Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:.1117
doi: 10.56294/sctconf2024.1117

Category: STEM (Science, Technology, Engineering and Mathematics)

ORIGINAL

Examining IoT in the angle of security with counter measures: a study

Examinando IoT desde el ángulo de la seguridad con contramedidas: un estudio

R. Parameswari[1], D. Raj Balaji[1]

[1]Research Scholar, Rathinam College of Arts and Science, Rathinam TechZone Campus, Eachanari, Coimbatore, 641021, Tamil Nadu, India. [2]Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Rathinam TechZone Campus, Eachanari, Coimbatore, 641021, Tamil Nadu, India.

Cite as: R. P, Raj Balaji D. Examining IoT in the Angle of Security with Counter measures: a Study. Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:.1117. https://doi.org/10.56294/sctconf2024.1117

Submitted: 02-02-2024 **Revised:** 13-05-2024 **Accepted:** 31-08-2024 **Published:** 01-09-2024

Editor: Dr. William Castillo-González

Corresponding author: R. Parameswari

ABSTRACT

Introduction: the collective networks of linked objects and technologies that enable communications between items and systems, including clouds, are referred to as Internet of Things (IoT). Recent decades of technological developments have paved the way for society to continue becoming more digitally integrated.
Method: IoT has turned into a massive network of smart gadgets that communicate online and grown into a new technological paradigm. The possibility that IoT may involve storing of sensitive data online, security is an essential component. Regrettably, the biggest obstacle to IoT technology adoption is security. Therefore, enhancing the security of IoT devices is currently the top concern for industries and academics.
Results: a sizable corpus of research on the topic covers a number of problems and possible solutions. But the majority of current research falls short of providing a thorough analysis of assaults within IoT.
Conclusion: the goal of this IoT investigation is to provide guiding information on dangers and assaults, followed by a thorough review of defense mechanisms against important IoT security attacks.

Keywords: IoT; Challenges and Opportunities; Iot Attacks; Vulnerabilities; Detection Methods.

RESUMEN

Introducción: las redes colectivas de objetos y tecnologías vinculados que permiten las comunicaciones entre elementos y sistemas, incluidas las nubes, se denominan Internet de las cosas (IoT). Las últimas décadas de desarrollos tecnológicos han allanado el camino para que la sociedad siga integrándose digitalmente.
Método: IoT se ha convertido en una red masiva de dispositivos inteligentes que se comunican en línea y ha crecido hasta convertirse en un nuevo paradigma tecnológico. Ante la posibilidad de que IoT implique el almacenamiento de datos confidenciales en línea, la seguridad es un componente esencial. Lamentablemente, el mayor obstáculo para la adopción de la tecnología IoT es la seguridad. Por lo tanto, mejorar la seguridad de los dispositivos IoT es actualmente la principal preocupación de las industrias y los académicos.
Resultados: un corpus considerable de investigaciones sobre el tema cubre una serie de problemas y posibles soluciones. Pero la mayoría de las investigaciones actuales no llegan a proporcionar un análisis exhaustivo de los ataques dentro de IoT.
Conclusión: el objetivo de esta investigación de IoT es proporcionar información orientativa sobre peligros y ataques, seguida de una revisión exhaustiva de los mecanismos de defensa contra importantes ataques de seguridad de IoT.

Palabras clave: IoT; Desafíos y Oportunidades; Ataques IoT; Vulnerabilidades; Métodos de Detección.

INTRODUCTION

IoT is a collective term for networks of interconnected devices and technologies that allow items to communicate with one other and with the cloud. Current reduced costs have resulted in processing by small devices. For instance, light switches can have integrated RAM of less than 1MB added to enable phone service accesses. The goal of equipping homes, workplaces, and organizations with IoT devices is that they can automatically transfer data to and from the Internet—has given rise to an entire industry. IoT includes a variety of sensing devices for real-time acquisitions of environmental data. IoT encompasses graphical user interfaces, software, and smart devices. Televisions, security cameras, and fitness equipment with computational capability are examples of smart gadgets. They gather information from their surroundings and transfer that information over the internet. Applications are groups of software and services that combine data from different IoT devices and analyze them for conclusions using artificial intelligence (AI) and ML technologies. Graphical user interfaces can be used to manage a fleet of devices or IoT devices. IoT is compatible with several upcoming and enabling technologies including Wireless Sensor Networks (WSNs) which are made up of sensors placed in sensing areas to track changes such environmental monitoring.[1] IoT has transformed internet's functioning, increasing the degree of interconnectedness between cyberspaces and humans (physical) systems. The term "internet of things" was popularized by Kevin Ashton (1999) who used radio frequency identification (RFID) in supply chains.[2] IoT refers to objects or devices that can be liked to the internet by academicians, governmental and other organizations in multiple applications. National Intelligence Council (NIC) of the United States projected that anything from plants to food packages, cars, furniture, and more may have sensors installed. The tentative uses of IoT devices throughout time are shown in figure 1.

