IoT. *Wireless Netw*, 25(2):805–817, 2019.

[20] Chien, Hung-Yu and Wu, Tzong-Chen and Hsu, Chien-Lung. RFID Authentication with Un-Traceability and Forward Secrecy in the Partial-Distributed-Server Model. *IEICE Trans. Inf. & Syst.*, E98.D(4):750–759, 2015.

[21] Chung, Mingâ€□ An and Chang, Weiâ€□ Hsuan. Lowâ€□ cost, lowâ€□ profile and miniaturized singleâ€• plane antenna design for an Internet of Thing device applications operating in 5G, 4G, V2X, DSRC, WiFi 6 band, WLAN, and WiMAX communication systems. *Microw Opt Technol Lett*, 62(4):1765–1773, 2020.

[22] Collotta, Mario and Pau, Giovanni and Talty, Timothy and Tonguz, Ozan K. Bluetooth 5: A Concrete Step Forward toward the IoT. *IEEE Commun. Mag.*, 56(7):125–131, 2018.

[23] Decuir, Joseph. Introducing Bluetooth Smart: Part II: Applications and updates. *IEEE Consumer Electron. Mag.*, 3(2):25–29, 2014.

[24] Dua, Aneesh and Tyagi, Vibhor and Patel, Nd and Mehtre, Bm. IISR: A Secure Router for IoT Networks. *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, pages 636–643, Mathura, India, 2019. IEEE.

[25] Ezhilarasan, E. and Dinakaran, M. A Review on Mobile Technologies: 3G, 4G and 5G. *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, pages 369–373, Tindivanam, Tamilnadu, India, 2017. IEEE.

[26] Fan, Kai and Jiang, Wei and Li, Hui and Yang, Yintang. Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE Trans. Ind. Inf.*, 14(4):1656–1665, 2018.

[27] Fan, Xueqi and Susan, Fransisca and Long, William and Li, Shangyan. Security analysis of zigbee. *MWR InfoSecurity*, :1–18, 2017.

[28] Farha, Fadi and Ning, Huansheng and yang, shunkun and xu, Jiabo and Zhang, Weishan and Choo, Kim-Kwang Raymond. Timestamp Scheme to Mitigate Replay Attacks in Secure ZigBee Networks. *IEEE Trans. on Mobile Comput.*, :1–1, 2020.

[29] FernÃ¡ndez-CaramÃ©s, Tiago and Fraga-Lamas, Paula and SuÃ¡rez-Albela, Manuel and Castedo, Luis. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors*, 17(12):28, 2016.

[30] Froiz-MÃ-guez, IvÃ¡n and FernÃ¡ndez-CaramÃ©s, Tiago and Fraga-Lamas, Paula and Castedo, Luis. Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes. *Sensors*, 18(8):2660, 2018.

[31] Gill, Khusvinder and Yang, Shuang-Hua and Yao, Fang and Lu, Xin. A zigbee-based home automation system. *IEEE Trans. Consumer Electron.*, 55(2):422–430, 2009.

[32] Granjal, Jorge and Monteiro, Edmundo and Sa Silva, Jorge. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Commun. Surv. Tutorials*, 17(3):1294–1312, 2015.

[33] GSA, 2015. The Road to 5G: Drivers, Applications, Requirements and Technical Development. 2019.

[34] Gupta, Aman and Verma, Tanmay and Bali, Soshant and Kaul, Sanjit. Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks. *2013 Fifth International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–60, Bangalore, India, 2013. IEEE.

[35] Guri, Mordechai and Zadov, Boris and Elovici, Yuval. ODINI: Escaping Sensitive Data From Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *IEEE Trans.Inform.Forensic Secur.*, 15:1190–1203, 2020.

[36] Haataja, Keijo and HyppÃ¶nen, Konstantin and Pasanen, Sanna and Toivanen, Pekka. *Bluetooth Security Attacks* of SpringerBriefs in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[37] Hariharakrishnan, Jayaram and N, Bhalaji. Adaptability Analysis of 6LoWPAN and RPL for Healthcare applications of Internet-of-Things. *JISMAC*, 2(2):69–81, 2021.

[38] Harris III, Albert F. and Khanna, Vansh and Tuncay, Guliz and Want, Roy and Kravets, Robin. Bluetooth Low Energy in Dense IoT Environments. *IEEE Commun. Mag.*, 54(12):30–36, 2016.

[39] Huang, Zucheng and Yuan, Feng. Implementation of 6LoWPAN and Its Application in Smart Lighting. *JCC*, 03(03):80–85, 2015.

