Received: 28 April 2022 | Revised: 21 September 2022 | Accepted: 19 October 2022

DOI: 10.1002/spy2.285

SURVEY PAPER

WILEY

Review of security issues in Internet of Things and artificial intelligence-driven solutions

Ali Kamil Abed | **Angesh Anupam**

Department of Computer Science, Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, UK

Correspondence
Ali Kamil Abed, Department of Computer Science, Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, UK.
Email: ali.kamil95@gmail.com

Abstract

Internet of Things (IoT) is a network of several hardware and software systems which is broadly based upon internet services and several state-of-the-art sensing and communication technologies. The emergence of 5G technology will witness a further surge in the growth of IoT across the world but simultaneously security concerns pertinent to the IoT technology also need rigorous evaluations. This article will present a thorough survey of the security challenges in an IoT network, recent cases of attacks on IoT technology, communication protocols prevalent in IoT systems and the role of artificial intelligence (AI) in IoT security. For the first time, all the major attributes related to IoT security along with potential solutions using AI are reviewed and articulated together. This work would act as a useful resource for understanding useful perspectives in future research focused around the development of more secured IoT communication protocols as well as AI tools for handling privacy and security in IoT.

KEYWORDS

AI in IoT, cyber-security, IoT, IoT vulnerability

1 | INTRODUCTION

The concept of the Internet of Things (IoT) was invented in 1999 by a member of the radio frequency identification (RFID) named Kevin Ashton, and over the decades it has become more relevant to the real world due to its technological advancement and its capabilities that it supplies to its users.[1] The IoT technology can be defined as a system of interrelated computing devices, digital machines, buildings, animals, physical objects, or individuals that are provided with the ability to interact, collect and exchange different types of data throughout its devices with or without human interaction.[2] The IoT is not a singular technology, however, it is a combination of different types of hardware and software machinery.[3] There are many technologies available in the market, that are operative and supported by strong machinery association alliances, which focus on delivering the necessary IoT requirements for various types of users. These types of machinery provide the users with privacy, security, and control over the actions and data being processed throughout the internet and its devices. Some examples of these technologies include short-range communication protocols such as Z-Wave, ZigBee, Sigfox, Wi-Fi, or Bluetooth.[4]

The IoT has seen a progression and a significant growth of communication and software technologies, which has shaped everyday life, leading the world into a new era of "Smart Things,"[5] where millions of objects are connected to one and other by sharing, communicating, and sensing information. All of these connections are based on private or public

Internet protocol (IP) systems. These connected objects analyze and collect information frequently, which enable the users to manage, plan, decision making, taking the appropriate action when needed.[6] A study projects that in 2030 there would be 125 billion IoT devices connected to the internet worldwide, which is a 12% increase on average annually, from nearly 27 billion in 2017.[7] The substantial growth of the IoT evolution and its technologies has resulted in privacy and security complications that have led to a data breach or data thefts. The IoT technology offers a lot of benefits, however, it also has its limitations which need to be carefully monitored.[5,8] It is important to understand the types of exposures, vulnerabilities, security, and privacy threats that IoT technology experiences. The purpose of hacker's malicious activities and attacks seek to target the vulnerabilities of IoT operating systems and technologies to cause damage or data theft.[9] Furthermore, malicious activities can vary, they could occur from unauthorized access, social engineering, malware, malicious insider as well as physical theft. By not having a robust system in place can result in serious consequences resulting in sensitive data being stolen.

The IoT can be categorized into three groups—technologies that manage security and privacy for its users, technologies that allow machines to obtain appropriate information, and technologies that allow machines to process consistent information.[4] In simple words, the first category states that IoT is pivotal for the security and privacy of customers whereas, the last two bring in the concept of intelligence embedded into IoT technology. The role of communication is pertinent in IoT and there should be varied types of communication machinery, which need to be placed in order to mark the requirements of the IoT-based applications. Some important requirements are security, speed, reliability, and energy efficiency. The popular communication protocols relevant to IoT are, ZigBee, Bluetooth, Sigfox, Wi-Fi, and Z-Wave.[10]

The IoT revolution is still a work in progress despite achieving several milestones in various areas. A lot of new approaches in IoT technology are sought after, particularly in its existing communication protocols and AI-based solutions to tackle the upcoming security threats. This study provides a comprehensive report on the common types of IoT security threats, recent cyber attacks dampening the faith in this evolving technology, various communication protocols popular in an IoT framework, and the artificial intelligence (AI) based solutions to deal with any potential cyber threats affecting the IoT network of interest. An exhaustive review of the latest reference literature including research papers, web-based articles and reports from the industry was carried out under this study. This article would serve as a resource for providing useful perspectives in future research focusing on the development of new communication protocols. This article would also augment the research works centered around harnessing AI and machine learning (ML) based tools to deal with smart attackers. The research questions of this review work can be summarized as (a) What are the types of security and privacy concerns for IoT networks? (b) What are the types of IoT communication protocols that empower its machinery and the scope of improvements in the existing protocols? (c) How can AI and ML techniques empower privacy and security for IoT devices?

The rest of this article is organized as follows. Section 2 describes various applications of IoT and the role of AI. Section 3 provides a comprehensive review of privacy and security challenges in IoT. Section 4 reflects upon some recent cyber-attacks on IoT services. Some popular communication protocols in IoT are presented in Section 5. The issues in the existing communication protocols are highlighted to serve as pointers for further research. Section 6 highlights some threats within an IoT environment, followed by a demonstrated threat model used for risk evaluation. Section 7 contains a review of the AI-based solutions useful in tackling potential security threats to IoT networks and all the stakeholders. The research outcomes of this study by appropriately linking to the posed research questions are discussed in Section 8. Finally, the concluding remarks and future implications of this research are presented in Section 9.

2 | VARIOUS APPLICATIONS OF IOT AND ROLE OF AI

There are many IoT applications offering capabilities to machines to interact with consumers, empowering their experience within smart environment. For example, smart locks, smart lighting, smart thermostats, smart sensors, and smart hubs. The use of smart locks, which are connected to the smart hubs, enables the user with peace of mind and security, allowing them to know who is coming in and going out of the territory. A smart lock can be remotely accessed anywhere in the world, through smart devices such as smartphones, which gives the users the ability to lock or unlock the doors and can hold up to 30+ individual unique codes to access the lock. In addition, smart lighting allows the user to control the lights remotely, brighten them, dim them, turn them on and off or change the lightening colors of it. Furthermore, this includes light switches, dimmers, outlets, relays, and plug-in modules. Installing the smart light technology within the environment can enable the user to create scheduled times to switch on the lights at different times, including when smart locks unlock the door when a person arrives. Additionally, smart lighting offers benefits to the user, including saving money on energy bills, saving time, and full control either remotely or via voice control within the environment. A smart thermostat is a technology that enables the user to take full advantage of the temperature within a smart home environment, accessed remotely anywhere in the world via a smartphone. The advantage of having this type of mechanism installed within a building or smart home enables the consumer to control energy usage, which saves money on energy bills. A smart sensor is a technology that can enable consumers to detect changes within the environment. For example, smoke detection, flood detection, and motion around the installed areas. Furthermore, having sensors installed within a smart building or home enables the user to act responsibly in case of an emergency, receiving notifications alerts via smartphones. Smart sensors empower users to take control of the environment. A smart hub is the main technology that controls all the other smart mechanisms within an environment, enabling the users the benefit from taking full control of the technological surroundings. It must be connected to a Wi-Fi router, to be fully compatible with other mechanisms, such as cameras, alarm panels, or thermostats. A user can operate this via smart apps using a smartphone.[11]

AI is driving the future of technologies into reality. For example, the automobile industry employs a good mixture of AI-based IoT, enabling consumers to drive their cars hands-free. The mechanism of using a self-driving vehicle is that it is loaded with sensors that are constantly monitoring everything that is occurring around the vehicle, with the use of AI application to make the correct decisions. The applied sensors within the vehicle enable it to capture thousands of data every millisecond and the use of AI empowers the data to act accordingly in a fast manner. The AI-enabled IoT capabilities in an automobile enable automatic parking, braking, and changing lanes, which is a huge impact on the future of driving.[12]

Healthcare is one of the most crucial and critical sectors in the broader landscape of big data. AI in healthcare is the introduction of computer systems that have the intelligence of humans to assist medical professionals in their daily work. The use of AI in healthcare empowers quality of life, and preventive care, providing more accurate treatments and diagnoses. Furthermore, AI enables healthcare professionals to track and predict the spread of infectious diseases by analyzing data from various sources.[13] The use of fitness trackers within healthcare such as the Apple Watch or Fitbit can assist with enabling the wellness and health of individuals at all costs. These smart wearable technologies can track individuals' activity levels, heart rate, and quality of sleep, which are all connected through Bluetooth and recorded via an app on smartphones.[14]

3 | PRIVACY AND SECURITY CHALLENGES

There are many challenges associated with the privacy and security of IoT technologies. The purpose of the intruders' malicious activities is to target the vulnerabilities of IoT operating systems and technologies to cause damage and data theft. Malicious cyber-attacks can vary, they could occur from unauthorized access, social engineering, malware, malicious insider as well as physical theft.[15]