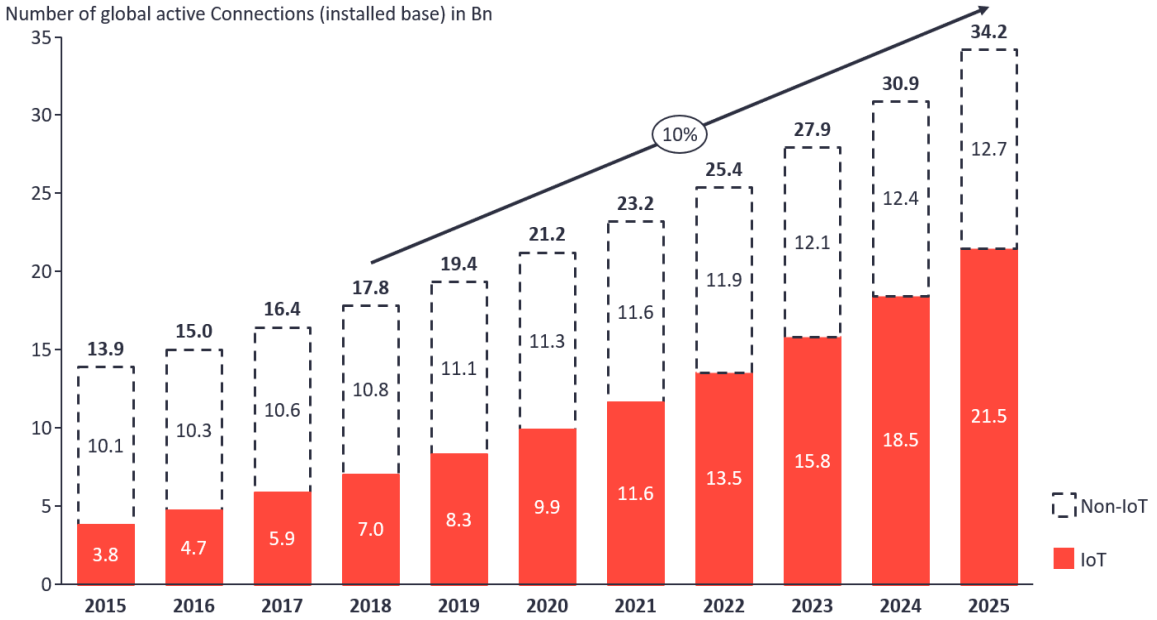

Figure 1. Active Global Connections in Billions

Typical examples of IoT applications include websites or mobile apps where smart gadgets are mabaged. Moreover, even more widespread network configurations are being developed, in which every conceivable device—mostly heterogeneous—connects with every other device to detect, collect, and analyze data of various kinds, acting on the intelligence derived from profound understanding of the data. Most of these acts don't involve any human contact.[3] There are several methods for connecting automobiles, including autos, to the internet. Infotainment systems, smart dashcams, or even the car's linked gateway can do it. Data is gathered from the wheels, fuel tanks, odometer, speedometer, brakes, and accelerator to track driver performance and vehicle health. There are several applications for linked autos. (1) tracking rental car fleets for reducing costs and enhancing fuel efficiencies; (2) tracking driving habits of users; (3) automatically informing friends and family in the case of an accident; and (4) anticipating and averting vehicle repair requirements. Enhancing home networking and increasing safety and efficiency are the key goals of smart home technology. Smart thermostats and smart outlets, for example, offer more precise temperature management and power use monitoring. IoT

https://doi.org/10.56294/sctconf2024.1117

sensors might be used by hydroponic systems to manage gardens. Home automation applications for linked devices include the following: (1) automatically shutting down inactive devices; (2) managing and maintaining rental properties; (3) recovering missing objects, such as wallets or keys; and (4) automating everyday tasks like dusting and making coffee. IoT technology help to improve infrastructure maintenance and urban planning efficiency. Governments are using IoT applications to solve challenges in healthcare, radiations and air quality measurements, and identifying necessary repairs for vital infrastructure like roads, bridges, and pipelines, and revenue generation through improved parking management. Figure 2 illustrates IoT applications in the contemporary technological context.

Figure 2. Examples for IoT Applications of IoT

IoT has several benefits, but security and privacy are the most pressing challenges in its growth.[4] IoT devices must be linked to the Internet for fulfilling their functions. Attackers on the Internet can steal users' sensitive information in any illegal means, causing significant damages for users.[5] This implies that user information must be kept safe and available only to legitimate users. Hence, this work aims to picturize attacks that can occur on IoT and provide information about needed security mechanisms. Following this introductory section, elements of IoT and its Architecture are detailed in section 2. Challenges faced by IoT Systems in implementations are detailed in section 3 followed by discussion on threats and Attacks faced by IoT in section 4. Suggestions for securing IoT systems form section 5 and emerging Trends in IoT Security Threats with Solutions are detailed in section 6. This work concludes in section 7.

Elements of IoT and Architecture

The positioning and setup of IoT devices to satisfy the individual requirements and wants of users is referred to as IoT architecture. IoT systems are split into purpose based layers where elements of IoT include identifications, sensing, communications, services and semantics which are detailed below.

- Identifications: Every object in a network has a distinct identity thanks to identification. The two phases in the identification process are naming and addressing. Naming is giving anything a name, while addressing is giving it a specific address. Because two or more items always have separate addresses even if they may have the same name, these two conceptions are very different from one another. Items in a network can be named using a variety of techniques, including ubiquitous codes and electron products codes (EPC).[6] Every object has a unique address assigned to it via IPv6. At first, IPv4 was used to allocate addresses, but with so many IoT devices, this approach was unable to meet the demand for addresses. As a result, IPv6's 128 bit number addressing technique is employed.
- Sensing: Sensing obtains information from surrounding objects which are transferred to the storage media. Several sensing devices, such as wearable sensors, RFID tags, actuators, and smart sensors collect required data.
- Communications: One of the main objectives of IoT is communications by linking and allowing communications between devices where files or messages are shared in communications. RFID [7], Bluetooth [8], Wi-Fi [9], Near Field Communications (NFC) [10], and Long Term Evolutions (LTE) [11] offer technological communication capabilities.
- Computations: Sensors are used to gather data from the objects, which is then used for computations. It is employed to eliminate pointless and superfluous data. IoT processes use hardware and software platforms. Intel Galileo, Arduino, and Raspberry Pi are examples of hardware platforms; operating systems are a major component of software systems for processing. Numerous operating

https://doi.org/10.56294/sctconf2024.1117

systems are in use, including Android, Lite OS [12], Tiny OS [13], and others.

- Services: Four distinct services are offered by IoT applications.[14] The first service is connected to identification. It is employed in the request to ascertain the transmitting objects' identities. Subsequently, data from multiple sources are aggregated and processed. Cooperative services are third and respond to devices suitably by making decisions based on the information acquired. The last service, known as ubiquitous service, reacts quickly to devices, regardless of the time or location.
- Semantics: IoT has an obligation to assist people in completing their jobs where semantics are crucial elements for IoT's intelligence. Once all the data has been gathered, it decides how to react to the devices in the most effective way.

The first architecture of IoT consisted of three levels, but as it developed, it was unable to meet all of the needs. Afterwards, a support layer for security was added to a four-layer design.[15] The growth of IoT was significantly aided by the four-layer design. Concerning security and storage in the four-layer design, there were also certain problems. Five-layer architecture was suggested by researchers to protect IoT.[16] Similar to earlier systems, it encompasses perception, transport, and application layers. There are two additional levels to it. The names "processing layer" and "business layer" relate to these recently proposed layers. The recently proposed design is expected to be capable of addressing IoT requirements. It also offers the ability to safeguard IoT apps. The following is an explanation of how these levels work.

