IJEMD-CSAI, 2 (1) (2023), 1 – 29 https://doi.org/10.54938/ijemdcsai.2023.02.1.252

International Journal of Emerging Multidisciplinaries:
Computer Science and Artificial Intelligence

Research Paper
Journal Homepage: www.ojs.ijemd.com
ISSN (print): 2791-0164 ISSN (online): 2957-5036

Innovations in Security: A Study of Cloud Computing and IoT

Hamza Azam[1*], Mohammad Ahnaf Tajwar[1], Sathesan Mayhialagan[1], Allister Jet Davis[1], Chan Jia Yik[1], Danish Ali[1] and Siva Raja Sindiramutty[1]

[1] School of Computer Science, Taylor's University, Subang Jaya, Selangor, Malaysia

**Corresponding author*

Abstract

This paper delves into the pivotal role of security in cloud computing and IoT technologies, scrutinizing their components, processes, and threats while showcasing real-world examples. It begins by defining cloud computing and the Internet of Things (IoT) to establish a foundational understanding. Subsequently, it explores their extensive applications across various domains, emphasizing their relevance and widespread integration. The primary focus centers on dissecting the security issues within both cloud computing and IoT realms. For IoT, the paper examines security components, processes, and threats, citing tangible technology instances to underscore their significance. Similarly, within cloud computing, it delves into security components, processes, and threats, spotlighting practical security applications. The impact assessment section evaluates the benefits of cloud computing and IoT security, candidly addressing associated limitations and challenges. These insights offer a glimpse into potential advancements, acknowledging the need for future developments. This comprehensive study underscores the criticality of security in cloud computing and IoT, serving as an invaluable resource for practitioners and researchers alike. Understanding the security implications of these evolving technologies is pivotal in harnessing their full potential for the future.

Keywords: Cloud Computing; Internet of Things (IoT); Security Issues; Technology Innovations.

Email addresses: **hamza@sd.taylors.edu.my (H. Azam), mohammedahnaf.tajwar@sd.taylors.edu.my (M.A. Tajwar), satheesanmathialagan@sd.taylors.edu.my (S. Mayhialagan), allisterjet.davis@sd.taylors.edu.my (A.J. Davis), chanjiayik@sd.taylors.edu.my (C.J. Yik), danishlynx@gmail.com (D. Ali), siva.sindiramutty@taylors.edu.my (S. R. Sindiramutty)**

1. Introduction

1.1 Definition of cloud computing

Cloud computing represents a novel approach to Information Technology services, empowering providers to deliver a wide array of innovative solutions via the Internet. These novel solutions encompass tools, platforms, computational resources, application-specific solutions, and virtualized hardware (Alouffi et al., 2021). These services are characterized by their scalability and on-demand availability, with the subscription model being based on user consumption metrics or a subscription model. Presently, the cloud computing environment is predominantly characterized by three prominent service types: Software as a Service (SaaS): In this setup, specific software tools are directly accessible to users via internet browsers. These tools are hosted on cloud servers rather than being installed locally, enabling efficient updates and access from anywhere in the world (Rahman & Subriadi, 2022; Shafiq et al., 2022). Platform as a Service (PaaS): PaaS provides developers with a unique platform that offers optimal settings for building, testing, and launching applications (Malviya & Dwivedi, 2022; S. H. Gill et al., 2022). Service providers furnish all the necessary utilities and libraries. Infrastructure as a Service (IaaS): IaaS delivers essential IT resources through the cloud, encompassing storage, processing capabilities, and networking components (Aletabi & Abdallah, 2023; Alruwaili et al., 2021). The responsibility for maintaining, overseeing, and optimizing these components lies with the provider. Despite the manifold advantages, security concerns loom large in the domain of cloud computing (Alouffi et al., 2021; Shafiq et al., 2021). Therefore, cloud computing security is paramount for consumers, businesses, and Cloud Service Providers (CSPs) as it safeguards against potential security threats. In this paper, various aspects of cloud computing, such as Cloud Computing Security Components, Cloud Computing Security Processes, and Cloud Computing Security Threats, are critically reviewed and analyzed.

1.2 Definition of the internet of things

The Internet of Things (IoT) stands as a groundbreaking frontier in the realm of technology. The extensive network of IoT encompasses a plethora of systems, including self-driving vehicles, microgrids, and smart drones, all made possible by the exponential advancements in communication technology, device accessibility, and computational systems. For instance, microgrids that consolidate distributed energy sources, self-driving vehicles for automated transportation, and smart drones are being utilized for surveillance purposes (Mohamad Noor & Hassan, 2019; Muzammal et al., 2021, Muthukkumar, R, et al., 2022). However, security remains a paramount concern in the realm of the IoT paradigm. As these devices and networks are interconnected in regular operations, it is essential to ensure that these devices are resilient against potential threats that may arise at any time. To address these security challenges, academic circles have been actively working to develop enhanced privacy and security measures specifically designed for the IoT (Ogonji et al., 2020; Muzammal et al., 2021a). In this paper, various aspects of IoT, such as security components, security processes, and security threats, are discussed in the relevant section.