3.1 | Cyber-attack

A cyber-attack within IoT can be defined as an assault toward networks/systems, by disturbing their operating functions and exploiting the weaknesses within it by using different types of hacking tools and methods. The purpose of a cybercriminal to strike a cyber-attack on technologies is to gain an advantage of the systems by retrieving valuable information, or for personal satisfaction. Furthermore, the attack, which is conducted by cybercriminals can vary, it can depend on the purpose of the attack and what sort of gain is achieved.[16] Cybercriminals can be of different types such as government bodies, groups of individuals, private companies etc. The players behind the cyber-attacks are the individuals who are the danger to the new era of the smart world.[17] Cyberattacks occur from gaining authentication data, passive attacks like monitoring unprotected system communication to exploit its vulnerabilities, and attacks on networks/software systems, which target the unencrypted traffic to seek valuable data.[18]

3.2 | Software and hardware systems challenges

Weaknesses can be found in many parts of the IoT operating systems or networks. Some of the main weaknesses that IoT devices experience are the software systems, networks, procedures, and policies that are used within the software systems. IoT has two different constituent systems, namely, software systems and hardware systems. It is further argued that the weaknesses can be spotted within the software system, for example in its application software, operating systems, or within its controls, such as gadget drivers and communication protocols. Moreover, there are many other ways, which could lead IoT technologies to experience vulnerabilities within their software systems, including software issues and human factors. Some of the main technical vulnerabilities occur from human errors because of the software design. On the other hand, having issues with the hardware system can be challenging to fix the vulnerabilities, even if the issues have been spotted within the hardware interoperability and compatibility. There can be consequences for not starting a project correctly, understanding the necessities, planning, and communicating correctly as developers and with users. Moreover, poor knowledge, management skills, and lack of resources could lead to vulnerabilities being inedited within an IoT system, which could expose the security and privacy of a user.[16] Organizations can invite complications due to a lack of planning in selecting an appropriate IoT application. Users and consumers can suffer due to personal information being stolen especially in industrial and commercial sites, for example, medical industries, where the patient's sensitive information can be taken due to the lack of resources implemented in the hardware and software systems.[19]

3.3 | Structured and unstructured attacks

There are two kinds of human threats which can be caused by people, they are "external" or "internal threat."[20] An external threat can be a group of individuals or a single individual working outside the system which looks to disturb or attack a network.[21] On the other hand, an internal attack can be caused by a group of people that has permitted accessibility within the systems.[22] Furthermore, it can be categorized into different types, such as unstructured attacks and structured attacks. Unstructured attacks can vary, they can be caused by hackers that utilize different types of hacking tools, to extract data or personal information from technologies.[23] The process of a structured attack can be caused by hackers or groups who understand and recognizes the weaknesses within a system, which could alter scripts and codes to take full control. Moreover, it is argued that the advanced persistent threat (APT) is an example of a structured attack. The APT is an experienced network attack which aims to target networks with high-value data. For example, governments, organizations, businesses, financial industries, and manufacturers attain valuable information.[24]

3.4 | Access and reconnaissance attacks

An access attack is used to gain access to unauthorized information targeting IoT devices or systems. It can be split into two groups, remote access attack and physical access attack.[18] The process of a physical attack is where the criminals gain entry to physical technologies whereas remote access is done over the internet through IP-linked gadgets. Moreover, the literature states that most IoT technologies that operate outdoors and are left unattended are highly targeted and vulnerable to these sorts of attacks from occurring.[18] A reconnaissance attack can be recognized as an attempt to collect and discover sensitive data in relation to an operating system. This type of attack may be disregarded by security officers as a "network noise" which is used in a denial-of-service (DoS) attack or subsequent access attack.[25] Some methods which are used to gain data from this sort of attack are by conducting illegal mapping and discoveries of networks, vulnerabilities, and services of technologies. Some example can be from packet sniffers,[26] requesting IP address data or scanning the system ports.[27]

3.5 | Denial-of-service and viruses

Supervisory control and data acquisition (SCADA) attacks focus on Internet protocol/transmission control protocol (IP/TCP) by exploiting the vulnerabilities within it. It can come as a DoS attack which is a type of distributed attack used by cybercriminals to launch numerous attacks on a target using "innocent computers" which are also known as zombies, that are on different sites. It is a form of ransomware, which takes over a network/system. Moreover, it can also come in like a virus that looks to affect the technologies associated with the internet and take control of data.[28] IoT devices are extremely vulnerable to such attacks happening.

A virus is defined as a malicious program or a code, implemented to change the behavior and actions of an operating system.[29] Computer-virus function by placing themselves in files that support instructions to perform their malicious codes. The virus is easily transmittable and can move to another technology. Some of the major signs of a computer virus can be recognized while operating a computer system, for example, frequent pop-up windows, unusual slow device performance, frequent crashes, and unusual activities such as access password changes.

3.6 | Ransomware

Malware is malicious software that includes various types of malicious components, for example, spyware, viruses, trojans, and ransomware.[30] A "ransomware" is malware, which can be split into two words, ransom, and ware. A "ransom" stands for the sum of money required to be paid, while the "ware" indicates it is a malware type of attack. IoT experiences major ransomware attacks, in which the intruders attempt to target the victim's data and encrypt it by using robust algorithms to make the system or data inaccessible. Once the system is affected by the malware, the intruder demands a ransom which is normally paid in "Bitcoin" a form of cryptocurrency which is not traceable, in return for a decryption key for the victims to attain access to the stolen data.[31] Demand is often given a deadline for the victims to pay, after which the information will be erased if the payment has not been made.[32] Some organizations refuse to make a payment of this ransom and spend a large amount of money to attain the lost files and rebuild the systems. There are different ways where ransomware can get attached to a device. Cybercriminals use phishing methods to attack a target, in which malicious software is attached either to an email, link, or advertisement where the victim is lured to click for a piece of information which in reality is a malicious one. Moreover, a lack of cybersecurity training can lead to such things from reoccurring.[33]

3.7 | Dictionary and brute force

Some of the most common privacy issues which IoT and its technologies face are password-based attacks. This method is used by individuals or groups to attempt to duplicate a valid user password and to crack down passwords by using two techniques, it includes, dictionary attack and brute force attack. A dictionary attack is where the hackers attempt to try different combinations of letters and numbers to gain the user's password. On the other hand, a brute force attack is a hacking tool which is used by intruders to try to crack down all sorts of combinations of passwords in order to achieve the correct password of the users.[18]

3.8 | Authentication and authorization

Authentication is similarly important as authorization when confirming and permitting access. IoT networks comprise a colossal number of gadgets. Most of these gadgets need to be connected to networks to process or produce sensitive information. Furthermore, for the information to be transmitted and received to the gateway of the IoT, it must authenticate itself. Default credentials set by the manufacturers without changing the gadgets can result in security and privacy challenges.[34] A research study conducted by a Slovakian Internet security company called ESET in 2016 studied privacy and security challenges within internet routers. The study tested 12 000 routers and 15% of them had weak security. The findings which the study was able to identify a high percentage of the routers had weak and insecure username and password, which was default credentials as "admin," which makes it easy for the hackers to gain access to.[35]

4 | RECENT ATTACKS ON IOT TECHNOLOGIES

4.1 | Frantic locker (Flocker) smart TV attack

In 2015, this type of ransomware was detected on android phone lock screens and progressed to smart TV the following year. As soon as this type of ransomware enters the smart TV, it locks and shuts it down, which also makes the reset factory settings unavailable. Moreover, the Flocker malware then displays a message on the screen stating that it is from a law enforcement agency, such as the United States cyber police, which then demands them to pay a ransom. This demands the victim to pay the ransom through cryptocurrency, with a 200-dollar gift card delivered through iTunes, for the victim to gain access to the smart TV.[36]

4.2 | Smart bulb attack

Many commercial IoT devices do not fulfill vigorous authentication mechanisms, which makes the devices vulnerable to exposure, including replay attacks such as commercial smart bulbs. A showcasing test was conducted which enabled them to produce a secret channel for launching a ransomware strike within an organization by utilizing a device like an office scanner.[37] The scanner created a gateway, a secret channel between the attacker and the malware which was used to intrude into the organization. To breach the security system of the organization, the sensitivity of the light's scanner was exploited which could be controlled by the intruders who were located far away. If the IoT devices are not correctly secured with an effective safety protocol, it can lead the technologies from being taken full control and making the IoT networks hostage.[36] The study[37] performed an attack on a commercial smart bulb and managed to change the brightness of the bulb by 5% and to switch the bulb states in 25 ms in frequency levels that a human eye cannot detect.