- Perception layer: often referred to as a sensor layer. It functions similarly to the nose, ears, and eyes of a human. It is in charge of recognizing objects and gathering data from them. To gather data, a variety of sensors—such as 2-D barcodes and RFID—are affixed to items. The needs of the intended applications are taken into consideration while selecting sensors. These sensors could gather information on motion, vibration, location, air quality, and other pertinent subjects.[17]
- Transport Layer/Network Layer: sends data to the processing procedures of the next layer.[17] Analog input must first be converted into digital representation via IoT gateways. Subsequently, gateways use data transfer protocols (DTPs) to move data.
- Network Layer: sometimes referred to as layers of transmission which link perceptions with applicational layers. They transport and send data collected by sensors. Transmission medium come in two flavors: wireless and wired. It also links network devices, smart objects, and networks.[18]
- Application Layer: Every application that makes use of or has made use of IoT technology is defined at the application layer which include smart homes/cities, healthcare, and animal monitors. Services might vary depending on the application as they are dependent on sensor data. Among the several application layer concerns, security is the most important. IoT poses a variety of hazards and weaknesses, both internal and external, when utilized to construct a smart home.[19]
- Support Layer: The fourth layer was created with security in mind for IoT design. Data is directed straight to network layers increase chances of threats. Tri-layered architectural limitations lead to the proposal of an additional layer. A support layer in a four-layer structure receives information from the perception layer. Two tasks are under the purview of the support layer. It ensures that data is safe from unauthorized access and transferred by authorized users. Verifying users and information may be done in a few different ways. Authentication is the most often used technique. Passwords, keys, and pre-shared secrets are used in its implementation. Information transmissions to network layers are also supporting layers' duties where data transmissions occur through cables and wireless methods.[20]
- Business Layer: The intended behavior of an application is referenced by the business layer, which functions as a system manager. Its responsibilities include managing and supervising the IoT's profit, application, and commercial models. This layer also protects the privacy of the user. It also has the capacity to control the generation, archiving, and modification of data. Attackers can exploit an application without interfering with business logic due to this layer's vulnerability. Application defects resulting from insufficient or nonexistent security mechanisms account for most security concerns. The following are typical problems with business layer security.[21]

Global consensus on IoT architecture is wanting. Scholars have put up a wide variety of architectures. While some experts advocate for a four-layers in design as they believed that applicatios' needs cannot be satisfied by three layered architectures. IoT five layers were suggested owing to issues with privacy and security. Figure 3 displays layered architectures of IoT.

Numerous communication technologies are employed in IoT applications, including 2G, 3G, 4G, ZigBee, Bluetooth, RFID, and WSNs (described above). several connected devices, security threads, new standards, device computational capabilities, and complex communication provide several obstacles for these communication systems.[22] Next generation networks, or 5G networks are rapidly becoming available through IoT to satisfy the expectations of the smart environment and industry and solve these difficulties.[23] The factors that need to be addressed in IoT are discussed in the next section.

https://doi.org/10.56294/sctconf2024.1117

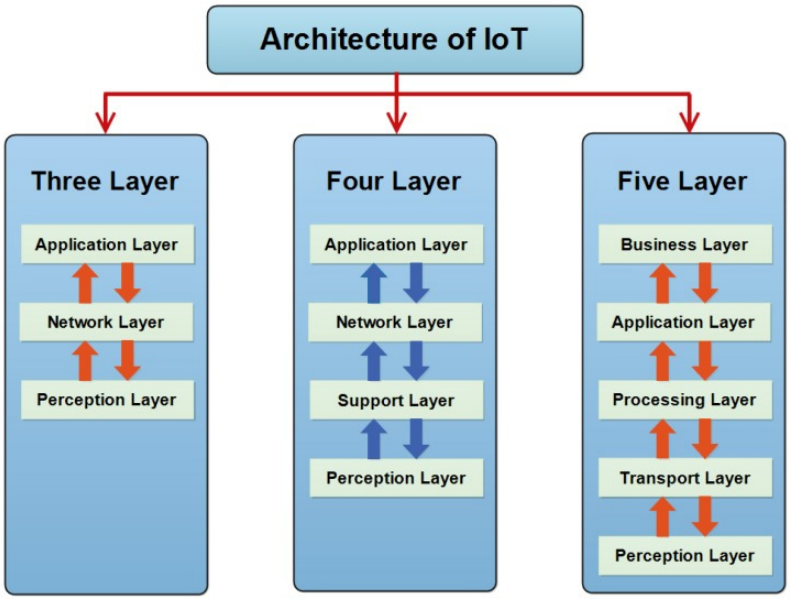

Figure 3. IoT's layered architectures

Challenges in implementing IoT Systems

Notwithstanding the widespread use of IoT applications, There are still many barriers and restrictions WSNs are important IoT supporting technology, even when the architecture of IoT limits their use. For more than 20 years, IoT has been transforming several sectors by enabling people and businesses to remotely monitor, analyze, and control objects. Globally, IoT applications are growing phenomenally resulting in enhanced opportunities for manufacturers, developers, and users, but face different challenges.

- Addressing Schemes: An essential component of IoT application operation and success is the ability to uniquely identify things. Applications for IoT must be able to remotely monitor and operate thousands of devices while also classifying each one uniquely. The four most important characteristics of a unique address are persistence, scalability, uniqueness, and dependability. For these smart devices to be able to connect with one another and join the internet, they need a proper and distinct address. With just 4,3 billion addresses available, Internet Protocol Version 4 (IPv4), which uses 32-bit addresses, is almost out of space. IPv6, the subsequent version, uses 128-bit addresses and has a massive address abundance of 3:4 1038, or 340 trillion trillion trillion.[24]
- Big Data: IoT is a remarkable technology that utilizes vast amounts of data gathered and aggregated through smart things. Techniques to turn this data into knowledge that can be used will need to be developed. Data is predicted to double in size every two years and reach 44 Zettabytes soon.[25] Figure 4 depicts significant hurdles in IoT i.e. "5V" (Value, Velocity, Volume, Variety, and Veracity).

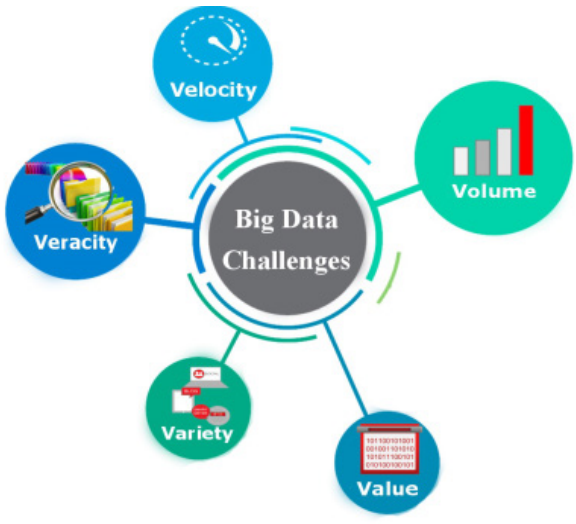

Figure 4. The "5V " Challenges

https://doi.org/10.56294/sctconf2024.1117

- Velocity: relates to rates at which information are accumalated, transmitted and processed.
- Variety: refers to endpoint data colleted by smartphones, machines, sensors, etc. These unstructured data, vary in their formats including plain texts, CSVs, XMLs, audios, and videos.
- Veracity: implies ensuring the accuracy of the data collected and preserved.
- Volume: is the volume of all data kinds that are gathered, saved, retrieved, and updated from various sources. The volume of data generated by IoT is growing dramatically.
- Value: The next stage is to extract value from the vast amounts of precisely collected data. Consequently, developing novel methods that enable informed decision-making within the required time frame—such as feature extraction and trend analysis using AI—becomes more challenging.