2. Applications in Real World

2.1 Cloud computing

Cloud computing is a significant player in the realm of online computing. By harnessing the power of the cloud, organizations can access vast amounts of computing power and storage solutions without the need for on-premises infrastructure (Rashid & Chaturvedi, 2019). Consequently, cloud computing plays a crucial role in various sectors:

E-Learning: In the field of education, cloud computing provides an excellent environment for learners, educators, and researchers (Gill et al., 2023). An institution's cloud infrastructure can facilitate students and educators in accessing essential data and resources, enhancing the learning experience. Examples include virtual classrooms, simulation tools, and virtual labs.

Digital Governance: Governments can significantly improve their operational efficiency by implementing cloud-based solutions (Rashid & Chaturvedi, 2019). This approach streamlines the delivery of public services across government agencies and simplifies complex tasks such as application management, installation, and updates. Examples of e-governance using the cloud include complaint resolution systems, e-police, and e-court systems.

Business Process Management: As businesses expand, the integration of cloud computing into process management, including resource planning, becomes increasingly vital (M. Sharma et al., 2023). Managing tasks such as application management, HR, and payroll can become challenging and costly. Transitioning these complex processes to the cloud can reduce these challenges and enhance efficiency. Business cloud solutions encompass supply chain and vendor management, HR management, and customer relationship management.

2.2 Internet of Things

The potential applications of IoT are extensive and diverse, permeating nearly every facet of daily life for individuals, organizations, and the broader community. The IoT domain spans a wide range of sectors, including industrial applications, urban development in smart cities, agriculture, and healthcare (Hussein, 2019; Humayun, Jhanjhi, Alsayat, et al., 2021). Here are some notable applications of IoT:

Smart Cities: IoT significantly enhances urban infrastructure, paving the way for more efficient cities (Khattak et al., 2023; Zahra et al., 2022). Key applications involve AI-driven monitoring of traffic, smart lighting, and waste management. Cities like Boston are incorporating IoT into various systems, from parking meters to sewage grates. Smart Agriculture and Water Management: IoT can revolutionize agriculture by providing metrics on factors such as soil moisture, nutrient levels, and microclimate conditions, along with forecasting weather changes to help users mitigate risks such as fungi and other contaminants (Lutz & Coradi, 2022; Gopi et al., 2021). Retail and Logistics: Integrating IoT into the supply chain and retail management offers advantages like real-time tracking of storage conditions, product traceability, and automated processing of vendor payments in diverse settings (Aliahmadi et al., 2022; Saeed et al., 2020). In the retail sector, IoT can guide shopping based on selected lists, streamline payments based on biometrics, and automate shelf restocking (Hussein, 2019). Smart Living: IoT in the home sector provides remote control access to various applications, enhancing energy efficiency and safety (Leong et al., 2022; Humayun et al., 2020, Humayun et al., 2022). Smart appliances can monitor users' electricity

consumption, adjust temperature based on ambiance, and enable remote management of various appliances via mobile devices. Smart Environment: The use of IoT can revolutionize environmental strategies, from monitoring air quality and traffic management in cities to assessing water pollution (Pratomo, 2023; Almusaylim et al., 2020; Almuayqil, S. N et al., 2022). Additionally, IoT aids in waste management by monitoring and reducing industrial pollutants. Enhanced weather forecasting is made possible through IoT sensors placed on buildings and in various locations.

3. Background

3.1 Cloud computing

To understand what Cloud Computing Security is, let's first comprehend what cloud computing entails. As stated by Rajeswari (2019) from AJK College of Arts and Science, cloud computing is a collection of computing resources, including development tools, data storage, servers, applications, and more, accessible on-demand via the internet. These resources are hosted remotely at data centers and provided by Cloud Service Providers (CSPs). Examples of cloud computing include Salesforce, IBM Cloud, and Cisco (I. Hussain et al., 20222).