4.3 | Mirai distributed denial of service attack on IoT

Mirai is one of the largest distributed denial of service (DDoS) attacks ever recorded.[38] In 2016, the malware targeted thousands of IoT technologies that were connected to the internet infecting and exploiting the vulnerabilities within it, accomplishing an aggressive ability of about 1.2 terabits per second and using methods such as dictionary attacks based on 60 entries. The attack impacted half of Europe and the United States taking down its internet for a long period of time.[5] The process of Mirai started by scanning the Internet for hosts with an open telnet port where it pursued to gain access to devices if the password credentials were weak. Hence, after it gained access, Mirai installed the malware and monitored the command and control (CNC). Lastly, once the malware got triggered, the CNC taught all the bots within the network to generate a flood of traffic to overpower the target. The key architecture of Mirai is based on the Agent Handler model, which is put into preparation by the following plausible mechanisms:

- CNC server: This is where the components cooperate with users, allowing them to take control of the botnet. It is associated with a database and supports three actors within the system, namely, the bot, admin, and user. The mode of operation of these three actors can be described here:
  - Bot: This is when the Mirai worm operates and infects the IoT appliances. The worm connects to the CNC server, operated by the botnet which corresponds regularly, waiting for further commands to be distributed.
  - Admin: This is the main actor who performs several operations, such as setting up new attacks, tallying the existing bots, and controlling the database by adding new users to it.
  - User: This is the paying consumer which receives login credentials.
- The Mirai botnet: This botnet is the main component running on an infected IoT and it composes of three submodules and the main module.
  - The scanner: This is where the module scans for weaknesses within the IoT technology. Once the weaknesses have been identified, it then reports back to the reporting server.
  - The killer: A module which aims to destroy possible rival malware within the same device.
  - The attacker: A module which aims to execute DDoS attacks when requested from the CNC servers.
- Reporting server: The servers that are in control of obtaining results of the vulnerable information from the bots and redirecting to the loader server.
- Loader server: The mechanism used by the intruders to operate the Mirai worm is conducted in a "rapid scanning phase," targeting vulnerable technology, such as video recorders, printers, and routers.[39]

5 | COMMUNICATION PROTOCOLS IN IOT

5.1 | Sigfox

Sigfox technology was founded in 2009 by Christophe Fourtet and Ludovic Le Moan and is currently operating in more than 60 countries worldwide, covering 5 million km^2.[40] The firm's headquarter is based in Labège, France, the country's well-known "IoT Valleys." The technology is one of the most representative low-powered wide-area network (LPWAN) systems among the other LPWAN operators. It is a cost-efficient technology that provides connectivity between the cloud and its IoT devices.[41] The technology consumes low power, which empowers the battery to stay connected for a long period of time. Moreover, it has been argued that the technology has 10 years of battery lifespan and is the cheapest IoT service provider for consumers among the other service providers.[42] The Sigfox protocol stack consists of the application layer, transport layer, medium access control (MAC) layer, and physical layer. The physical layer controls the demodulation and modulation and the framing mechanisms process during the reception and transmission of the protocol signal.[43]

This communication protocol mainly operates within cities around the world and can connect from 1 to 1000 devices.[40] Sigfox is a cellular wireless communication that functions over a long distance with its technologies that offers custom arrangements fundamentally for low-throughput IoT and machine-to-machine (M2M) applications by benefiting its end-to-end network administrations utilizing its licensed machinery. The modulation which Sigfox utilizes within its end gadgets is binary phase-shift keying (BPSK) to interact with its base positions. It enables IoT technologies to interact within long distances to the networks,[44] and enables messages which has a fixed bandwidth of 100 Hz to be sent with a speed of 100 bps.[45] Sigfox utilizes a standardization of Sigfox-based-network collaboration with ETSI[46] and enables a distance range of 10 km urban and 40 km rural for its technologies to connect between its sensor nodes and gateways.[47] In event of free space line of sight (LOS) and connection, the signal can travel over 1000 km.[48] Additionally, the body of Sigfox can send a maximum of 140 messages 12 bytes long per day to a base station. All the messages include payload of (uplink 96 bits/downlink 64 bits), preamble (uplink 32 bits/downlink 32 bits), device identifier (uplink 32 bits/downlink 32 bits), frame synchronization (uplink 16 bits/downlink 13 bits), frame check sequence (uplink 16 bits/downlink 8 bits) and authentication codes (uplink 16–40 bits/downlink 16 bits).[42]

The official webpage of Sigfox[40] mentions some security principles implemented within the networks. It utilizes a star topology, in which many technologies transmit its messages to Sigfox network base stations. Every single base station deployed by Sigfox around the world is connected to a cloud system. Once a radio signal is sent reaching the base station within the range, the data is then transmitted into the Sigfox cloud system through a point-to-point link using an encrypted virtual private network (VPN). The Sigfox base stations report, demodulate and detect the messages into the cloud, which then is transmitted to the IT servers. These cloud systems utilize hypertext transfer protocol secure (HTTPS) encrypted interfaces for the websites, call-backs and APIs. Sigfox provides an end-to-end authentication technique, which is built on a secret key. The secret key is accumulated in a non-accessible memory associated with a visible and fixed ID kept in read-only memory. The secret key, which is utilized by the data transmitted by the devices creates a unique, signature for each message, that validates the sender. Each message is sent randomly three times at three different frequencies to protect the radio frames against sniffing, which gives the system a robust security protocol. The most pre-eminent areas where Sigfox technology can be installed and adapted are in smart buildings and manufacturing sectors, this is due to its low cost and long battery life.[47]

5.2 | ZigBee protocol

ZigBee is a short-range communication protocol that was created by ZigBee Alliance, which operates as a wireless technology for IoT. This technology is used in many fields including homes, industries, medical and military fields. It has a range of radio bandwidth which is used to transmit the total amount of data per unit. The bandwidth that the technology carries out is a minimum of 915 MHz and a maximum transmittable rate of 2.4 GHz per unit 49. Additionally, the data rate which it is used to transmit its information from one device to another is from 20, 40, 100, and 250 kbps. Although ZigBee has its advantages in transmitting data from one device to another, it can also connect a maximum of 64 000 devices within a range of 30 m mainly indoor.[49] The protocol has been evolving for a long period of time based on its standardization layers. The layers which are designed within the technology provide exclusive features for the IoT that are connected within a smart home, for example, low power, easy usage, high security, and low cost.[50] The ZigBee utilizes star and mesh topologies which enables its routers to spread their communication to other networks.[51] The purpose of this technology is to operate within the IoT, which supports the data coming from different sensors within different smart technologies. It operates through a control system, Hub, and sensors which are connected to the internet and Bluetooth.[52]

The standardization layer which ZigBee utilizes is Institute of Electrical and Electronics Engineers 802.15.4 (IEEE 802.15.4) which is built within the layers of the network.[53] A physical and MAC layer is built within the IEEE standard. The main layers within the specification are the application layer, network layer, and ZigBee device object (ZDO).[54] Apart from the two high-level networks, ZDO allows the users to manage, join networks, access device roles, and attain efficient security for IoT technologies.[55] The network layer consists of mesh, star, and tree topology which is processed within the network.[51] The networks must ensure that it is connected to one coordinator through the internet, to operate and control their maintenance and parameters. The personal area network coordinator (PANC) is the main coordinator that enables devices to bind, start, and path data within their networks and technologies.[51] On the other hand, the full function device (FFD) is the router, which is typical, within the powered gadgets and its purpose is to act as the network coordinator. The reduced function device (RFD) is the end device within the network that enables information to route between the networks. The RFD can only communicate to FFD devices and is proposed for simple tasks such as switching off and on functions.[56]

The ZigBee protocol is considered a robust and strong network, which enhances the security of its devices.[57] Moreover, the use of a mesh network within the protocol allows strong privacy for its stakeholders. The ZigBee protocol utilizes encryption methods within its layer, such as data authentication, data encryption, 32/64/128-bit encryption, and the advanced encryption standard (AES) algorithm. These encryption methods are utilized within the IoT devices which use a symmetric key encryption.[58] A vast number of organizations use ZigBee, such as Amazon Alexa and Samsung Smart Things. ZigBee technology enhances the control of systems, appliance control, safety system, and surveillance, which enables stakeholders to control its technologies.[59,60] There are some complications that the user could experience while install ZigBee within the desired environment. It is mainly designed for short-range distance and replacing the currently installed technology can be costly.[61]

5.3 | Bluetooth protocol

Bluetooth is a technology named after the 10th century Danish King, Harold Bluetooth, which is a hot subject among other wireless developing providers. The technology has an open specification that is governed by the Bluetooth Special Interest Group (SIG), which is led by five founding companies and other four companies that were added in 1999. Currently, there are more than 1200 companies associated with Bluetooth SIG.[62] The Bluetooth protocol is a short-range wireless communication that is utilized by many empowering technologies to communicate between each other.[63] Bluetooth wireless technology delivers peer-to-peer communications over its devices.[64] This communication technology is standardized as IEEE 802.15.1 specification, which is used to enable the capabilities and functionalities of its technology for its users.[65] The wireless application offers AES 128-bit- encryption security feature, which ensures that information cannot be sniffed over the air.[66] For it to provide information confidentiality and usage protection, it offers security measures in both the link layer and application layer. The three basic security features which Bluetooth offers in its standards are:

- Authorization: Ensuring the device is fully authorized before allowing it to gain access and control of its resources.
- Authentication: Validating the device's communication and its identity based on its Bluetooth address. Moreover, it does not offer native authentication for its users.
- Confidentiality: Ensuring only approved connected devices can access transmitted data and view it by avoiding data compromise triggered by eavesdropping.