Currently, multiple management solutions are available for analyzing and managing big data. The study in [26] focussed on IoT device data from smart buildings. The framework offers new methods for storing and analyzing fast data produced by sensors. The technology enhanced user experience by demonstrating voluminous data without human intervention. IoT based smart meters for gas and water were presented in [27]. The utility and consumers receive information from the intelligent model for a substantial volume of data.

- Energy Consumption: IoT generates billions of internet-connected objects and networks. Energy is as a vital resource in IoT. This means that using energy-intensive protocols like HTTP, TCP, and others to transmit unnecessary data and protocol overheads is not a wise use of resources. Therefore, creating intelligent routing mechanisms and energy-efficient network architectures in IoT networks remains a significant problem.
- Devices/Links Heterogeneity: The diversity of devices and links is a key component of IoT concept, since it will operate on various sets of protocol suites, data formats, etc. The majority of sensors in WSNs are homogenous, meaning they share the same power, communication, and computational capabilities for delivering various services, IoT uses a wide range of networks, connections, and device connectivity. Because of this, the diverse character of links and objects is essential to the connectivity of IoT devices, posing a special difficulty that must be overcome. Therefore, one may wonder if it is feasible to have a single architectural model that can be used to support such a large variety of gadgets and applications.
- Transmission Media (TM): The physical route known as TM is what creates the connection and moves the data from the source to the recipient. IoT networks employ a variety of technologies, including RFID, Bluetooth, Zigbee, LoraWAN, Sigfox, and others, to send and receive data. IoT is not exempt from the standard issues with transmission medium, such as high error rate, bandwidth, fading, inference, etc. Specialized energy, network gear, and bandwidth that is compatible with each communication channel are needed. Hence, in IoT applications, improving the TM is a problem to maintain and extend the lifetime of networks.
- Quality of Service (QoS): In numerous applications, data need to be transmitted within specific time frames to destinations where services, packet losses, delay managements, and bandwidths contribute towards QoS in networks. Thus, for the purposes of implementation, optimization, and administration, quality of service requires study and stability.
- Massive Scaling: There may be tens of billions or perhaps more sensor nodes in use around the planet. One significant difficulty that affects routing methods is massive scale. Scalability is the growing number of networks and devices with the introduction of IoT. For these enormous numbers of sensor nodes, any routing method must be appropriate and sufficiently scalable.[28]

Cyber risks have always been a possibility for IoT devices. Numerous instances exist where IoT devices are hijacked or merged into botnets (like the notorious Mirai botnet) to get access to or exploit other parts of a network. Subsequent sections address threats and attacks against IoT systems, followed by possible defense strategies.

Threats and Attacks on IoT

Several research works have examined and classified risks and attacks on IoT. Surveys on a range of ubiquitous technologies have been provided for analyzing attacks and risks.[29] The majority of embedded systems are computationally incapable of efficiently implementing complex security rules and encryption methods [30]. The following list of IoT vulnerabilities [31] is provided:

- Inadequate Physical Security: The majority of IoT devices function autonomously in unmonitored settings. These devices are easy physically accessible to adversaries, who can then seize control. Due to this, attackers may compromise control or cyber data, reveal cryptographic algorithms, damage physical devices, or make duplicate firmware;
- Insufficient Energy Harvesting: Energy limitations of IoT devices are contraints where overloading devices with legitimate or tampered signals, an attacker can deplete stored energy and prevent legitimate use;
- Insufficient Authentications: It is challenging to implement sophisticated authentication techniques

due to the energy and computing limitations of IoT paradigm. Attackers may utilize weak authentications to establish malicious fake nodes, jeopardize data integrity, and obtain access to IoT devices and network connections. Authentication keys that have been transferred or used are always susceptible to corruption, loss, or destruction. Insecure key storage and transfer reduces the effectiveness of sophisticated authentication schemes;

- Inadequate Encryptions: In IoT domains, data protection is crucial, particularly for key cyber-physical systems (CPS) including building automation, industrial facilities, and electrical utilities. Encryption ensures that data is transferred and kept securely and that only authorized people may access and use it. Algorithms are the foundation of cryptographic systems, but constraints on IoT resources impact their effectiveness, durability, and efficiency. A potential attacker could be able to circumvent encryption with little difficulty in order to obtain private data or alter actions;
- Unnecessary Open Ports: A lot of IoT devices have open ports that aren't necessary for them to function, which exposes susceptible services. This makes it possible for bad actors to connect and take advantage of several weaknesses.
- Inadequate Access Controls: Proper credential management is necessary for secure IoT devices and data. Complicated passwords are often absent from IoT devices and their cloud management systems. After installation, a lot of devices don't ask users to modify the default password. Most clients have extensive authorization. As a result, the device's integrity and data security may be jeopardized by an attacker gaining unauthorized access;
- Inadequate Patch Managements: It's critical to routinely patch embedded firmware and software, as well as IoT operating systems. This technique increases functionality while lowering vulnerabilities. According to several reports, manufacturers frequently neglect to install automatic patch updates or deploy security changes. Because there are no integrity guarantees in place, existing update systems are open to both malicious alterations and widespread use;
- Weak Programming Practices: Stdies have analyzed vulnerabilities of firmware upgrades in spite of strict development standards and security measures where usages of root users as primary access points, and absences of SSLs are few of these risks. Therefore, by exploiting well-known security flaws, an attacker can carry out buffer overflows, modify data, or obtain device access.