[40] Hummen, RenÃ© and Hiller, Jens and Wirtz, Hanno and Henze, Martin and Shafagh, Hossein and Wehrle, Klaus. 6LoWPAN fragmentation attacks and mitigation mechanisms. *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec '13*, pages 55, Budapest, Hungary, 2013. ACM Press.

[41] Inc, Digi International. What Is Zigbee Wireless Mesh Networking?.

[42] Ishak, Muhammad Yusry Bin and Ahmad, Samsiah Binti and Zulkifli, Zalikha. Iot Based Bluetooth Smart Radar Door System Via Mobile Apps. *2019 1st International Conference on Artificial Intelligence and Data Sciences (AiDAS)*, pages 142–145, Ipoh, Perak, Malaysia, 2019. IEEE.

[43] Jegan, G. and Samundiswary, P. Wormhole Attack Detection in Zigbee Wireless Sensor Networks using Intrusion Detection System. *Indian Journal of Science and Technology*, 9(45), 2016.

[44] Jia, Xiaolin and Feng, Quanyuan and Fan, Taihua and Lei, Quanshui. RFID technology and its applications in Internet of Things (IoT). *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pages 1282–1285, Yichang, China, 2012. IEEE.

[45] Jisha S and Philip, Mintu. Rfid based security platform for internet of things in health care environment. *2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, pages 1–3,

Coimbatore, India, 2016. IEEE.

[46] Juma, Mazen and Monem, Azza Abdel and Shaalan, Khaled. Hybrid End-to-End VPN Security Approach for Smart IoT Objects. *Journal of Network and Computer Applications*, 158:102598, 2020.

[47] Kasinathan, Prabhakaran and Pastrone, Claudio and Spirito, Maurizio A. and Vinkovits, Mark. Denial-of-Service detection in 6LoWPAN based Internet of Things. *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 600–607, Lyon, France, 2013. IEEE.

[48] Khan, Haibat and Martin, Keith. On the Efficacy of New Privacy Attacks against 5G AKA:. *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, pages 431–438, Prague, Czech Republic, 2019. SCITEPRESS - Science and Technology Publications.

[49] Khanji, Salam and Iqbal, Farkhund and Hung, Patrick. ZigBee Security Vulnerabilities: Exploration and Evaluating. *2019 10th International Conference on Information and Communication Systems (ICICS)*, pages 52–57, Irbid, Jordan, 2019. IEEE.

[50] Kim, Hwankuk. 5G core network security issues and attack classification from network protocol perspective. *J. Internet Serv. Inf. Secur.*, 10(2):1–15, 2020.

[51] Kim, Yeon-Su and Kim, Ki-Tae and Lee, Bo-Kyung. CoAP/6LoWPAN-based Smart Home Network system using DTLS. *The Journal of The Institute of Internet, Broadcasting and Communication*, 18(6):53–61, 2018. ISBN: 2289-0238 Publisher: The Institute of Internet, Broadcasting and Communication.

[52] Kuor-Hsin Chang. Bluetooth: a viable solution for IoT? [Industry Perspectives]. *IEEE Wireless Commun.*, 21(6):6–7, 2014.

[53] Lee, In and Lee, Kyoochun. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4):431–440, 2015.

[54] Lei, Xinyu and Tu, Guan-Hua and Li, Chi-Yu and Xie, Tian and Zhang, Mi. SecWIR: securing smart home IoT communications via wi-fi routers with embedded intelligence. *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, pages 260–272, Toronto Ontario Canada, 2020. ACM.

[55] Li, Yan and Chi, Zicheng and Liu, Xin and Zhu, Ting. Passive-ZigBee: Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption. *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, pages 159–171, Shenzhen China, 2018. ACM.

[56] Li, Yuhong and BjÃ¶rck, Fredrik and Xue, Haoyue. IoT Architecture Enabling Dynamic Security Policies. *Proceedings of the 4th International Conference on Information and Network Security - ICINS '16*, pages 50–54, Kuala Lumpur, Malaysia, 2016. ACM Press.

[57] Lodha, Riya and Gupta, Suruchi and Jain, Harshil and Narula, Harish. Bluetooth Smart Based Attendance Management System. *Procedia Computer Science*, 45:524–527, 2015.

[58] Lu, He-Jun and Liu, Dui. An improved NFC device authentication protocol. *PLoS ONE*, 16(8):e0256367, 2021.