Bluetooth technology has three types of security modes, namely, security mode 1, security mode 2, and security mode 3.[62] Security mode 1 offers no security enforcement for its devices, suggesting that the device which is connected is essentially taking no steps to protect itself against intruders. Security mode 2 imposes security at the service level, which means the application might be safe but without any extra device protection, while security mode 3 provides the highest level of security mechanisms to any intrusions to its connected devices. This wireless technology is considered as a low-power, low-profile and low-cost that offers the opportunity for its technology to generate small wireless systems on an ad-hoc foundation.[67] Regardless of its features, Bluetooth supports approximately up to 10 m range for its technologies to stay connected and must be close to one other. The wireless communication operates at a frequency of 2.4 GHz radio bandwidth and transfers information at a rate of 2 Mbps.[68] Bluetooth utilizes a frequency hopping spread spectrum (FHSS) to achieve an increased data rate up to 3 Mbps.[69] Bluetooth personal area network (PAN) supports up to 7 connected technologies and enables the system to occupy up to 250 kB of network resources. The use of Bluetooth frequency hopping spread spectrum (FHSS) is aimed to operate in noisy radio frequency environments, enabling it to use frequency-hopping and fast acknowledgement. Furthermore, the wireless technology's radio modules are designed to prevent intrusion from other signals by hopping to a new frequency, after it has received or transmitted a package.[62] Bluetooth is compatible with different technologies, this includes electronic technologies, computers, entertainment networks, and cell phones. It is much more convenient for hands-free applications.[68] What makes the technology so unique is that it can exchange data among a range of fixed and mobile devices and can handle both voice and data transmissions simultaneously.[70] However, a major drawback of this wireless technology is that it can easily lose connection if it goes near its maximum compatible range.[71]

5.4 | Z-Wave protocol

Z-Wave technology is an implementation of a complete IoT substratum, comprising well-specified networking, application, and communication layer protocols. The protocol composes capable actuators, controllers, sensors, internet gateways, and routers to provide office and home automation services.[72] The Z-Wave is a low-powered and low-cost communication protocol that empowers technologies within smart homes, to enable users to take control of security cameras, thermostats, windows, lights, locks, and medical equipment.[73] It is a short-range radio frequency, wireless communication protocol developed by Zensys for the use of smart home applications using the internet and Bluetooth devices.[74] The International Telecommunication Union (ITU) G.9959 specification is the registered standard in which Z-Wave operates and utilizes AES symmetric 128-bit encryption. It is the same encryption that is used in many banks, which enables the protocol to act securely.[73] This protocol utilizes 300 and 200 series chips which do not offer many security services.[75]

The Z-Wave system's architecture has two types of mechanisms—controllers and slaves.[76] Z-Wave system's architecture consists of four different layers which include the MAC layer, transfer layer, routing layer, and application layer, which enable the network to control how information is being switched within technologies. Controllers are the technologies that control other Z-Wave technologies, while the slaves are the devices that are controlled by other Z-Wave machinery. Z-Wave is a wireless mesh topology system that operates at 900 MHz radio bandwidth that may support the capacity of connected 232 devices.[77] This protocol supports transmission of small data up to 100 kbps and covers a distance of up to 100 m point-to-point (P2P) connectivity.[78] Z-Wave offers some benefits for its users and security protocols, however, it is argued that to maintain the security of the network and prevent unauthorized access, the user will require some knowledge of the network wires, as the technology utilizes frequency transmission, which makes it vulnerable for intruders to gain access to its network.[79] Some of the features which Z-Wave technology holds is that it is developed in C++ and is portable to most Mac OS, Windows, and Linux platforms. The pairing operation, which the protocol utilizes allows devices to pair with one another similarly to Bluetooth pairing. In a Z-Wave protocol, the device needs to be paired with the controller, which is usually accomplished by pressing the switch or resetting the device.[80] Some examples of Z-Wave controllers which operate under the protocol are Eon Labs Z-Stick and Verde Vera.

5.5 | Wi-Fi

The term "Wi-Fi" is also known as wireless fidelity, which enables users to connect to the internet within a premise without having to connect to wires. It is a wireless technology, which enables the IoT to receive and send information outdoors and indoors, within the range of the base station.[81] The architecture of Wi-Fi consists of a base station that is connected to a wireless host that gives access to network resources. The base station is in control of receiving and sending information to and from wireless hosts. The connectivity of these two components is operated via a wireless communication link. The link of the communication is in charge of transporting the data between the hosts and the base station.[82] Furthermore, Wi-Fi wireless technology is an enabled communication wireless system, which empowers IoT technologies, such as hubs, tablets, smartphones, computers, etc. The wireless system has a range of 10–100 m connectivity distance with a data rate operating from 11–54 Mbps per device. The topology in which the system operates is star and mesh. It has authentication and encryption of AES block cipher and RC4 Stream. Currently, IEEE 802.11ah is the most recent Wi-Fi developed a base standard that the wireless system is currently utilizing. However, the established Wi-Fi IEEE 802.11 base standard is efficient at the nearest access point and has complications with users who have large size homes. The latest standard enables IoT applications with greater range, easier connectivity, and ultra-low power for its technologies.[83] The wireless system has a minimum bandwidth of 2.4 GHz and a maximum of 5 GHz per unit, empowering its system's operation to reduce complexity. Applications and technologies in a smart home utilize a range of different wireless network protocols, like ZigBee, Z-Wave, Bluetooth, and Wi-Fi.[83] The main advantage of Wi-Fi is that it is cost-effective and does not require expensive wiring installed. It offers compatibility with many smart technologies, which can interoperate with other networks.[84] On the other hand, some of the weaknesses it holds are that it limits the mobility of the users to move around, and this can result in loss of connectivity. Other drawbacks of wireless technology are that it can interfere with other devices, high power necessities, impedance from different gadgets because of utilizing somewhat jam-packed transmission bandwidth, security, communication misfortunes affected by obstructions, and lack of inter-operability.[85]

6 | THREAT MODEL

A threat is defined as an act that takes a gain over the weakness of a security system and impacts it negatively.[86] There are two primary sources from which a threat can originate: natural causes and human causes. There are many ways in which natural causes could occur, such as floods, hurricanes, earthquakes, or even fire which could damage technologies severely. In situations such as natural causes, some safeguards could be implemented to prevent such devastations from happening. Common ways to approach natural causes are contingency plans and natural catastrophe recovery strategies such as backing up the data.[87] There are two kinds of human threats which can be caused by people, they are "external" or "internal" threats.[20] An external threat can be a group of individuals or a single individual working outside the system which looks to disturb or attack a network.[21] On the other hand, an internal attack can be caused by a group of people that has permitted accessibility within the systems.[22]

The term "threat" model can be defined as a risk evaluation and a mitigation exercise that allows the ability of a network environment to become more secure. Threat modeling involves communication and understanding the threats to the computing network environment. It is crucial to understand how to mitigate and reduce the risks in applications, systems, and network-aware devices and to be aware of the types of threats that these components encounter.[88] The model can be used in different incompatible and perhaps distinct ways and can be interpreted differently. It can mean isolating risks into groups such as tampering or constructing a set of idealized attackers. In simple terms, it is the use of concepts to support the thinking of complication threats. The first step of threat modeling to a network system to is utilize the information that is already gathered.[89]

There are various threat models which can be used in an IoT environment.[90] These models are security cards; attack trees; hybrid threat modeling method; persona non grata, attack trees; quantitative threat modeling method; operationally critical threat, common vulnerability scoring system; process for attack simulation and threat analysis model; LINDDUN model, which can be expanded as linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance; Microsoft STRIDE model, which is an acronym of six threat categories, which are spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. This study examines the STRIDE model and the types of threats that are violated within an IoT environment, which are shown in Figure 1.

A threat that is targeted within an IoT environment such as smart cities, smart homes, health care, or agriculture can be originated from inside or outside the network, known as a cyber-attack. Some of the threat sources include but are not restricted to hackers, phishers, criminal groups, bot-network administrators, malware creators, and spyware creators. An intruder can take advantage of compromised technology like smart bulbs, smart TV, and hubs to infect and control the applications, for example, ransomware. Furthermore, an invader can interfere with a Bluetooth pairing correspondence between two smart devices and disguise themselves as the genuine sender or receiver to complete further assaults on the application networks. If the user is not familiar with the specification of a wireless network, a device can easily lose connection if it goes near its maximum permissible distance, eventually resulting in major drawbacks of the technology. Moreover, with the use of Z-Wave, it is argued that to maintain the security of the network and prevent unauthorized access, the user will require some knowledge of the network wires, as the technology utilizes frequency transmission, which makes it vulnerable to intruders to gain access to its network.[79] Additionally, intruders, who target smart applications within a smart home, stealing vulnerable data, can place users in a vulnerable position of their information being exposed. Attackers can gain access to vulnerable devices, targeting credentials that are set by default, resulting in privacy and security complications for their devices.

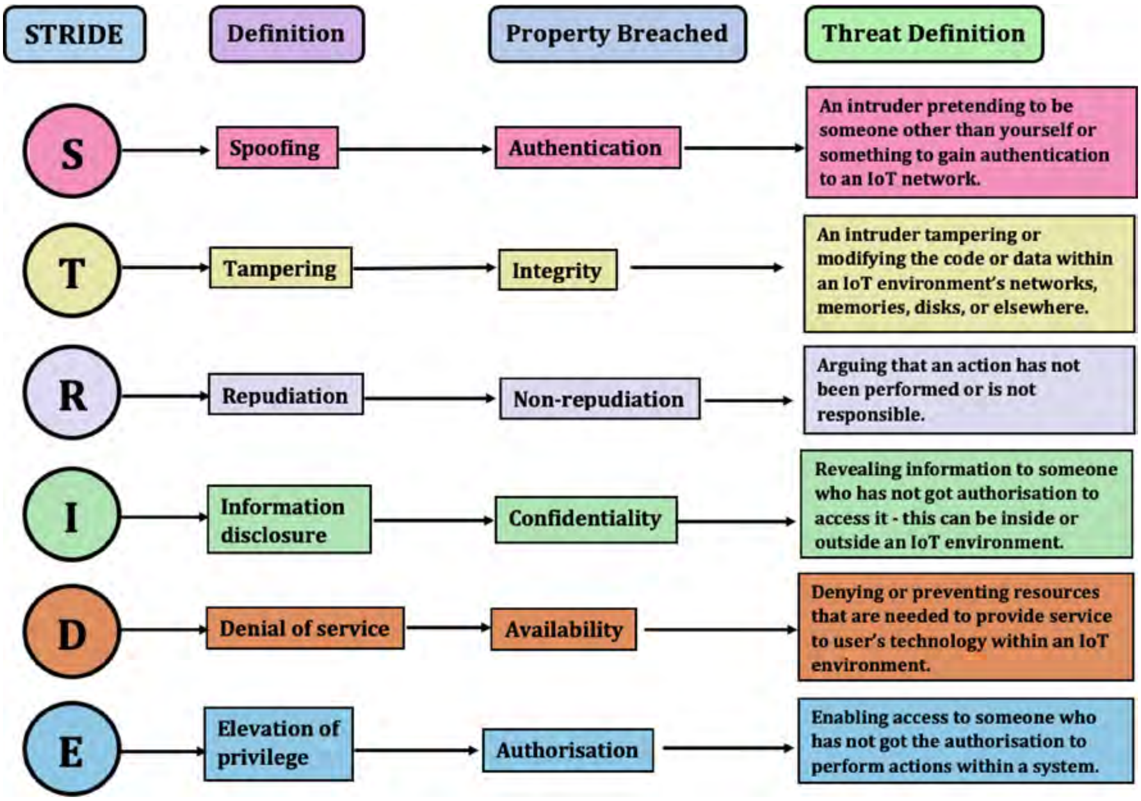
STRIDE
Definition
Property Breached
Threat Definition
S
Spoofing
Authentication
An intruder pretending to be someone other than yourself or something to gain authentication to an IoT network.
T
Tampering
Integrity
An intruder tampering or modifying the code or data within an IoT environment's networks, memories, disks, or elsewhere.
R
Repudiation
Non-repudiation
Arguing that an action has not been performed or is not responsible.
I
Information disclosure
Confidentiality
Revealing information to someone who has not got authorisation to access it - this can be inside or outside an IoT environment.
D
Denial of service
Availability
Denying or preventing resources that are needed to provide service to user's technology within an IoT environment.
E
Elevation of privilege
Authorisation
Enabling access to someone who has not got the authorisation to perform actions within a system.