Inadequate Audit Mechanisms: Many IoT devices lack thorough logging protocols, which allows harmful activities to remain hidden from IoT sources;

Attacks are the process of locating and categorizing security flaws in the context of IoT according to how they can be exploited. The category is divided into three main subcategories, each of which offers thorough justifications and examinations of attacks aimed at data integrity, availability, and secrecy and authentication. Usually, attackers damage the equipment, implant malware on it, or get access to the data of other businesses. Considering that insufficient security measures are built into IoT devices. They therefore represent one of the weakest points in an organization and present a serious security risk.[32] Basic IoT devices frequently lack the integrated security solution needed to fend against cyberattacks. Since the majority of IoT devices are meant to carry out basic tasks, their uses and applications are restricted. Because of this, people regularly disregard their security posture, leaving them vulnerable to cyberattacks. Hackers or groups may use zero-day exploits and common vulnerabilities to get access to IoT devices and use them in a variety of ways to conduct extensive cyberattacks.[33] Some of the various ways that IoT systems are targeted differ from traditional IT (Information Technology) threats in that they include:

- Resources: The processing speeds and resources of IoT devices are often low. They might therefore be more open to attacks than IT because they lack security mechanisms that guard against them;
- Device Diversities: The form factor, operating system, and network connection of different types of IoT devices vary greatly. Therefore, standardized security protocols are more complex, increasing the vulnerability of particular devices to assaults;
- Physical Impact: Cyberattack on IoT might are dangerous as IoT devices in infrastructures or life-sustaining systemss like healthcare equipments, On the other hand, the majority of IT assaults seek to compromise services or pilfer data; Legacy Devices: IoT devices typically last longer. As a result, a lot of outdated electronics will be linked and in use. Older devices are more susceptible to hacks and attacks because they are unable to receive security patches or software updates.
- Weak/Default Passwords: Attackers can compromise and breach sensitive or confidential data exchanges between devices and servers by taking advantage of vulnerabilities in IoT device communication protocols and services, which are made possible by insecure network services. The inability to modify default logins and passwords, weak or default passwords, implementations of stricter password requirements, and absence of reliable password recovery mechanism are some additional vulnerabilities. For instance, man-in-the-middle (MitM) attacks aim at systems' weaknesses in their endpoint authentications and execute complex attacks.

https://doi.org/10.56294/sctconf2024.1117

- Insecure Ecosystem Interfaces: Insecure portions of the ecosystem are those parts of the internet, backend API, cloud, or mobile interface that make it possible for the device or its linked parts to be compromised. For instance, inadequate encryption, insufficient input and output filtering, and a deficiency in authorization or authentication.
- Absence of Secure Update Mechanism: Device updates cannot be made safely. This comprises procedures for preventing rollbacks, unencrypted data transfers, unsafe delivery, firmware certification for individual devices, and notifications of security modifications brought about by updates.
- Usages of harmful or outdated components: Using software or libraries that are too outdated or risky could expose the device to security holes. This entails using hardware or software from a contaminated supply chain and inadvertently switching system platforms. Insecure or out-of-date software dependencies could pose a threat to the security of the Internet of Things ecosystem. Manufacturers who use open-source components to make their IoT devices have to negotiate a complex and challenging supply chain. These parts may inherit known weaknesses to attackers, creating a risk that might be exploited.
- Inadequate Privacy Protection: Personal information about users that is accidentally, wrongly, or illegally used and kept on devices or within ecosystems and may include medical information, energy consumption, and driving patterns. Inadequate safeguards will compromise privacy, and if the right steps are not taken, there can be legal consequences.
- Insecure Data Transfer and Storage: Wherever in the ecosystem that sensitive data is stored, transferred, or processed, there is no encryption or access control in place. Data utlizations in automated controls and decision making processes makes it crucial for reliability and integrity of IoT applications. It would be detrimental if there were any unauthorized usage or access.
- Device management: Device managements (i.e., assets, updates, secure decommissions, system monitors and responses) lack in managing security. If an unauthorized device is exposed to IoT environment, it can monitor activity, access company networks, and intercept data.
- Inadequate Privacy Protection: User personal data that is inadvertently, improperly, or unlawfully utilized and stored on the device or in the ecosystem. Insufficient security measures will jeopardize privacy, and failure to take appropriate action may result in legal ramifications.
- Insecure Data Transfer and Storage: Wherever in the ecosystem that sensitive data is stored, transferred, or processed, there is no encryption or access control in place. Given that data are:
- Insecure Default Settings: These are either preconfigured devices or systems with risky default settings, or they are unable to increase system security by limiting user setting modification. Once these settings are identified, attackers can concentrate on firmware vulnerabilities, hardcoded default passwords, and concealed backdoors within the device. It is difficult for the user to adjust various parameters simultaneously.

Of all these vulnerabilities, weak or default passwords are among the most often discovered ones in IoT devices. Users hardly ever update weak passwords that are susceptible to Brute Force attacks or change their passwords to easily access the device. Once the device is accessible, the attackers proceed with more infections for achieving their goals.[34]

Suggestions for securing IoT systems

IoT threats and attacks provide new challenges that require specific security solutions for completely protecting against these risks.[35] IoT devices typically have a little power supply, thus in order to send and receive data, they must make use of what little power they have. Because adding security protocols, authentication, or encryption could significantly increase the power consumption of simple transfers, IoT devices are unable to do so. This work suggests a few slotions for overcoming threats and attacks enforcing security in IoT systems.

- Addressing Schemes: IoT heterogeneity was addressed by a team of academics who created a lightweight addressing technique. The nodes addressing in this approach is implemented by multi encoding and virtual domain. The suggested plan demonstrates a workable and appropriate IPv6 over 6LowPAN connection between WSNs and the internet. The implementation of automated identification for IoT nodes was achieved through the use of a distributed address allocation mechanism in the identification and addressing system for IoT devices. An addressing method that combines the AODV routing protocol and the cluster-tree algorithm is also presented in this study. It implements the nodes addressing technique in IoT networks both locally and widely. In light of this, developing a consistent addressing system for IoT is a hot topic and a significant task.
- Big Data issues: Velocity: pertains to the speed at which data is acquired, sent, and analyzed. The pace at which applications process data varies. While some applications—like analytics programs—need real-time processing, other applications—like data arrival—may be able to handle it rapidly. Variety: describes the wide range of data types that endpoints—such as computers, sensors, smartphones, and other devices—gather. The data content is unstructured and is available in multiple formats, such as

audio, video, CSV, XML, and plain text. It is necessary to organize and process the variety of data in a meaningful and consistent manner.