[59] Madlmayr, Gerald and Langer, Josef and Kantner, Christian and Scharinger, Josef. NFC Devices: Security and Privacy. *2008 Third International Conference on Availability, Reliability and Security*, pages 642–647, 2008. IEEE.

[60] Mahalat, Mahabub Hasan and Saha, Shreya and Mondal, Anindan and Sen, Bibhash. A PUF based Light Weight Protocol for Secure WiFi Authentication of IoT devices. *2018 8th International Symposium on Embedded Computing and System Design (ISED)*, pages 183–187, Cochin, India, 2018. IEEE.

[61] Mindmatrix. 4G. 2021. Page Version ID: 1042204074.

[62] Minoli, Daniel and Sohraby, Kazem and Occhiogrosso, Benedict. IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications. *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pages 13–18, Philadelphia, PA, USA, 2017. IEEE.

[63] Morak, J. and Hayn, D. and Kastner, P. and Drobics, M. and Schreier, G. Near Field Communication Technology as the Key for Data Acquisition in Clinical Research. *2009 First International Workshop on Near Field Communication*, pages 15–19, Hagenberg, Austria, 2009. IEEE.

[64] Morgner, Philipp and Mattejat, Stephan and Benenson, Zinaida and MÃ¼ller, Christian and Armknecht, Frederik. Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning. *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 230–240, Boston Massachusetts, 2017. ACM.

[65] Moyers, Benjamin R. and Dunning, John P. and Marchany, Randolph C. and Tront, Joseph G. Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices. *2010 43rd Hawaii International Conference on System Sciences*, pages 1–9, Honolulu, Hawaii, USA, 2010. IEEE.

[66] Mukherjee, Sankar and Biswas, G.P. Networking for IoT and applications using existing communication technology. *Egyptian Informatics Journal*, 19(2):107–127, 2018.

[67] Naik, D. Rahul and Das, Lyla B. and Bindiya, T. S. Wireless Sensor networks with Zigbee and WiFi for Environment Monitoring, Traffic Management and Vehicle Monitoring in Smart Cities. *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pages 46–50, Kathmandu, 2018. IEEE.

[68] Nieminen, Johanna and Gomez, Carles and Isomaki, Markus and Savolainen, Teemu and Patil, Basavaraj and Shelby, Zach and Xi, Minjun and Oller, Joaquim. Networking solutions for connecting bluetooth low energy enabled machines to the internet of things. *IEEE Network*, 28(6):83–90, 2014.

[69] Ok, Kerem and Aydin, Mehmet N. and Coskun, Vedat and Ozdenizci, Busra. Exploring underlying values of NFC applications. *Proceedings of the Third International Conference on Information and Financial Engineering, Singapore*, pages 290–294, Singapore, 2011.

[70] Okada, Satoshi and Miyamoto, Daisuke and Sekiya, Yuji and Nakamura, Hiroshi. New LDoS Attack in Zigbee Network and its Possible Countermeasures. *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 246–251, Irvine, CA, USA, 2021. IEEE.

[71] Oliveira, Luis M.L. and Rodrigues, Joel J.P.C. and Neto, Carlos and de Sousa, Amaro F. Network Admission Control Solution for 6LoWPAN Networks. *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 472–477, Taichung, Taiwan, 2013. IEEE.

[72] Pandakekok9. Wi-Fi. 2021. Page Version ID: 1022754138.

[73] Pasikhani, Aryan Mohammadi and Clark, John A. and Gope, Prosanta and Alshahrani, Abdulmonem. Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review. *IEEE Sensors J.*, 21(11):12940–12968, 2021.

[74] Peng, Chunyi and Li, Chi-yu and Tu, Guan-Hua and Lu, Songwu and Zhang, Lixia. Mobile data charging: new attacks and countermeasures. *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, pages 195, Raleigh, North Carolina, USA, 2012. ACM Press.

[75] Pongle, Pavan and Chavan, Gurunath. A survey: Attacks on RPL and 6LoWPAN in IoT. *2015 International Conference on Pervasive Computing (ICPC)*, pages 1–6, Pune, India, 2015. IEEE.

[76] Proehl, Greg. An Introduction to Near Field Communications | Mouser Electronics.

[77] Qian, Yongfeng and Jiang, Yingying and Chen, Jing and Zhang, Yu and Song, Jeungeun and Zhou, Ming and PustiÅ¡ek, MatevÅ¾. Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, 72:266–273, 2018.

[78] Raza, Shahid and Misra, Prasant and He, Zhitao and Voigt, Thiemo. Building the Internet of Things with bluetooth smart. *Ad Hoc Networks*, 57:19–31, 2017.