So, what is cloud computing security? Cloud computing security encompasses a set of best practices, protocols, and technologies employed to safeguard the entire cloud computing environment, covering infrastructure, applications, and data mentioned above. In general, CSPs primarily assume responsibility for backend development to mitigate security risks. Hence, a comprehensive scope of security for cloud computing is required to protect the physical network, such as routers, data storage, core network computing software and hardware, virtualization frameworks like virtual machines, end-user hardware, like the Internet of Things (IoT), and applications like productivity suites, data, runtime environments, middleware like Application Programming Interfaces (APIs), administrators, and Operating Systems (OS) (as illustrated in Image Figure 1.0 below) (Kaspersky, n.d.).

Cloud computing has experienced a surge in adoption since the COVID-19 pandemic crisis. According to Sumina (2022), 94% of enterprises use cloud services, and 48% store important or classified data in the cloud. Consequently, cloud computing security plays a critical role for consumers, businesses, and CSPs, serving as the frontline defense against security threats and breaches. Cloud computing security involves security policies and protocols, including robust data encryption and access control to prevent unauthorized access to sensitive data (George & George, 2021). In the event of a security breach, organizations and consumers become vulnerable.

Cloud computing security is more than just data protection; it also includes threat detection. Thanks to the utilization of global threat intelligence and endpoint scanning in cloud computing security, threats can be more easily detected, and their impact on an organization's critical assets can be assessed (George & George, 2021). Furthermore, cloud computing security can address regulatory compliance (George & George, 2021). Managed security services and infrastructure in cloud computing security help ensure industry-specific compliance requirements and regulatory standards are met. If an organization aims to enhance system availability by thwarting Distributed Denial of Service (DDoS) attacks, cloud computing security can assist in monitoring, analyzing, identifying, and continuously mitigating DDoS attacks. Its intelligence, scalability, flexibility, customizability, and built-in redundancies make it effective against slow, low, and volumetric attacks (George & George, 2021). The continuous monitoring offered by cloud

computing security means there is 24/7 visibility into an organization's cloud-based assets and applications, enabling a swift response to emerging threats and their impact on business (Rajeswari, 2019).

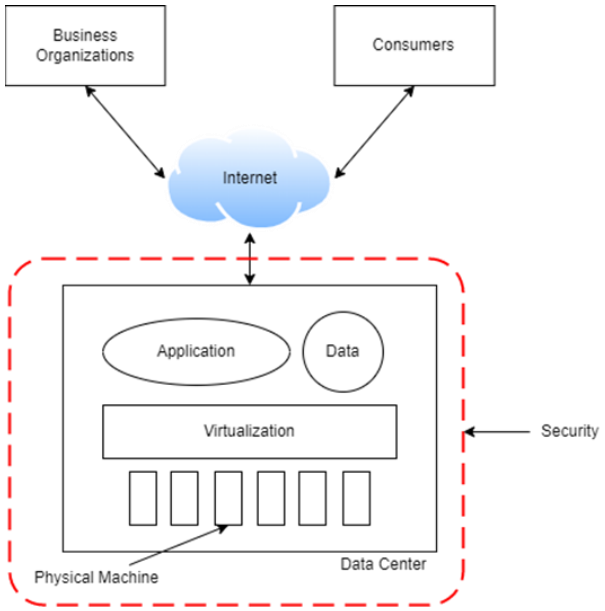

Figure 1.1: Basic Illustration of Cloud Computing Architecture with Security Protection (Bollinadi & Damera, 2017).

3.2 Internet of Things (IoT) Security

The Internet of Things (IoT) refers to devices or objects integrated with software, sensors, and other technologies that enable them to connect and exchange data with one another over the Internet (Oracle, n.d.). IoT security involves the measures taken to secure these internet-connected devices or objects from breaches and threats by monitoring, identifying, protecting, and regulating vulnerabilities that could pose security risks (Azrour et al., n.d.; Humayun et al., 2020b, Basavaraju, P. H, et al., 2022; Humayun, Jhanjhi, et al., 2022).

IoT devices find applications in various industries and sectors, which can generally be classified into consumer applications, business applications, and government applications (Wojcicki et al., 2022; Almusaylim, Alhumam, & Jhanjhi, 2020). Examples of consumer applications include devices that contribute to smart homes, smartphones, smartwatches, and more. Business applications encompass industrial machinery sensors, vehicle trackers, security cameras, and others. Government applications involve traffic monitoring sensors, wildlife trackers, and similar systems. The widespread implementation of IoT devices means they can be vulnerable to intrusion since they are often left unguarded and interconnected over the internet. Unauthorized access to IoT devices can result in security issues, as these devices may be configured to carry out malicious actions by intruders (Sathish et al., 2016; Diro et al., 2020). Thus, ensuring security in IoT is of utmost importance.