- Energy Consumptions: Energy consumption is the most crucial aspect to take into account if IoT is to have a sustainable impact. Typically, millions of nodes for a given application cannot have their batteries changed when they run out and the nodes require a new battery. IoT must therefore function essentially as a disposable system, with nodes lasting for as long as is reasonably possible before being thrown away. A unique scheduling technique for nodes positioned between two or more sensing fields was provided by the study by [36]. For border nodes with high energy consumption and diverse sleep and listen patterns, the S-MAC protocol was created. These nodes often reach the listening state due to their heterogeneous scheduling. The goal of the effort was to lower border node energy consumption, which lengthened WSN lifespan. Sensing fields were separated into groups by the developers of [37], who then assigned message brokers to groups for gathering data from sensors and transmitting them. The suggested approach worked well in terms of energy usages and service responses. A heterogeneous dual processor with a fast coreH and an ultra-low power near threshold coreL is suggested by work published in [38].
- Devices/Links Heterogeneity: [39] provided an SDN-Docker-based architecture for network and device heterogeneity. The suggested research provided an example of the architecture and connection amongst IoT devices constructed on an SDN-based network. The DIAT scheme offers a simple, scalable distributed architecture for large-scale IoT networks. It is especially made to get past incompatibilities with devices and installations.[40]
- Transmission Media (TM): According to the study that was published in [41], the authors examined and assessed the range and coverages of LoRaWAN and Sigfox across large areas. Interferences were observed at a frequency of 868 MHz in Europe. The study found that fewer than 1 % of up-link and down-link failure rates were provided by both techniques. It is also shown that indoor coverage has increased by up to 99 %. Backscatter antennas were used by the authors of a different study [41] to develop full-duplex wireless IT for reducing energy consumptions and latencies where interference from pre-existing links were reduced. Moreover, simultaneous information flows in forward and backward directions were allowed.
- Quality of Service (QoS): The authors of reference [42] offer a general framework that makes it possible to build multi-component IoT cloud infrastructures in a way that considers quality of service. The model that was recommended demonstrated suitable operational and systemic features for fog facilities. The study in [43] introduced a hybrid push-pull traffic strategy for IoT data transport. Comparing the suggested technique to normal IPv6, it demonstrated negligible packet loss and lowered network load and performance by 50 %. The authors of [44] proposed a novel method of integrating named data networks with pub/sub systems. This method produced scalable Internet of Things cloud services. The authors of another study [45] have improved the scalability of an effective IoT cloud connection that facilitates resource provisioning and dynamic management. According to their reported results, network support for both regulated and uncontrolled devices could be ensured via the MQTT and CoAP protocols.
- 5G and 4G Technologies enabled IoT: Fourth generation (4G) technology has been widely used in IoT and has been continuously improving to satisfy the needs of future networks.[46] We are getting closer to fifth generation (5G) technology with current research. Every technology sees the introduction of new features and the resolution of bugs. All users can simultaneously stream high-quality audio and video at up to 1 Gbps bandwidth speed thanks to long-term evolution (4G) technology. In the next two years, 5G, the next generation of mobile internet networks, should be operational. Although it is a development of 4G LTE, it offers consistent connectivity for smartphones and other devices, is ten times faster, has higher data rates, is more secure, has less latency, and lasts longer on batteries.[47] It should be able to manage over 1000 times the amount of mobile data that the present cellular networks can handle. These features will probably make next-generation networks and solutions perfect for IoT applications. This outcome shows how IoT technologies will be supported by the 5G platform to meet application and market expectations. Moreover, it will be the solution for non-orthogonal waveforms, machine-to-machine (M2M) communications, big MIMO systems, non-orthogonal multiple access, etc. in IoT applications. III.
- Device Security: Devices with firmware and hardware protections at the perception layer are the first to be affected. Protecting actual IoT endpoints against malware and hijacks is part of it. Use cryptographic keys for accurate authentication, protect your devices with hardened exteriors, prevent unauthorized code from running on linked devices, and address firmware update and security patch issues to keep your devices safe.[48]
- Connection Security: Encryption is commonly used to safeguard data transfers over networks. The transport layer security (TLS) protocol is the basis for IoT connection security. End-to-end encryption prevents unauthorized users from obtaining and exploiting data.[48]

https://doi.org/10.56294/sctconf2024.1117

- Cloud Security: Since encryption lessens the likelihood that private information would be made public due to data breaches, it is a crucial part of cloud security. Strict permission constraints and authentication procedures need to be implemented to limit access to IoT apps. Devices must first get authorization to stop rogue devices from connecting to the cloud or an IoT system. Moreover, it is almost a given that additional flaws in device firmware will be found as new technologies and methods of exploiting them develop over time. In the absence of new information, these vulnerabilities might develop over the course of the device's life. Manufacturers are usually unable to offer direct device access or on-site updates due to the large dispersion of IoT devices. During remote firmware changes, the device may use a lot of power if there is not enough data throughput. A formula for catastrophe arises when you consider that IoT devices may depend on the network infrastructure (such as WiFi) of end users. The gadget is more susceptible to cyberattacks as it may be used to access other networked devices and applications.
- Low-power Connectivity: Llw-power communication technologies incorporate new security techniques SIM cards are utilized by cellular networks for device authentication, and security mechanisms like IMEI locks guarantee that a certain SIM card may only be utilized by the assigned device. Additionally, when needed, low-power remote firmware upgrades are supported using cellular networks. Finally, businesses like Emnify can assist in bridging security gaps with their virtual private network (VPN) capabilities and enhanced control over the communications of your devices.
- Creation of Secure IoT devices: To guarantee the security of IoT devices, we integrate many security layers at every stage of the product development process. Secure by design is the approach we have been employing to protect things from the ground up. Integrated security design and VAPT testing incorporation into product development lifecycles assists clients in deploying safe items in public spaces that aid in shielding goods from risks associated with IoT security.
- Data security solutions: By encrypting and securely safeguarding data to prevent unauthorized access, these solutions can aid in data protection.
- Data Loss Prevention (DLP): By detecting and preventing unauthorized access, copying, and transmission, DLP systems can aid in the prevention of data loss.
- Data governance solutions: By guaranteeing that data is only accessible by authorized individuals, kept in a safe location, and shielded from unauthorized alterations, these solutions can assist enterprises in managing their data securely.

Emerging Trends in IoT Security Threats with Solutions

Amazing breakthroughs have been made possible by IoT, which has connected systems and objects in previously unthinkable ways. But this interconnectedness also presents fresh, dynamic security risks. It's critical to comprehend the most recent developments in IoT security dangers if you want to remain ahead of the competition.