FIGURE 1 STRIDE threat model classifications for IoT environment

7 | AI IN IOT SECURITY

In this section, we will investigate the role of AI in ensuring the security of an IoT network. AI is a recreation of human intelligence and discernment which are administered by computer machine systems to perform certain tasks. It processes distinctive human behavior, such as the ability to learn from previous involvements, discover meanings, generalizes, or reason specific tasks. The field of AI encompasses ML and deep learning, which gives the systems the ability to automatically improve and learn from experiences.[91] The three popular learning algorithms are supervised learning techniques, unsupervised learning techniques, and reinforcement learning techniques.[92]

The revolution of IoT smart technologies, enabling to act and sense, makes the IoT framework efficient. The increase of smart technologies that are connected to the systems creates a large volume of information, which is a challenging task to perform and process in an IoT environment. According to Cisco Systems, Inc. (CISCO), there will be an estimated 70 billion devices connected by 2024.[93] An IoT encircles an excessive number of actuators, sensors information handling, and information storage capacities interconnected by the internet. In this way, any IoT-empowered gadget can detect its environmental elements, communicate, store, and cycle the information assembled, and act in a like manner. The genuine perceptiveness of an IoT is not entirely settled by the degree of handling or acting that it can perform. A non-smart IoT network will have restricted capacity and will not be able to develop with the information. In any case, a smarter IoT network will have AI and may serve the real objective of adaptation and automation. AI is the art of imparting knowledge to machines so they can do assignments that customarily required the human mind. Simulated intelligence-based frameworks relevant to IoT are advancing quickly concerning the application, variation, managing speed, and capacities.[94] AI performs computations intelligently and can embed smartness in an IoT system as well as intelligently augment the security of the system. In an AI-driven IoT system, decisions should be taken before any undesired situation occurs. This could be possible if robust AI models form the basis of an IoT system. Additionally, it is essential to address the security complication within an IoT network, to make the network further robust.[95] There could be more than one framework for AI-based IoT. Some interesting mechanisms and frameworks can be found in these literatures.[96-99] AI can improve the accuracy rate, and operational efficiency, and improve the analysis of a system.[95] It has been proved that IoT's large amount of data within a real-time frame enables their AI system to become more accurate.[94] Implementing AI and its techniques enable IoT technology for growing to its true potential. The technologies within IoT are often created with not-so-great arrangements for security, and hence AI implementation can play major roles while dealing with cyber threats.[100] Therefore, it is essential to understand the types of algorithms and techniques which AI and ML provide.[53,101] The robustness of any AI-based application is highly related to the quality of the data. A reliable data collection framework is highly recommended to mitigate any sort of trust deficit.[102]

The use of supervised learning techniques can enable IoT devices to evaluate activities and timings within IoT applications in order to detect malware.[103] The implementation of supervised learning techniques utilizes a preparation set to instruct models to their desired outputs. The preparation dataset incorporates inputs and right yields, which permit the model to learn after some time. Moreover, the input information which is inserted within the model alters its weights through a reinforcement learning process, which enables the model to fit correctly. The use of its algorithms quantifies its precision through the loss function, changing until the mistake has been adequately limited.[104] The regression technique is a type of supervised learning which focuses on forecasting, predicting, and identifying relations between primary datasets.[105] Some popular regression algorithms are, linear regression, polynomial regression, and logistic regression.[104] Unlike regression, the classification techniques focus on recognizing, analyzing and sorting data patterns into categories to make a response. For example, it can be used in labeling security threats in an IoT network. The classification algorithms accurately assign data into different groups by testing, labeling, and defining them.[104]

Artificial neural network (ANN) is a model class which tries to replicate the neurons associated with the human brain. ANN, for instance, can be utilized to label the network traffic for IoT devices. Applying support vector machines (SVMs) into the network can detect spoofing attacks[106] and intrusion within the networks.[107] The K-nearest neighbors (KNN) and random forest classifier play a crucial role in identifying malicious ransomware and interruption within the IoT system.[108,109] Moreover, the use of deep neural network (DNN) can be utilized to detect spoofing attacks within IoT technologies, if it has memory and adequate computation resources.[110] The implementations of these techniques empower IoT technologies to identify activities within the system to prevent specific malicious activities from occurring. An experiment was conducted on IoT devices to identify malicious activities within its applications using ML techniques in a study.[109] Moreover, the use of random forest and K-NN classification techniques were applied within this experiment model to spot malware. The use of random forest and K-NN classification techniques enabled the malware detection scheme to produce a 99.7% and 99.9% detection rate to spot malware within the IoT system. A genetic-KNN-based ML model for malicious activities recognition in water-based Industrial Internet of Things (MARWIIoT) is used in a recent work.[111] Different ML approaches are reviewed in Reference 112 to identify malicious activities within android-based systems.

Under unsupervised learning, it is crucial to understand the underlying techniques and how it empowers IoT systems without human interventions. Unsupervised learning utilizes different approaches and algorithms to function its operations. It is a machine learning algorithm which is widely used for clustering, analyzing, grouping and discovering hidden patterns within datasets without requiring human interference within the process.[104] Unsupervised learning approaches can be split into different categories, which include, association mining, clustering, latent variable models, anomaly detection, etc. Association mining can support identifying matters that occur frequently within the dataset. This can be very useful for detecting some frequently occurring security concerns in an IoT network. The clustering approach as mentioned previously, allows the system to manage and split similar datasets into groups, while anomaly detection can identify unfamiliar activity within the datasets. Moreover, the use of latent variable models focuses on processing the information, for example dropping different types of features within a dataset. The advantage of this model is that it will flag any unusual points within the systems.[113]

Reinforcement learning techniques consist of different algorithms, such as Dyna-Q, post decision state (PDS), deep Q-network (DQN), and Q-learning.[114] It is a type of ML technique where an operating agent learns to perform a task through repetitive error and trail exchanges with a dynamic situation.[115] The use of reinforcement learning techniques operates agents within its environment that learn and make better verdicts from involvements, which are interacting with the operation. Moreover, these functional agents within the model function learn by experience and reward themselves depending on the instructions that are given.[116] Implementing reinforcement algorithms within IoT can enable its devices to select a security protocol that can restrict types of threats.[107] Furthermore, the use of Q-learning empowers IoT devices to enhance their privacy and security by improving the performance of malware detection and authentication.[103] A general architecture for detecting potential IoT security threats using ML tools is shown using Figure 2.