Why is IoT security important? It's because IoT devices lack physical partitions (GSM Association, 2020; Humayun, Jhanjhi, Hamid, et al., 2020). Unlike traditional network security, where device access can be restricted, such restrictions are inapplicable to IoT device networks since IoT devices must be configurable to the network when moved to different locations. IoT devices can serve as entry points for attackers to identify Wi-Fi configuration vulnerabilities. Depending on the discovered flaws, attackers may gain access to data transmissions, potentially stealing information such as credentials from the data stream. Furthermore, since IoT devices are often deployed in public areas, this provides attackers with opportunities for intrusion if the devices are not properly secured (GSM Association, 2020; Almusaylim & Jhanjhi, 2018b). If intruders gain physical access to these devices, they can compromise device internals, intercept communication, extract sensitive messages, manipulate device functionality, and cause data leaks, ultimately affecting the confidentiality, integrity, and availability of IoT systems. Therefore, the absence of IoT security measures leaves the door open for cyberattacks at any time.

4. Discussion on Security Issues

4.1 IoT Security Components

Four fundamental components constitute the IoT Security System:

Sensors/Devices: Sensors are devices that collect data, which can be either real-time or based on timestamps, such as every minute. Examples of sensors include temperature sensors for monitoring temperature and light sensors for measuring light brightness. A single device may consist of multiple sensors bundled together to function as a system rather than a standalone sensing device. A prime example of this is smartwatches, which are equipped with numerous sensors to offer multiple functionalities (Tawalbeh et al., 2020; Alshammari et al., 2017).

Connectivity: The connectivity phase involves the transportation of data collected by these sensors for storage or processing. Typically, this data transfer occurs through cloud infrastructure using technologies like Wi-Fi, Bluetooth, and cellular networks, among others. The choice of technology depends on the type of device and its intended function, with considerations including factors like bandwidth, speed, and power consumption (Tawalbeh et al., 2020; Humayun et al., 2022).

Data Processing: Once the data is collected and successfully transmitted, it needs to be processed. This processing can range from simply checking whether a temperature reading from a sensor falls within an acceptable threshold to more complex tasks, such as recognizing and identifying objects using technologies like computer vision. There may also be instances where user interaction is required, such as when a temperature reading exceeds the acceptable threshold. The figure below illustrates some interactions between the user and the system.

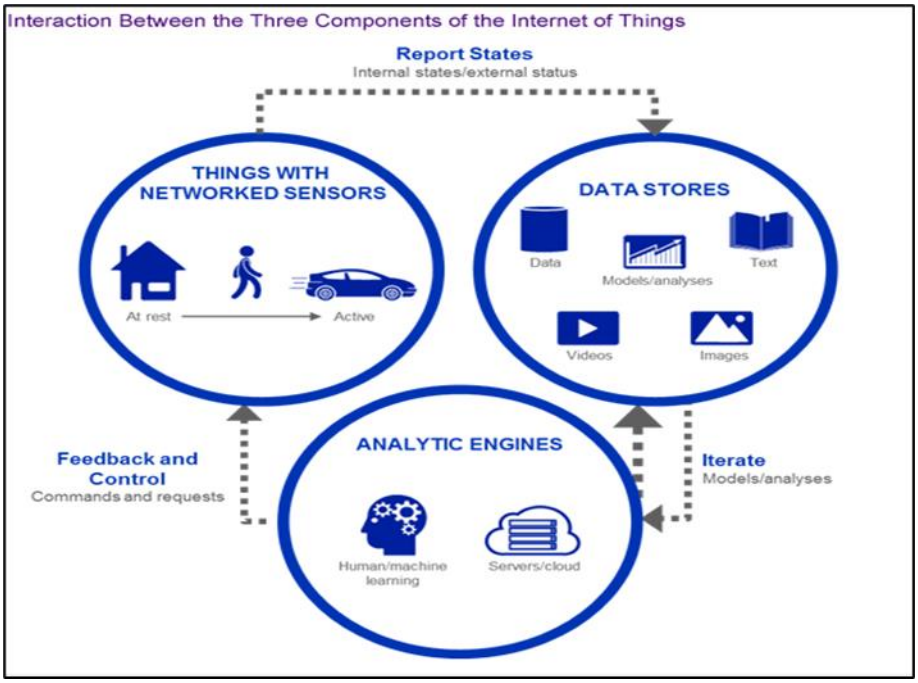

Figure 1.2: Interaction between the three components of the IoT (Patel, 2018)

User Interface

Moving on to the final component, this is where all the information collected and processed becomes accessible and available to the user in various ways. This can range from simple notifications or alarms to more interactive scenarios. In some cases, users may actively monitor interfaces, such as security camera feeds, allowing them to view live recordings or access web interfaces to review recorded content. The extent of user interaction depends on the nature and complexity of the IoT system and its specific application. For instance, in the case of smart refrigerators, users might need to adjust the temperature based on specific situations. On the other hand, there could be predefined criteria that trigger actions when certain conditions are met (Panchiwala & Shah, 2020). The figure below illustrates a straightforward dashboard of a smart home IoT system.