- Ransomware Attacks on IoT Devices: A growing number of ransomware attacks target IoT devices by encrypting their firmware and requesting a fee to unlock the keys. Critical IoT systems, such medical equipment or industrial controls, could be affected by a successful attack.
    - Mitigation: To reduce the harm caused by ransomware attacks, upgrade firmware frequently, use strong authentication, and set up backup systems.
- Edge-Based Attacks: As IoT devices becoming more potent, hackers are concentrating on taking advantage of weaknesses at the network edge. Edge devices, such as sensors and gateways, could serve as ports of entry for hackers.
    - Mitigation: Use security tools such as intrusion detection.
- AI-Enhanced Attacks: Cybercriminals are leveraging ML and artificial intelligence to identify weaknesses and create more advanced attack plans. AI-driven attacks are more difficult to identify and stop because of their quick evolution and adaptation.
    - Mitigation: To proactively detect and address changing threats, integrate AI and ML into your security strategy.
- Supply Chain Attacks: IoT devices are compromised by focusing on the supply chain. Users could be seriously at danger from viruses or backdoors on compromised devices.
    - Mitigation strategies include putting in place device integrity checks, carefully screening vendors, and building a strong supply chain security architecture.
- 5G Vulnerabilities: As 5G networks are implemented, more devices will be able to connect quickly and with low latency, creating new attack surfaces. Faster connectivity could result in more serious data breaches and quicker IoT vulnerability exploitation.
    - Mitigation: Put in place security features unique to 5G networks, like secure authentication and network slicing.

https://doi.org/10.56294/sctconf2024.1117

- IoT device Vulnerabilities in the Ecosystem: IoT devices frequently depend on a complicated web of interconnected parts and outside services, which might lead to weak points. weaknesses in every area of the ecology.
    - Mitigation: Make sure third-party services follow security best practices, update all components on a regular basis, and conduct security assessments.
- Quantum Computing Threats: Data from IoT devices may be exposed if quantum computing manages to crack existing encryption systems. If encryption is cracked by quantum computers, then sensitive data might be compromised.
    - Mitigation: Research encryption techniques that are resistant to quantum occurrences and be ready to switch to them when needed.

CONCLUSION

IoT technology has advanced significantly for a variety of applications that make use of several enabling and emergent technologies. IoT merely uses the most recent advancements in processing power and communication infrastructure to integrate and link a huge number of gadgets. Increasing IoT applications aims to connect many smart gadgets, technologies, and apps to improve people's quality of life. This technology is quickly finding its way into everyday life. In general, IoT enables the automation of anything in the surrounding area. IoT systems have a variety of security challenges, for which many designs have been proposed. The concern over security is growing as the number of IoT devices rises. A large number of these devices are vulnerable by default and lack fundamental security features like authentication and encryption. Attackers might therefore be able to jeopardize the security of the devices and information gathered. To increase the security of Internet of Things devices, many actions can be implemented. These include using security features like as encryption and authentication, ensuring that devices are properly updated and set, and keeping a look out for suspicious activity on devices. Majority of IoT risks are common with low-risks while certain high-impact attacks have the potential to do significant harm. One significant concern is that hackers could be able to access private information kept on Internet of Things devices. Personal data like names, passwords, and addresses; financial data like credit card and bank account numbers; and even highly classified military data like troop movements and tactical plans could fall under this category. Keeping Up with IoT Security Scene The environment of IoT security is always changing, so it's critical to keep up with new threats. To protect the integrity and safety of their IoT ecosystems, both individuals and organizations need to be on the lookout for new threats, implement cutting-edge security measures, and adjust to the constantly shifting environment. We need to keep improving our defenses against new security risks as IoT technology does. The features and restrictions of the communication technologies have been shown. This paper provided an overview of the theory underlying this idea and its applications. The layered structures of the Internet of Things have been the subject of numerous studies, and we have also covered security attacks that exploit these architectures to compromise the functionality of the technology. The literature on IoT security has been reviewed, and recommendations have been made. In addition, a number of open security issues related to IoT technologies have also been covered. The problems and difficulties must be resolved, and security measures must be put in place right away.

REFERENCES

1. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials. 17(4), PP. 2347-76. https://doi.org/10.1109/COMST.2015.2444095

2. Li S, Xu LD, Zhao S. The internet of things: a survey. Information systems frontiers. 17, PP. 243-59. https://doi.org/10.1007/s10796-014-9492-7

3. Farhan L, Kharel R, Kaiwartya O, Hammoudeh M, Adebisi B. Towards green computing for Internet of things: Energy oriented path and message scheduling approach. Sustainable Cities and Society. 38, PP. 195-204. https://doi.org/10.1016/j.scs.2017.12.018

4. Yaqoob I, Ahmed E, Hashem IA, Ahmed AI, Gani A, Imran M, Guizani M. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications. 24(3), PP. 10-6. https://doi.org/10.1109/MWC.2017.1600421

5. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless networks. 20, PP. 2481-501. https://doi.org/10.1007/s11276-014-0761-7

6. Koshizuka N, Sakamura K. Ubiquitous ID: standards for ubiquitous computing and the internet of things.

IEEE Pervasive Computing. 9(4), PP. 98-101. https://doi.org/10.1109/MPRV.2010.87

7. Want R. An introduction to RFID technology. IEEE pervasive computing. 5(1), PP. 25-33. https://doi.org/10.1109/MPRV.2006.2

8. McDermott-Wells P. Bluetooth scatternet models. IEEE potentials. 23(5), PP. 36-9. https://doi.org/10.1109/MP.2005.1368914

9. Ferro E, Potorti F. Bluetooth and Wi-Fi wireless protocols: a survey and a comparison. IEEE Wireless Communications. 12(1), PP. 12-26. https://doi.org/10.1109/MWC.2005.1404569

10. Want R. Near field communication. IEEE Pervasive Computing. 10(3), PP. 4-7. https://doi.org/10.1109/MPRV.2011.55

11. Crosby GV, Vafa F. Wireless sensor networks and LTE-A network convergence. In38th Annual IEEE conference on local computer networks, pp. 731-734. https://doi.org/10.1109/LCN.2013.6761322

12. Cao Q, Abdelzaher T, Stankovic J, He T. The liteos operating system: Towards unix-like abstractions for wireless sensor networks. In2008 International Conference on Information Processing in Sensor Networks (ipsn 2008), pp. 233-244. https://doi.org/10.1109/IPSN.2008.54

13. Levis P, Madden S, Polastre J, Szewczyk R, Whitehouse K, Woo A, Gay D, Hill J, Welsh M, Brewer E, Culler D. TinyOS: An operating system for sensor networks. Ambient intelligence. PP. 115-48. https://doi.org/10.1007/3-540-27139-2_7

14. Gigli M, Koo S. Internet of Things, services and applications categorization. Advances in Internet of Things, 1, PP. 27-31.

15. Darwish D. Improved layered architecture for Internet of Things. Int. J. Comput. Acad. Res. (IJCAR). 4(4), PP. 214-23.

16. Sethi P, Sarangi SR. Internet of things: architectures, protocols, and applications. Journal of electrical and computer engineering. 2017(1), PP. 9324035. https://doi.org/10.1155/2017/9324035

17. Sengupta J, Ruj S, Bit SD. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of network and computer applications. 149, PP. 102481. https://doi.org/10.1016/j.jnca.2019.102481

18. Prabhakar S. Network security in digitalization: attacks and defence. Int. J. Res. Comput. Appl. Robot. 5(5), PP. 46-52.