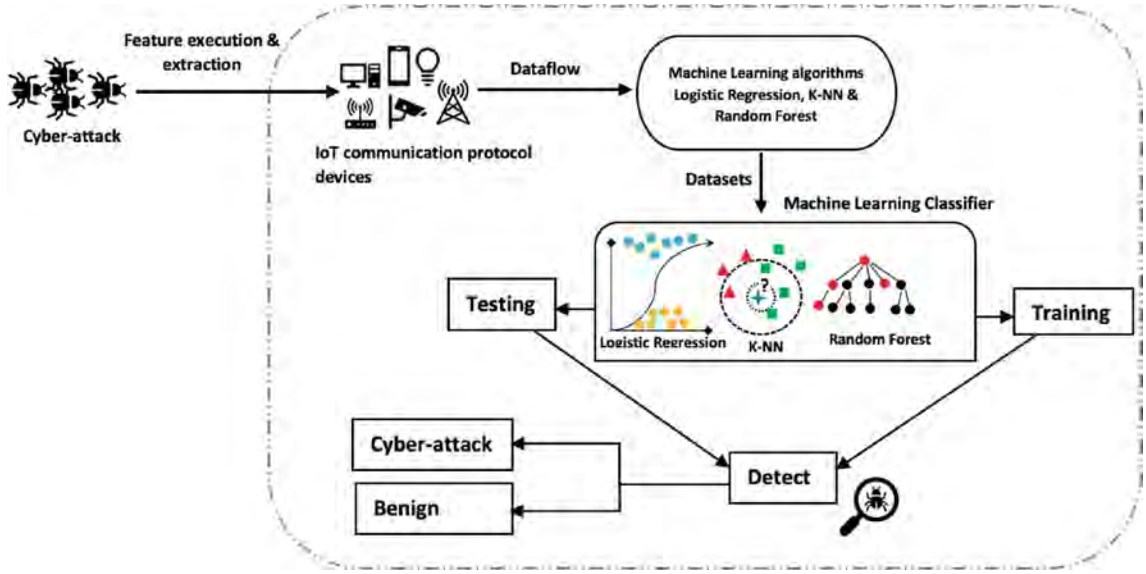
Feature execution & extraction
Cyber-attack
Dataflow
IoT communication protocol devices
Machine Learning algorithms Logistic Regression, K-NN & Random Forest
Datasets
Machine Learning Classifier
Testing
Training
Logistic Regression
K-NN
Random Forest
Cyber-attack
Benign
Detect

FIGURE 2 The general architecture for mitigating IoT security threat under an AI framework

TABLE 1 Comparative performance analysis of the various security protocols

Characteristics	ZigBee	Z-Wave	Bluetooth	WiFi	Sigfox
Max range	30 m	100 m	10 m	10–100 m	10 km urban–40 km rural 1000 km free space
Max data rate	250 kbps	100 kbps	2 Mbps	11–54 Mbps	100 bps
Max bandwidth	915 MHz–2.4 GHz	900 MHz	2.4 GHz	2.4–5 GHz	100 Hz
Network size	64 000 devices	232 devices	7 devices	250 devices	1–1000 devices
Topology	Mesh, star, cluster free tree	Mesh	Point-to-point piconet and scatternet	Star, mesh	N/A
Base standard	IEEE 802.15.4	ITU G.9959	IEEE 802.15.1	IEEE 802.11 ah	Sigfox based/network
Authentication/encryption	AES symmetric 32/64/128-bit encryption	AES symmetric 128-bit encryption	AES symmetric 128-bit encryption	RC4 stream and AES block cipher	Not supported

8 DISCUSSION

In this section, we will summarize how the findings of this study are linked to the proposed research questions. We discussed privacy and security in the IoT and the types of challenges it encounters. Furthermore, the research also identified the scalability of information that is being generated and transferred throughout IoT and how much cyberattacks have increased over the years. In May 2020 alone, 8.8 billion data breaches were recorded which shows a worrying threat toward the privacy and security of IoT. This study has revealed that intruders can gain access to individuals' personal information by data mining, cyber spying, tracking, eavesdropping and other methods of exploiting IoT devices. The study identified the most recent attacks on IoT and how they can impact the security and privacy of its devices. For example, the Mirai (DDoS) attack on IoT was one of the largest cyberattacks ever recorded infecting and identifying weak credentials, exploiting the vulnerabilities of devices, and controlling them.

Various types of IoT communication protocols were investigated during this study. Table 1 highlights the major differences among these protocols. It can be observed from the table that the short-distanced protocol Z-Wave supports its

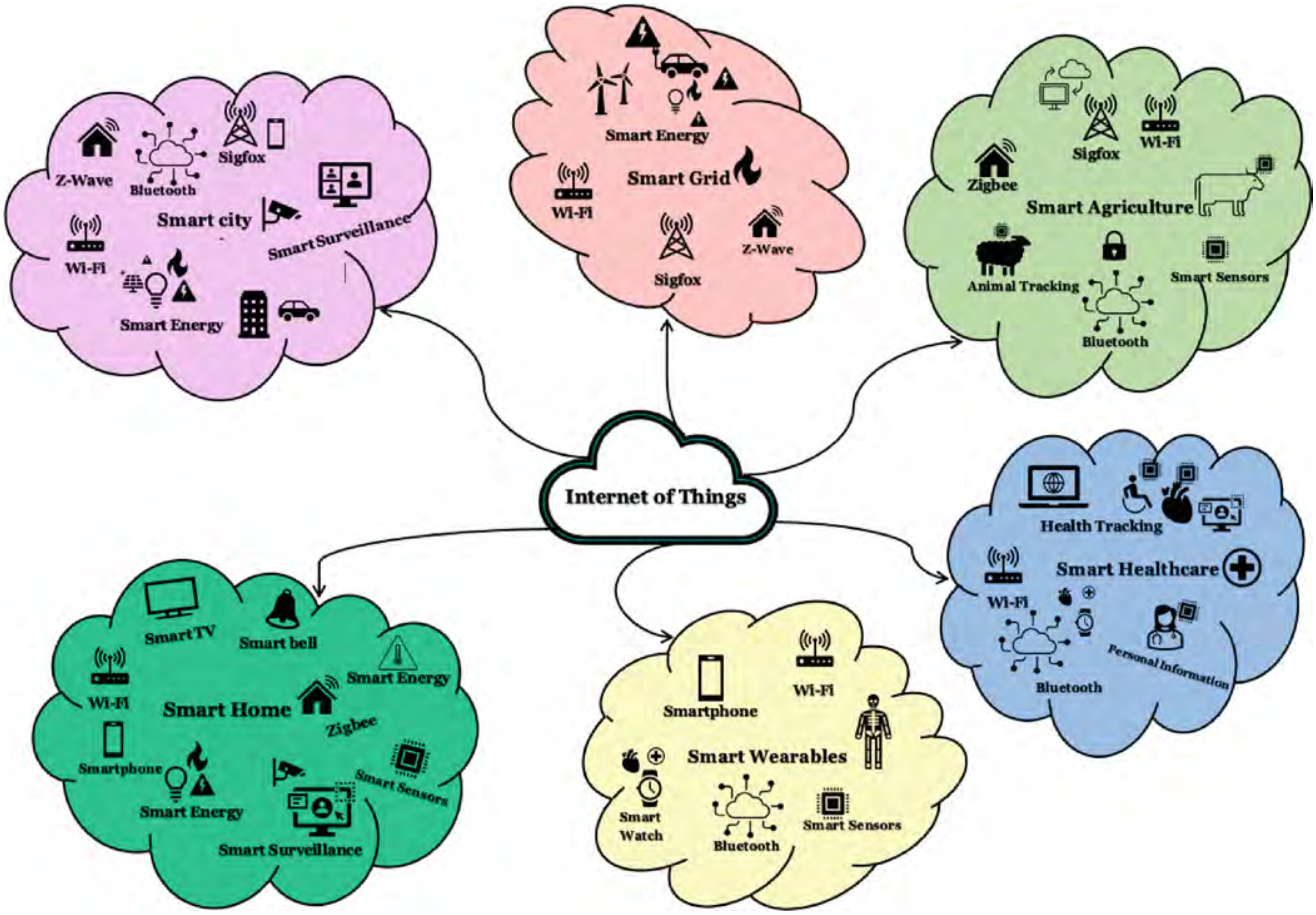

FIGURE 3 Pictorial representation of communication model of IoT

connected devices with up to 100 m making it one of the dominant protocols in range compared to ZigBee's 30 m, WiFi's 10–100 m, and Bluetooth's 10 m maximum range. Sigfox however supports up to 10 km urban or 40 km rural range. Furthermore, the results indicate that Wi-Fi supports a maximum data rate of 54 Mbps, which makes it a dominant player over ZigBee's 250 kbps, Bluetooth's 2 Mbps Sigfox's 100 bps, and Z-Wave's 100 kbps maximum data rate. However, the results from Table 1 indicate that the most predominant overall short-range communication protocol is ZigBee due to its support, maximum bandwidth, network size, AES authentication/encryption, bass standard, and topologies. These features make it the most suitable protocol for stakeholders to utilize. Table 1 also states that Sigfox can be utilized for a long-distance communication protocol, which is more suitable for a wider range. A pictorial representation of some popular use cases under various communication protocols are shown in Figure 3.

The survey of AI and ML methods in this study enabled us to understand how these methods can manage and enhance privacy and security for the IoT with minimal human involvement. Some key literature on experimental research, related to AI applications in IoT security was reviewed in this study. Through these available data, KNN and random forests can be regarded as powerful tools for detecting Malware in an IoT system. Moreover, the role of neural networks and deep learning in handling security threats in IoT have also been appreciated in recent literature. In summary, it can be argued that modern days security threats affecting our IoT systems require smart technologies as solutions. Therefore, AI encompassing several state-of-the-art ML techniques can serve as a suitable tool for ensuring security in an IoT network.