[79] Raza, Shahid and Wallgren, Linus and Voigt, Thiemo. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 11(8):2661–2674, 2013.

[80] RBERLIA. Connectivity of the Internet of Things - learn.sparkfun.com.

[81] Reddy Maddikunta, Praveen Kumar and Hakak, Saqib and Alazab, Mamoun and Bhattacharya, Sweta and Gadekallu, Thippa Reddy and Khan, Wazir Zada and Pham, Quoc-Viet. Unmanned Aerial Vehicles in Smart Agriculture: Applications, Requirements, and Challenges. *IEEE Sensors J.*, 21(16):17608–17619, 2021.

[82] Roselli, L. and Mariotti, C. and Mezzanotte, P. and Alimenti, F. and Orecchini, G. and Virili, M. and Carvalho, N.B. Review of the present technologies concurrently contributing to the implementation of the

Internet of Things (IoT) paradigm: RFID, Green Electronics, WPT and Energy Harvesting. *2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, pages 1–3, San Diego, CA, USA, 2015. IEEE.

[83] Said, Omar and Masud, Mehedi. Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, 5(1):1–17, 2013.

[84] Salleh, A. and Ismail, M. K. and Mohamad, N. R. and Abd Aziz, MZ An and Othman, M. A. and Misran, M. H. Development of greenhouse monitoring using wireless sensor network through ZigBee technology. *International Journal of Engineering Science Invention*, 2(7):6–12, 2013.

[85] Santis, L. De and Paciello, V. and Pietrosanto, A. Blockchain-Based Infrastructure to enable Trust in IoT environment. *2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, pages 1–6, Dubrovnik, Croatia, 2020. IEEE.

[86] Seliem, Mohamed and Elgazzar, Khalid. IoTeWay: A Secure Framework Architecture for 6LoWPAN Based IoT Applications. *2018 IEEE Global Conference on Internet of Things (GCIoT)*, pages 1–5, Alexandria, Egypt, 2018. IEEE.

[87] Sethi, Pallavi and Sarangi, Smruti R. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, 2017:1–25, 2017.

[88] Shaik, Altaf and Borgaonkar, Ravishankar and Park, Shinjo and Seifert, Jean-Pierre. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 221–231, Miami Florida, 2019. ACM.

[89] Sherburne, Matthew and Marchany, Randy and Tront, Joseph. Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid. *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*, pages 37–40, Oak Ridge, Tennessee, 2014. ACM Press.

[90] Simpson, Anna Kornfeld and Roesner, Franziska and Kohno, Tadayoshi. Securing vulnerable home IoT devices with an in-hub security manager. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 551–556, Kona, HI, 2017. IEEE.

[91] Singh, Anuj Kumar and Patro, B. D. K. Security Attacks on RFID and their Countermeasures. In Bhateja, Vikrant and Satapathy, Suresh Chandra and Travieso-Gonzalez, Carlos M. and Flores-Fuentes, Wendy, editors, *Computer Communication, Networking and IoT*, pages 509–518. Springer Singapore, Singapore, 2021. Series Title: Lecture Notes in Networks and Systems.

[92] Singh, Ashwini and Meshram, Sakshi and Gujar, Tanvi and Wankhede, P. R. Baggage tracing and handling system using RFID and IoT for airports. *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, pages 466–470, Pune, India, 2016. IEEE.

[93] Singh, Kapil. Security in RFID Networks and Protocols. *International Journal of Information and Computation Technology*, 3(5):425–432, 2013.

[94] Singh, Manmeet Mahinderjit and Adzman, KAAK and Hassan, Rohail. Near Field Communication (NFC) technology security vulnerabilities and countermeasures. *International Journal of Engineering & Technology*, 7(4.31):298–305, 2018.

[95] Singh, Saurabh and Sharma, Pradip Kumar and Moon, Seo Yeon and Park, Jong Hyuk. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Human Comput*, 2017.

[96] SndkCrop. Introduction on IoT with IoT Scope & 8 Protocols in details. 2019.

[97] Sruthy, S and George, Sudhish N. WiFi enabled home security surveillance system using Raspberry Pi and IoT module. *2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, pages 1–6, Kollam, 2017. IEEE.

[98] Stoyanova, Maria and Nikoloudakis, Yannis and Panagiotakis, Spyridon and Pallis, Evangelos and Markakis, Evangelos K. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Commun. Surv. Tutorials*, 22(2):1191–1221, 2020.