19. R. Agar, IoT architecture guide: Major and additional layers of IoT system, November 2022, https://www.helpwire.app/blog/iot-architecture/.

20. Sanzgiri A, Dasgupta D. Classification of insider threat detection techniques. InProceedings of the 11th annual cyber and information security research conference, pp. 1-4. https://doi.org/10.1145/2897795.2897799

21. K. Gülen, IoT protocols 101: The essential guide to choosing the right option, January 2023, https://dataconomy.com/2023/01/03/iot-protocols-comparison/.

22. Akpakwu GA, Silva BJ, Hancke GP, Abu-Mahfouz AM. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE access. 6, PP. 3619-47. https://doi.org/10.1109/ACCESS.2017.2779844

23. Sun L, Du Q. A review of physical layer security techniques for Internet of Things: Challenges and solutions. Entropy. 20(10), PP. 730. https://doi.org/10.3390/e20100730

24. Palattella MR, Accettura N, Vilajosana X, Watteyne T, Grieco LA, Boggia G, Dohler M. Standardized protocol stack for the internet of (important) things. IEEE communications surveys & tutorials. 15(3), PP. 1389-

406. https://doi.org/10.1109/SURV.2012.111412.00158

25. Farhan L, Shukur ST, Alissa AE, Alrweg M, Raza U, Kharel R. A survey on the challenges and opportunities of the Internet of Things (IoT). In2017 Eleventh International Conference on Sensing Technology (ICST), pp. 1-5. https://doi.org/10.1109/ICSensT.2017.8304465

26. Bashir MR, Gill AQ. Towards an IoT big data analytics framework: smart buildings systems. In2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1325-1332. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0188

27. Lloret J, Tomas J, Canovas A, Parra L. An integrated IoT architecture for smart metering. IEEE Communications Magazine. 54(12), PP. 50-7. https://doi.org/10.1109/MCOM.2016.1600647CM

28. Farhan L, Alissa AE, Shukur ST, Hammoudeh M, Kharel R. An energy efficient long hop (LH) first scheduling algorithm for scalable Internet of Things (IoT) networks. In2017 Eleventh International Conference on Sensing Technology (ICST), pp. 1-6. https://doi.org/10.1109/ICSensT.2017.8304511

29. Krishna RR, Priyadarshini A, Jha AV, Appasani B, Srinivasulu A, Bizon N. State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. Sustainability. 13(16), PP. 9463. https://doi.org/10.3390/su13169463

30. Ma W, Ma L, Li K, Guo J. Few-shot IoT attack detection based on SSDSAE and adaptive loss weighted meta residual network. Information Fusion. 98, PP. 101853. https://doi.org/10.1016/j.inffus.2023.101853

31. Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials. 21(3), PP. 2702-33. https://doi.org/10.1109/COMST.2019.2910750

32. A. Amir, What are IoT attacks?, 2023, https://www.educative.io/answers/what-are-iot-attacks

33. Common IoT attacks that compromise security, May 2022, https://socradar.io/common-iot-attacks-that-compromise-security/.

34. Victor P, Lashkari AH, Lu R, Sasi T, Xiong P, Iqbal S. IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. Peer-to-peer Networking and Applications. 16(3), PP. 1380-431. https://doi.org/10.1007/s12083-023-01478-w

35. IoT. Attacks, 6 security risks to be aware of, July 2023, https://www.byos.io/blog/iot-attacks.

36. Saha D, Yousuf MR, Matin MA. Energy efficient scheduling algorithm for S-MAC protocol in wireless sensor network. International Journal of Wireless & Mobile Networks. 3(6), PP. 129. https://doi.org/10.5121/ijwmn.2011.3610

37. Abdullah S, Yang K. An energy efficient message scheduling algorithm considering node failure in IoT environment. Wireless personal communications. 79, PP. 1815-35. https://doi.org/10.1007/s11277-014-1960-3

38. Wang Z, Liu Y, Sun Y, Li Y, Zhang D, Yang H. An energy-efficient heterogeneous dual-core processor for Internet of Things. In2015 IEEE international symposium on circuits and systems (ISCAS), pp. 2301-2304. https://doi.org/10.1109/ISCAS.2015.7169143

39. I. Bedhief, M. Kassar, and T. Aguili, “SDN-based architecture challeng-ing IoT heterogeneity,” in Proc. IEEE 3rd Smart Cloud Networks Systems (SCNS).

40. Sarkar C, SN AU, Prasad RV, Rahim A, Neisse R, Baldini G. DIAT: A scalable distributed architecture for IoT. IEEE Internet of Things journal. 2(3), PP. 230-9. https://doi.org/10.1109/JIOT.2014.2387155

41. Vejlgaard B, Lauridsen M, Nguyen H, Kovács IZ, Mogensen P, Sorensen M. Interference impact on coverage and capacity for low power wide area IoT networks. In2017 IEEE Wireless Communications and Networking

Conference (WCNC), pp. 1-6. https://doi.org/10.1109/WCNC.2017.7925510

42. Liu W, Huang K, Zhou X, Durrani S. Full-duplex backscatter interference networks based on time-hopping spread spectrum. IEEE Transactions on Wireless Communications. 16(7), PP. 4361-77. https://doi.org/10.1109/TWC.2017.2697864

43. Brogi A, Forti S. QoS-aware deployment of IoT applications through the fog. IEEE internet of Things Journal. 4(5), PP. 1185-92. https://doi.org/10.1109/JIOT.2017.2701408

44. Han S, Woo H. NDN-based Pub/Sub system for scalable IoT cloud. In2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 488-491. https://doi.org/10.1109/CloudCom.2016.0085

45. Bellavista P, Zanni A. Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP. In2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI) pp. 1-6. https://doi.org/10.1109/RTSI.2016.7740614

46. Li S, Da Xu L, Zhao S. 5G Internet of Things: A survey. Journal of Industrial Information Integration. 10, PP. 1-9. https://doi.org/10.1016/j.jii.2018.01.005

47. Yassein MB, Aljawarneh S, Al-Sadi A. Challenges and features of IoT communications in 5G networks. In2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1-5. https://doi.org/10.1109/ICECTA.2017.8251989

48. R. Agar, IoT architecture guide: Major and additional layers of IoT system, November 2022, https://www.helpwire.app/blog/iot-architecture/.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: R. Parameswari.
Data curation: R. Parameswari.
Formal analysis: R. Parameswari.
Research: D. Raj Balaji.
Methodology: D. Raj Balaji.
Drafting - original draft: R. Parameswari.
Writing - proofreading and editing: D. Raj Balaji.