9 | CONCLUSION

In this study, we first investigated the security and privacy concerns of IoT networks. With the massive growth in fast internet connectivity, sensor networks, communication systems, and advanced instrumentation systems, IoT technology has witnessed a surge in the recent few decades. This growth has resulted in various types of privacy and security challenges. In this study, we presented the necessary details about most of these challenges while trying to find the common links among them. To substantiate the implications of these challenges we evaluated the recent attacks on IoT technology. The next part of the study included a survey of the various popular communication protocols empowering the machinery of IoT along with evaluating the scope of improvements in the currently used protocols. In the final phase of this study, we surveyed the role of AI and ML approaches in augmenting the strengths of security and privacy in IoT systems. The novelty of this survey lies in the amalgamation of all the major pillars related to the security and privacy of IoT systems along with some plausible solutions to those issues. A thorough review of the AI approach for dealing with security and privacy is in sync with the parallel advancement in AI technologies and computing infrastructure required for the deployment of AI-based solutions. The findings of this study would serve as the recipe for implementing a new secured IoT system, for mitigating the risks associated with the existing IoT systems, as well as for pointing toward the required research in AI for enabling nearly full-proof large IoT systems. Future investigations related to IoT security could consider, AI embedded chips for security and privacy mechanisms of IoT. Blockchain solutions within IoT networks and the integration of AI and cloud systems could be pivotal in future research works to augment the security and privacy of IoT technology. These areas could empower the ongoing study to recognize further opportunities for IoT technology.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Ali Kamil Abed https://orcid.org/0000-0002-9740-3417
Angesh Anupam https://orcid.org/0000-0002-1472-9367

REFERENCES

1. Ashton K. That "Internet of Things" thing. *RFID Journal*. 2009;22(7):97-114.
2. What is IoT (Internet of Things) and How Does it Work? Definition from TechTarget.com. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT. Accessed September 18, 2022.
3. Patel KK, Patel SM. Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *Int J Eng Sci Comput*. 2016;6(5):6122-6131.
4. Vermesan O, Friess P. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg: River Publishers; 2013.
5. Moh M, Raju R. Machine learning techniques for security of Internet of Things (IoT) and fog computing systems. 2018 International Conference on High Performance Computing & Simulation (HPCS); 2018:709-715. IEEE.
6. Dash S, Prusty D. Domain-specific IoT applications. In: Kumar Pani S, Pandey M, eds. *Internet of Things: Enabling Technologies, Security and Social Implications*. Singapore: Springer; 2021:27-36.
7. IoT_ebook.pdf. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf. Accessed October 29, 2021.
8. Samaila MG, Neto M, Fernandes DA, Freire MM, Inácio PR. Challenges of securing Internet of Things devices: a survey. *Secur Priv*. 2018;1(2):e20.
9. Irwin L. It governance blog: How do data breaches happen? https://www.itgovernance.co.uk/blog/understanding-the-different-types-of-data-breaches; 2020.
10. Vermesan O, Friess P. *Internet of Things—From Research and Innovation to Market Deployment*. Vol 29. Aalborg: River Publishers; 2014.
11. Better and safer smart homes are built on Z-Wave. Z-Wave. https://www.z-wave.com/. Accessed September 3, 2022.
12. 31 Top artificial intelligence examples you should know 2022. Built In. https://builtin.com/artificial-intelligence/examples-ai-in-industry. Accessed September 3, 2022.
13. What is AI in Healthcare? Arm®. https://www.arm.com/glossary/ai-in-healthcare. Accessed September 3, 2022.
14. AI in Healthcare (+5 ways it's used in 2020). https://www.g2.com/articles/ai-in-healthcare. Accessed September 3, 2022.
15. IT Governance Blog: how do data breaches happen? https://www.itgovernance.co.uk/blog/understanding-the-different-types-of-data-breaches. Accessed October 28, 2021.
16. Kizza JM. *Guide to Computer Network Security*. Vol 8. Cham: Springer; 2013.
17. Schneier B. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons; 2015.
18. Abomhara M, Køien GM. Cyber security and the Internet of Things: vulnerabilities, threats, intruders and attacks. *J Cyber Secur Mobil*. 2015;4:65-88.
19. What are the 3 challenges IoT is currently facing? 360DigiTMG. https://360digitmg.com/what-are-the-3-challenges-iot-is-currently-facing. Accessed September 3, 2022.
20. Dahbur K, Mohammad B, Tarakji AB. A survey of risks, threats and vulnerabilities in cloud computing. Proceedings of the 2011 International Conference on Intelligent Semantic Webservices and Applications; 2011:1–6.

21. Baybutt P. Assessing risks from threats to process plants: threat and vulnerability analysis. *Process Saf Prog*. 2002;21(4):269-275.
22. Duncan AJ, Creese S, Goldsmith M. Insider attacks in cloud computing. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications; 2012:857-862. IEEE.
23. Tankard C. Advanced persistent threats and how to monitor and deter them. *Netw Secur*. 2011;2011(8):16-19.
24. Li F, Lai A, Ddl D. Evidence of advanced persistent threat: a case study of malware for political espionage. 2011 6th International Conference on Malicious and Unwanted Software; 2011:102-109. IEEE.
25. Burton J. *Cisco Security Professional's Guide to Secure Intrusion Detection Systems*. Boston: Syngress Publishing; 2003.
26. De Vivo M, Carrasco E, Isern G, De Vivo GO. A review of port scanning techniques. *ACM SIGCOMM Comput Commun Rev*. 1999;29(2):41-48.
27. Ansari S, Rajeev S, Chandrashekar H. Packet sniffing: a brief introduction. *IEEE Potentials*. 2003;21(5):17-19.
28. Ormiston K, Eloff MM. Denial-of-service & distributed denial-of-service on the Internet. ISSA; 2006:1-14.
29. What is a computer virus? Norton. https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html. Accessed October 28, 2021.
30. What is malware? Defined, explained, and explored. Forcepoint. https://www.forcepoint.com/cyber-edu/malware. Accessed October 28, 2021.
31. Song S, Kim B, Lee S. The effective ransomware prevention technique using process monitoring on android platform. *Mob Inf Syst*. 2016;2016:2946735.
32. Viruses vs. ransomware: types of malware explained. Cisco. https://www.cisco.com/c/en/us/products/security/virus-vs-ransomware.html. Accessed October 28, 2021.
33. Allen J. Surviving ransomware. *Am J Fam Law*. 2017;31(2):65-68.
34. Sadique KM, Rahmani R, Johannesson P. Towards security on Internet of Things: applications and challenges in technology. *Procedia Comput Sci*. 2018;141:199-206.
35. The Internet turned on itself in Friday's big attack. Archer. https://archerint.com/internet-turned-fridays-big-attack/. Accessed October 28, 2021.
36. Zahra SR, Chishti MA. Ransomware and Internet of Things: a new security nightmare. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence); 2019:551-555. IEEE.
37. Nassi B, Shamir A, Elovici Y. Oops! … I think I scanned a malware. arXiv preprint arXiv:1703.07751; 2017.
38. De Donno M, Dragoni N, Giaretta A, Spognardi A. DDoS-capable IoT malwares: comparative analysis and Mirai investigation. *Secur and Commun Netw*. 2018;2018:7178164.
39. Acarali D, Rajarajan M, Komninos N, Zarpelão BB. Modelling the spread of botnet malware in IoT-based wireless sensor networks. *Secur and Commun Netw*. 2019;2019:3745619.
40. Sigfox—The global communications service provider for the Internet of Things (IoT). https://www.sigfox.com/en. Accessed March 31, 2022.
41. Hernandez D, Peralta G, Manero L, Gomez R, Bilbao J, Zubia C. Energy and coverage study of LPWAN schemes for Industry 4.0. 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM); 2017:1-6. IEEE.
42. Hemjal MA. Sigfox Based Internet of Things: Technology, Measurements and Development [master's thesis]. Tampere: Tampere University; 2019.
43. Chen S, Xu H, Liu D, Hu B, Wang H. A vision of IoT: applications, challenges, and opportunities with China perspective. *IEEE Internet Things J*. 2014;1(4):349-359.
44. What is Sigfox—basics, architecture and security features. https://circuitdigest.com/article/what-is-sigfox-basics-architecture-and-security-features. Accessed March 31, 2022.
45. Lavric A, Petrariu AI, Popa V. Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions. *IEEE Access*. 2019;7:35816-35825.
46. ETSI—Welcome to the world of standards!. https://www.etsi.org/. Accessed September 8, 2022.
47. Mekki K, Bajic E, Chaxel F, Meyer F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*. 2019;5(1):1-7.
48. Centenaro M, Vangelista L, Zanella A, Zorzi M. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. *IEEE Wirel Commun*. 2016;23(5):60-67.
49. Mouftah HT, Erol-Kantarci M, Obaidat M, Anpalagan A, Woungang I. Smart grid communications: opportunities and challenges. In: Obaidat M, Anpalagan A, Woungang I, eds. *Handbook of Green Information and Communication Systems*. Vol 2013. Amsterdam: Elsevier; 2013:631-663.
50. Obaid T, Rashed H, Abou-Elnour A, Rehan M, Saleh MM, Tarique M. ZigBee technology and its application in wireless home automation systems: a survey. *Int J Comput Netw Commun*. 2014;6(4):115-131.
51. Yi X, Jia Z, Chen N, Zhu W, Wu Z. The research and implementation of zigbee protocol-based Internet of Things embedded system. 2010 2nd International Symposium on Information Engineering and Electronic Commerce; 2010:1-4. IEEE.
52. What is ZIGBEE wireless mesh networking? https://www.digi.com/solutions/by-technology/zigbee-wireless-standard. Accessed August 30, 2021.
53. The IoT needs artificial intelligence. IEEE Innovation at Work. https://innovationatwork.ieee.org/iot-needs-artificial-intelligence/. Accessed August 30, 2021.