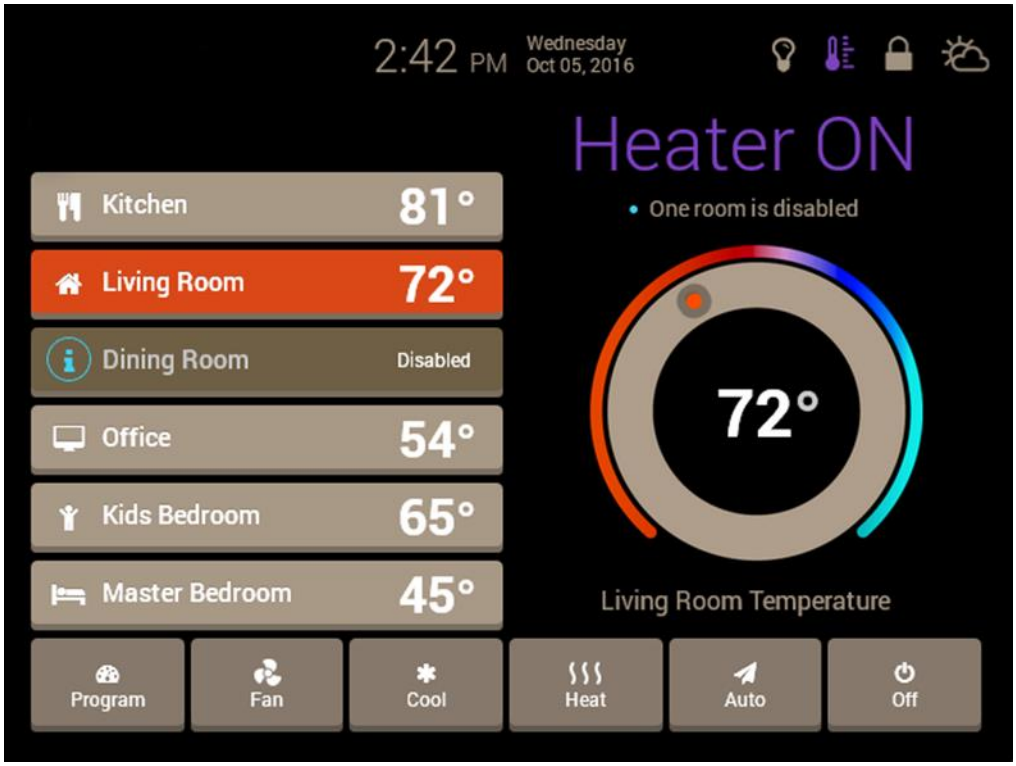

Figure 1.3: IoT Smart Home Dashboard (Smart Home Dashboard Sketch Freebie, n.d)

4.2 IoT Security Processes

Several sub-processes occur at these layers to constitute the entire IoT Security Process. Some research papers propose a three-layer architecture, while others suggest a four or five-layer architecture. In this paper, we will focus on the four layers that form the backbone of IoT security processes.

a. Perception Layer

IoT devices are typically designed for low energy consumption, which results in limited computational resources. This constraint makes it challenging to implement computationally intensive security solutions directly on the device (Rayapuri, 2018; Sankar et al., 2020, Sangkaran, T et al., 2020). A common security issue at this layer is the duplication or cloning of chips inside these devices for conducting cyberattacks (Yu et al., 2018). For example, an RFID tag could be cloned multiple times to initiate a Distributed Denial of Service (DDoS) attack.

b. Connectivity or Transport Layer

This layer is crucial in IoT security, as data transmission is key to the functioning of devices and the sustainability of entire IoT systems. Technologies like Intrusion Detection Systems are often employed to enhance security at this layer by monitoring packets and detecting attacks (Micheal and Bose, 2018). Various algorithms and statistical techniques are utilized to detect and classify threats. An example of threat detection is using deep learning models to identify DDoS attacks with remarkable accuracy (97%) (Susilo and Sari, 2020).

c. Processing Layer

At this layer, data collected from the network layer is processed. Processing techniques are applied to filter out extraneous information, ensuring that only relevant and useful data is collected. Security concerns at this stage may involve the use of malware to compromise user data confidentiality. This could be achieved through interaction with the system via viruses, trojan horses, worms, scripts, executable codes, or files (Rao and Clarke, 2020).