[99] Sun, Da-Zhi and Mu, Yi and Susilo, Willy. Man-in-the-middle attacks on Secure Simple Pairing in

Bluetooth standard V5.0 and its countermeasure. *Pers Ubiquit Comput*, 22(1):55–67, 2018.

[100] Sung, Yoonyoung and Lee, Sookyoung and Lee, Meejeong. A Multi-Hop Clustering Mechanism for Scalable IoT Networks. *Sensors*, 18(4):961, 2018.

[101] Sushanth, G. and Sujatha, S. IOT Based Smart Agriculture System. *2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pages 1–4, Chennai, 2018. IEEE.

[102] Talaviya, Gunjan and Ramteke, Rahul and Shete, A. K. Wireless fingerprint based college attendance system using Zigbee technology. *International Journal of Engineering and Advanced Technology (IJEAT)*, 2(3):201–203, 2013. Publisher: Citeseer.

[103] Tan, Ping and Wu, Han and Li, Peng and Xu, He. Teaching Management System with Applications of RFID and IoT Technology. *Education Sciences*, 8(1):26, 2018.

[104] Tanveer, Muhammad and Abbas, Ghulam and Abbas, Ziaul Haq and Bilal, Muhammad and Mukherjee, Amrit and Kwak, Kyung Sup. LAKE-6SH: Lightweight User Authenticated Key Exchange for 6LoWPAN-Based Smart Homes. *IEEE Internet Things J.*, 9(4):2578–2591, 2022.

[105] Tassone, Joseph and Biocchi, Mike. The Importance of Applying Security Practices in Wireless Communication: Bluetooth Low Energy and RFID. *Parallel Process. Lett.*, 28(03):1850010, 2018.

[106] Very Engineering Team. NFC and IoT: What You Need to Know. 2019.

[107] Valente, Fredy J. and Neto, Alfredo C. Intelligent steel inventory tracking with IoT / RFID. *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*, pages 158–163, Warsaw, 2017. IEEE.

[108] Vasseur, Jean-Philippe and Dunkels, Adam. Ip for smart objects. *White Paper*, 1:1–6, 2008. Publisher: IPSO Alliance.

[109] Verma, Abhishek and Ranga, Virender. CoSec-RPL: detection of copycat attacks in RPL based 6LoWPANs using outlier analysis. *Telecommun Syst*, 75(1):43–61, 2020.

[110] Verma, Abhishek and Ranga, Virender. Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors J.*, 20(11):5666–5690, 2020.

[111] Vila, JosÃ© and RodrÃ-guez, Ricardo J. Practical Experiences on NFC Relay Attacks with Android. In Mangard, Stefan and Schaumont, Patrick, editors, *Radio Frequency Identification. Security and Privacy Issues*, pages 87–103. Springer International Publishing, Cham, 2015. Series Title: Lecture Notes in Computer Science.

[112] Wang, Zhiqiang and Lin, Yuheng and Zhuo, Zihan and Gu, Jieming and Yang, Tao. GNFCVulFinder: NDEF Vulnerability Discovering for NFC-Enabled Smart Mobile Devices Based on Fuzzing. *Security and Communication Networks*, 2021:1–14, 2021.

[113] wikipedia. Bluetooth. 2021. Page Version ID: 1023095693.

[114] Wu, Jianliang and Nan, Yuhong and Kumar, Vireshwar and Tian, Dave Jing and Bianchi, Antonio and Payer, Mathias and Xu, Dongyan. {BLESA}: spoofing attacks against reconnections in Bluetooth low energy. *14th USENIX Workshop on Offensive Technologies (WOOT 20)*, 2020.

[115] Yan, Bo and Huang, Guangwen. Supply chain information transmission based on RFID and internet of things. *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, pages 166–169, Sanya, China, 2009. IEEE.

[116] Zhang, Wenbo and Wang, Jiaxing and Han, Guangjie and Huang, Shuqiang and Feng, Yongxin and Shu, Lei. A Data Set Accuracy Weighted Random Forest Algorithm for IoT Fault Detection Based on Edge Computing and Blockchain. *IEEE Internet Things J.*, 8(4):2354–2363, 2021.

[117] Zhang, Yue and Weng, Jian and Dey, Rajib and Jin, Yier and Lin, Zhiqiang and Fu, Xinwen. Breaking secure pairing of bluetooth low energy using downgrade attacks. *29th USENIX Security Symposium (USENIX Security 20)*, pages 37–54, 2020.