54. Hacking ZigBee networks. Infosec Resources. https://resources.infosecinstitute.com/topic/hacking-zigbee-networks/. Accessed September 3, 2022.
55. IEEE 802.15.4 (ZigBee radio) technology. http://www.drhdmi.eu/dictionary/ieee-802-15-4.html. Accessed September 3, 2022.
56. Farahani S. *ZigBee Wireless Networks and Transceivers*. London: Newnes; 2011.
57. Zillner T, Strobl S. ZigBee exploited—the good, the bad and the ugly. Black Hat; 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf. Accessed March 21, 2018.
58. Secure your data with aes-256 encryption. https://www.atpinc.com/blog/what-is-aes-256-encryption. Accessed August 30, 2021.
59. Huraj L, Šimon M, Horák T. Resistance of IoT sensors against DDoS attack in smart home environment. *Sensors*. 2020;20(18):5298.
60. Fältros J, Alinger I, von Bergen A. Safety Risks with ZigBee Smart Devices: Identifying Risks and Countermeasures in ZigBee Devices with an Eavesdropping Experiment [Dissertation]. Jönköping: Jönköping University; 2020.
61. Gislason D. *ZigBee Wireless Networking*. London: Newnes; 2008.
62. Kaur J, Kaur R, Kaur M. Bluetooth technology. *Int J Eng Comput Sci*. 2016;5:16001-16003.
63. Short-range wireless communication: Bluetooth, ZigBee & Infrared Transmission—video & lesson transcript. Study.com. https://study.com/academy/lesson/short-range-wireless-communication-bluetooth-zigbee-infrared-transmission.html#lesson. Accessed August 29, 2021.
64. Stirparo P, Loeschner J, Cattani M. Bluetooth Technology: Security Features, Vulnerabilities and Attacks. JRC Scientific and Technical Reports; 2011.
65. Bluetooth technology website. https://www.bluetooth.com/. Accessed August 29, 2021.
66. Bray J. *BlueTooth Application Developer's Guide*. Boston: Syngress; 2002.
67. Yeh TC, Peng JR, Wang SS, Hsu JP. Securing Bluetooth communications. *Int J Netw Secur*. 2012;14(4):229-235.
68. Short-range wireless communication: Bluetooth, ZigBee & Infrared Transmission—video & lesson transcript. Study.com. https://study.com/academy/lesson/short-range-wireless-communication-bluetooth-zigbee-infrared-transmission.html#lesson. Accessed October 28, 2021.
69. Frenzel L. *Electronics Explained: Fundamentals for Engineers, Technicians, and Makers*. London: Newnes; 2017.
70. Does Bluetooth have a future?—Essential guide. https://www.computerweekly.com/feature/Does-Bluetooth-have-a-future-Essential-Guide. Accessed October 28, 2021.
71. 4 advantages and disadvantages of Bluetooth—drawbacks and benefits of Bluetooth. https://www.hitechwhizz.com/2020/03/4-advantages-and-disadvantages-drawbacks-benefits-of-bluetooth.html. Accessed October 28, 2021.
72. OZW utilities. http://openzwave.com/home/. Accessed September 3, 2022.
73. Abdelmoumen R. A review of link layer protocols for Internet of Things. *Int J Comput Appl*. 2019;182(46):22-28.
74. What is Z-Wave protocol and its role in smart home automation solutions. https://circuitdigest.com/article/understanding-z-wave-protocol-and-its-role-in-home-automation. Accessed August 29, 2021.
75. Z-Wave security. Silicon Labs. https://www.silabs.com/wireless/z-wave/specification/security. Accessed August 29, 2021.
76. Gomez C, Paradells J. Wireless home automation networks: a survey of architectures and technologies. *IEEE Commun Mag*. 2010;48(6):92-101.
77. Koutras D, Stergiopoulos G, Dasaklis T, Kotzanikolaou P, Glynos D, Douligeris C. Security in IoMT communications: a survey. *Sensors*. 2020;20(17):4828.
78. Salman T, Jain R. Networking protocols and standards for Internet of Things. In: Geng H, ed. *Internet of Things and Data Analytics Handbook*. Vol 7. Hoboken, NJ: Wiley; 2015:14-18.
79. Pros and cons of Z-Wave. Pros an Cons. https://prosancons.com/technology/pros-and-cons-of-z-wave/. Accessed October 28, 2021.
80. Badenhop CW, Graham SR, Ramsey BW, Mullins BE, Mailloux LO. The Z-Wave routing protocol and its security implications. *Comput Secur*. 2017;68:112-129.
81. Suresh C, Vidhya V, Vishupriya J, Muthulakshmi R, Menaka S. Wireless fidelity. *Int J Res Comput Appl Robot*. 2016;4:50-59.
82. Nwabueze CA, Akaneme S. Wireless fidelity (Wi-Fi) broadband network technology: an overview with other broadband wireless networks. *Niger J Technol*. 2009;28(1):71-78.
83. Samuel SSI. A review of connectivity challenges in IoT-smart home. 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC); 2016:1-4. IEEE.
84. Olexa R. *Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations*. Amsterdam: Elsevier; 2004.
85. Cetinkaya O, Akan OB. Use of wireless sensor networks in smart homes. In: Rehmani MH, Pathan AK, eds. *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*. Boca Raton, FL: CRC Press; 2016:233-258.
86. Brauch HG. Concepts of security threats, challenges, vulnerabilities and risks. *Concepts of Security Threats, Challenges, Vulnerabilities and Risks*. Berlin, Heidelberg: Springer; 2011:61-106.
87. Turban E, Rainer RK, Potter RE. *Introduction to Information Systems: Supporting and Transforming Business*. New York: John Wiley & Sons, Inc.; 2007.
88. Johansson JM. Network threat modeling. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003; 2003:10. IEEE Computer Society.
89. Shostack A. *Threat Modeling: Designing for Security*. New York: John Wiley & Sons; 2014.
90. Al Asif MR, Hasan KF, Islam MZ, Khondoker R. STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI); 2021:1-6. IEEE.

91. Artificial intelligence—Definition, Examples, and Applications. Britannica. https://www.britannica.com/technology/artificial-intelligence. Accessed August 29, 2021.
92. Sagu A, Gill NS. Machine learning techniques for securing IoT environment. *Int J Innov Technol Explor Eng*. 2020;9(4):978-982.
93. Čolaković A, Hadžialić M. Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues. *Comput Netw*. 2018;144:17-39.
94. Ghosh A, Chakraborty D, Law A. Artificial intelligence in Internet of Things. *CAAI Trans Intell Technol*. 2018;3(4):208-218.
95. Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*. 2020;11:100227.
96. Kotenko I, Saenko I, Branitskiy A. Framework for mobile Internet of Things security monitoring based on big data processing and machine learning. *IEEE Access*. 2018;6:72714-72723.
97. Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MSH. Application of big data and machine learning in smart grid, and associated security concerns: a review. *IEEE Access*. 2019;7:13960-13988.
98. Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P. Network intrusion detection for IoT security based on learning techniques. *IEEE Commun Surv Tutor*. 2019;21(3):2671-2701.
99. Anthi E, Williams L, Słowińska M, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet Things J*. 2019;6(5):9042-9053.
100. Wang S, Qiao Z. Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments. *IEEE Access*. 2019;7:88693-88704.
101. Canedo J, Skjellum A. Using machine learning to secure IoT systems. 2016 14th Annual Conference on Privacy, Security and Trust (PST); 2016:219–222. IEEE.
102. Elkhodr M, Alsinglawi B. Data provenance and trust establishment in the Internet of Things. *Secur Priv*. 2020;3(3):e99.
103. Xiao L, Wan X, Lu X, Zhang Y, Wu D. IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? *IEEE Signal Process Mag*. 2018;35(5):41-49.
104. IBM United Kingdom—United Kingdom—IBM. https://www.ibm.com/uk-en. Accessed August 29, 2021.
105. Talabis MRM, McPherson R, Miyamoto I, Martin JL, Kaye D. Chapter 1—Analytics defined. In: Talabis MRM, McPherson R, Miyamoto I, Martin JL, Kaye D, eds. *Information Security Analytics*. Boston: Syngress; 2015:1-12.
106. Ozay M, Esnaola I, Vural FTY, Kulkarni SR, Poor HV. Machine learning methods for attack detection in the smart grid. *IEEE Trans Neural Netw Learn Syst*. 2015;27(8):1773-1786.
107. Alsheikh MA, Lin S, Niyato D, Tan HP. Machine learning in wireless sensor networks: algorithms, strategies, and applications. *IEEE Commun Surv Tutor*. 2014;16(4):1996-2018.
108. Branch JW, Giannella C, Szymanski B, Wolff R, Kargupta H. In-network outlier detection in wireless sensor networks. *Knowl Inf Syst*. 2013;34(1):23-54.
109. Narudin FA, Feizollah A, Anuar NB, Gani A. Evaluation of machine learning classifiers for mobile malware detection. *Soft Comput*. 2016;20(1):343-357.
110. Shi C, Liu J, Liu H, Chen Y. Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. Mobihoc'17. ACM; 2017; New York, NY, USA: Association for Computing Machinery.
111. Selim GE, Hemdan EED, Shehata AM, El-Fishawy NA. An efficient machine learning model for malicious activities recognition in water-based industrial Internet of Things. *Secur Priv*. 2021;4(3):e154.
112. Ham HS, Kim HH, Kim MS, Choi MJ. Linear SVM-based android malware detection for reliable IoT services. *J Appl Math*. 2014;2014:594501.
113. What is unsupervised machine learning? DataRobot. https://www.datarobot.com/wiki/unsupervised-machine-learning/. Accessed August 30, 2021.
114. He X, Dai H, Ning P. Improving learning and adaptation in security games by exploiting information asymmetry. 2015 IEEE Conference on Computer Communications (INFOCOM); 2015:1787-1795. IEEE.
115. MathWorks—Makers of MATLAB and Simulink. MATLAB & Simulink. https://uk.mathworks.com/. Accessed August 30, 2021.
116. BRKSDN-2263.pdf. https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSDN-2263.pdf. Accessed August 30, 2021.

How to cite this article: Abed AK, Anupam A. Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*. 2022;e285. doi: 10.1002/spy2.285