d. Application Layer

This layer involves monitoring, processing, sharing, and controlling information, which is a common feature of enterprise IoT applications. Security management approaches may vary depending on different application areas, such as smart health and smart home systems. The services offered by these applications depend on the type of information collected by the sensors. For example, in an IoT-based smart home system, security issues may arise due to the limited computational power and storage capacity, such as ZigBee. Cross-site scripting (XSS) attacks are one type of possible attack on IoT-based smart home systems, allowing attackers to insert and execute client-side scripts (e.g., JavaScript) within a trusted site viewed by the user. This can grant malicious attackers complete access to the application's contents, which they can modify as they please (Nizetic et al., 2020, Nawaz, A et al., 2021).

4.3 IoT Security Threats

There is a higher probability for an IOT application to receive a security threat because IOT infrastructure and devices are sensitive to enough probabilities, which makes it vulnerable to attacks, especially on these four layers which are the sensing layer, network layer, middleware layer, and application layer. The security threats can be represented in these four layers. Hence, mainly malicious is the only reason why IoT devices fail.

4.3.1 Sensing layer

a. Node Capturing

Sensors and actuators exemplify low-power nodes utilized in IoT applications, making them susceptible to various adversarial threats. Malevolent actors may endeavor to capture or substitute an IoT system's node with a malicious one. Once compromised, the attacker gains control over the substituted node, which disguises itself as a legitimate system component. This poses a significant security risk to the entire IoT program (Alouffi et al., 2021).

b. Jamming of a Node in a Wireless Sensor Network

Hackers can execute attacks like jamming by interfering with the radio frequencies used by wireless sensor nodes, disrupting their transmissions, and impeding communication. If this attack successfully targets critical sensor nodes, it can lead to interruptions in IoT services. Employing a high volume of corrupted signals, a DoS attack can overwhelm RF signals, disrupting the network and resulting in RF jamming.

c. Side-Channel Attack (SCA)

A side-channel attack is a malicious technique utilized by hackers to extract sensitive information. It can be employed to obtain confidential data from a chip, encompassing power consumption attacks, laser-based attacks, and timing attacks. A combination of these methods is typically required for a successful side-channel attack to leak confidential data, including details about processor microarchitecture, electromagnetic emissions, and power usage (Alouffi et al., 2021).

4.3.2 Network Layer

a. Access Attack

An Access Attack, also known as an Advanced Persistent Threat (APT), involves an unauthorized individual or adversary gaining entry to an IoT network (Awotunde & Misra, 2022). In this form of attack, the attacker may go undetected within the network for an extended period. The primary objective of this assault is not to cause network damage but to pilfer critical and sensitive information. IoT applications routinely collect and transmit vital data, rendering them particularly susceptible to such attacks.

b. Data Transit Attacks

Data Transit Attacks occur during the movement of data from one point to another, as opposed to data at rest in local servers. Data in transit is more vulnerable to attacks compared to data stored locally, primarily because IoT applications involve frequent data movements between sensors, actuators, the cloud, and other elements. The diversity of connection technologies used in data movement also contributes to the susceptibility of Data Transit Attacks.

c. Routing Attacks

Routing Attacks involve hackers attempting to manipulate the routing paths during data transit by introducing malicious nodes. A specific type of routing attack, known as a Sinkhole attack, creates a deceptive shortest routing path to attract and redirect traffic through compromised nodes. Another type, the Wormhole attack, establishes an out-of-band connection between two nodes to expedite data transfer. If these two attacks are combined, it presents a significant security threat. A Wormhole attack can be executed when an attacker gains control of a node and an internet-connecting device and bypasses the low-level security protocols in IoT applications.

4.3.3 Middleware Layer

a. Flooding Attack in the Cloud

A flooding attack in the cloud is a type of attack that impacts the quality of service, functioning similarly to a Denial of Service (DoS) attack. The objective of this attack is to reduce cloud resources. The hacker achieves this by continuously sending a large volume of requests to the cloud service, which significantly affects the cloud system and increases the server load.

b. Signature Wrapping Attack

A Signature Wrapping Attack targets web services that utilize XML signatures as part of their middleware. By identifying vulnerabilities in the Simple Object Access Protocol (SOAP), an attacker can bypass the signature algorithm, allowing them to launch attacks and manipulate intercepted messages. This attack is a method of tampering with the security of web services.

c. Cloud Malware Injection

In a Cloud Malware Injection attack, a hacker gains access to the cloud by injecting malicious code or implanting a virtual machine. They may attempt to establish a virtual machine instance or a malicious service module to impersonate a legitimate service. Through this approach, the attacker gains access to the victim's service requests and can acquire confidential data, which can be modified according to the specific circumstances or objectives of the attack. This type of attack poses a significant threat to cloud security and data integrity.

4.3.4 Application Layer

a. Access Control Attacks

Access control is a system that restricts access to data or accounts to only authorized individuals or processes. In IoT applications, access control attacks are critical because once access is exploited, the entire IoT application becomes vulnerable to attacks. Attackers who successfully bypass access controls can potentially compromise the security and integrity of the IoT network.

b. Sniffing Attacks

Cybercriminals can employ sniffer programs to monitor network traffic in IoT applications. In the absence of security mechanisms to prevent this, intruders can capture sensitive user data. Sniffing attacks can lead to the unauthorized collection of data, which could then be misused for various purposes, including unauthorized access or data theft.

c. Reprogramming Attacks

Unless the programming process is adequately secured, intruders may find it relatively easy to reprogram IoT devices. This presents a significant security risk, as unauthorized reprogramming can lead to IoT networks being hacked. Proper security measures are essential to prevent such reprogramming attacks and ensure the integrity of IoT device functionality.

4.4 Example of IoT security technology usage

The application of IoT security is indeed crucial in various scenarios, as outlined in your description. Let's break down the importance of IoT security in the context of smart utilities, smart agriculture, and Industrial IoT:

1. Smart Utilities:

Smart Metering and Grids: In the realm of smart utilities, like smart metering and grids, IoT security is vital. Smart grids are decentralized energy systems that rely on IoT for real-time communication and monitoring. Attackers can potentially compromise the grid through attacks such as Denial-of-Service (DoS) attacks, injections, or IP spoofing. The consequences can be severe, including disruptions in energy supply and even overloading power station nuclear reactors. The Ukraine Power Grid incident in 2016 is a stark example of the potential impact of such attacks. IoT security is essential to safeguard these critical infrastructure systems.

2. Smart Agriculture:

Agricultural Automation: IoT plays a significant role in automating agricultural processes. Farmers use IoT sensors for tasks like livestock tracking, automated fertilizer and water dispensing, and crop monitoring. Given the vast geographical area of agricultural plantations, a multitude of IoT devices are deployed. However, these devices are often resource-constrained, making them susceptible to attacks. Replay attacks, Man-in-the-Middle (MiM) attacks, and spoofing are common threats. With IoT security, including proper authentication mechanisms, these attacks can be mitigated, protecting farmers from resource theft, equipment damage, or IoT hijacking for malicious purposes.

3. Industrial IoT (Industry 4.0):

Manufacturing Automation: Industry 4.0 relies on Industrial IoT to automate manufacturing processes, improving efficiency and productivity. IoT sensors optimize machine control, provide predictive maintenance, and enhance monitoring. However, these machines are often controlled by Supervisory Control and Data Acquisition (SCADA) networks, making them vulnerable to cyber threats. The injection of viruses or worms into these networks can compromise the entire factory, leading to severe disruptions. The German Steel Mill Attack in 2014 is a case in point. IoT security is indispensable in ensuring the safe and uninterrupted operation of industrial processes.

In summary, the application of IoT security is essential wherever IoT technology is deployed. It helps safeguard critical infrastructure, protect agricultural resources, and ensure the uninterrupted operation of industrial processes. As IoT continues to expand, the need for robust security measures becomes even more critical to mitigate potential risks and vulnerabilities.

4.5 Cloud Computing Security Components

Cloud security is indeed a critical aspect of cloud computing, and understanding its various components is essential. Here's an overview of the key components involved in cloud security:

a. Data

Data in cloud security refers to all the information generated, processed, and stored in the cloud environment. This includes data modification and access. Protecting data is crucial, as it is often the primary target for malicious actors. For example, data stored in cloud-based services like Google Drive is considered information that needs to be securely managed.

b. Applications

Applications in the context of cloud security encompass a wide range of software services, from standard applications like email and word processors to more specialized and tailored software designed to handle specific types of data. Ensuring the security of these applications is essential to protect sensitive information. Tax or accounting software can serve as an example of application security requirements.

c. Operating System (OS)

The choice of an operating system is a significant decision when setting up a cloud environment. An OS manages the hardware and software resources, and it should be selected based on an organization's needs and requirements. Linux is commonly used for servers due to its specialization in handling server tasks, but the choice of OS must consider user-friendliness and other factors.

d. Virtualization

Virtualization is a key enabling technology for cloud computing. It allows the creation, migration, sharing, and management of virtual machines. The security of these virtual machines is paramount, as they can potentially harm physical hardware. Tools like VirtualBox enable the creation of virtual machines, and their security is a critical component of cloud security.

e. Servers

Even in a virtualized cloud environment, physical hardware is essential. This includes physical servers, network devices like routers and switches, and storage devices. Protecting the physical infrastructure is vital for ensuring the reliability and security of the cloud environment.

f. Storage

Storage in cloud security involves abstracting storage from physical hardware through virtualization. This enables the creation of storage pools and allows for automatic scaling and provisioning. The security of these storage resources is essential to prevent data breaches and unauthorized access.

g. Networking

Networking components are crucial in connecting cloud-based systems to public networks or creating virtual private networks within the cloud itself. Public cloud providers often offer secure virtual private networks (VPNs) to clients to access cloud resources securely. For example, Amazon Cloud provides a Virtual Private Cloud (VPC) to facilitate secure communication between cloud components. Understanding and implementing security measures for each of these components is vital to maintaining the integrity and confidentiality of data and services within a cloud environment.

4.6 Cloud Computing Security Processes

The process of cloud security is a fundamental aspect of maintaining the integrity and confidentiality of data and services in a cloud environment. Here are the key components of the cloud security process:

a. Identification

This process involves establishing the privilege of accessibility for specific users or accounts. It encompasses both authentication and authorization, ensuring that users are who they claim to be and that

they have the appropriate permissions. Access Control Lists (ACLs) are valuable tools for controlling and restricting access, which is critical for preventing unauthorized access to data or unauthenticated users accessing the system.

b. Security Controls

Security controls are measures put in place to establish and manage the overall security posture of an organization. This involves defining parameters, policies, and security configurations to be implemented across all accounts, users, and infrastructure. These controls help enforce security policies and best practices to protect against threats and vulnerabilities.

c. Compliance

The compliance process focuses on protecting customer/user privacy and aligning the cloud security architecture with industry standards and regulatory requirements. It ensures that the organization adheres to relevant laws and regulations, such as data protection laws (e.g., GDPR) and industry-specific compliance standards (e.g., HIPAA for healthcare).

d. Data Encryption

Data encryption is a critical process that ensures the security and privacy of user data. It involves encrypting data both at rest (when stored) and during transit (when moving within the cloud or externally). Data encryption helps minimize the potential impact of data breaches by making data indecipherable to unauthorized parties.

e. Governance

Governance in cloud security centers on creating and enforcing policies that prevent, detect, and mitigate threats. These policies help guide safe user behavior and often include user training and awareness programs. While governance processes are typically associated with larger organizations, they can also benefit individual cloud clients by promoting best practices and security awareness.

Implementing these processes systematically and thoroughly is essential to maintaining robust cloud security. Cloud security is an ongoing effort that requires a combination of technical measures, policy enforcement, and user education to protect against a constantly evolving threat landscape.

4.7 Cloud Computing Security Threats

Cloud computing security has been subjected to various types of attacks. These attacks primarily target the different layers of the cloud environment. One prevalent form of attack is Distributed Denial of Service (DDoS), which involves multiple compromised computers, often referred to as 'bots' or 'zombies,' launching coordinated attacks on network services or systems, rendering them inaccessible. DDoS attacks typically target three layers in Software-Defined Networking (SDN), which supports cloud providers in hosting virtual networks: the application layer, control layer, and data layer.

At the application layer, two methods are commonly used for executing application layer DDoS assaults. One method targets specific SDN applications, while the other focuses on the SDN's northbound API. The challenge here lies in the difficulty of isolating applications within the system. An attack on one application layer can inadvertently affect unrelated applications, potentially jeopardizing SDN security.

The control layer, often considered the crux of SDN security, is highly vulnerable to attacks due to a single failure. Control plane DDoS attacks can take the form of assaults on the controller, northbound APIs, and southbound APIs. Unique applications can create conflicting flow rules, leading to DDoS attacks in the control layer, as the controller only understands how to proceed with a specific set of flow rules.

In the data layer, DDoS attacks are initiated when routers are targeted, or when the southbound API is compromised. Preventing harmful programs from accessing the data plane is essential. Some of these issues can be mitigated by introducing minimal insight into data plane devices. One approach is to employ an SDN setup checking design device, often referred to as an 'SDN scanner,' which remotely identifies networks that employ SDN, demonstrating the feasibility of DDoS attacks. Modifying existing network monitoring tools, such as ICMP checking and TCP SYN filtering, is a straightforward way to implement this method. This remote attack on an SDN network can significantly disrupt the implementation of an SDN scheme without the need for sophisticated equipment.

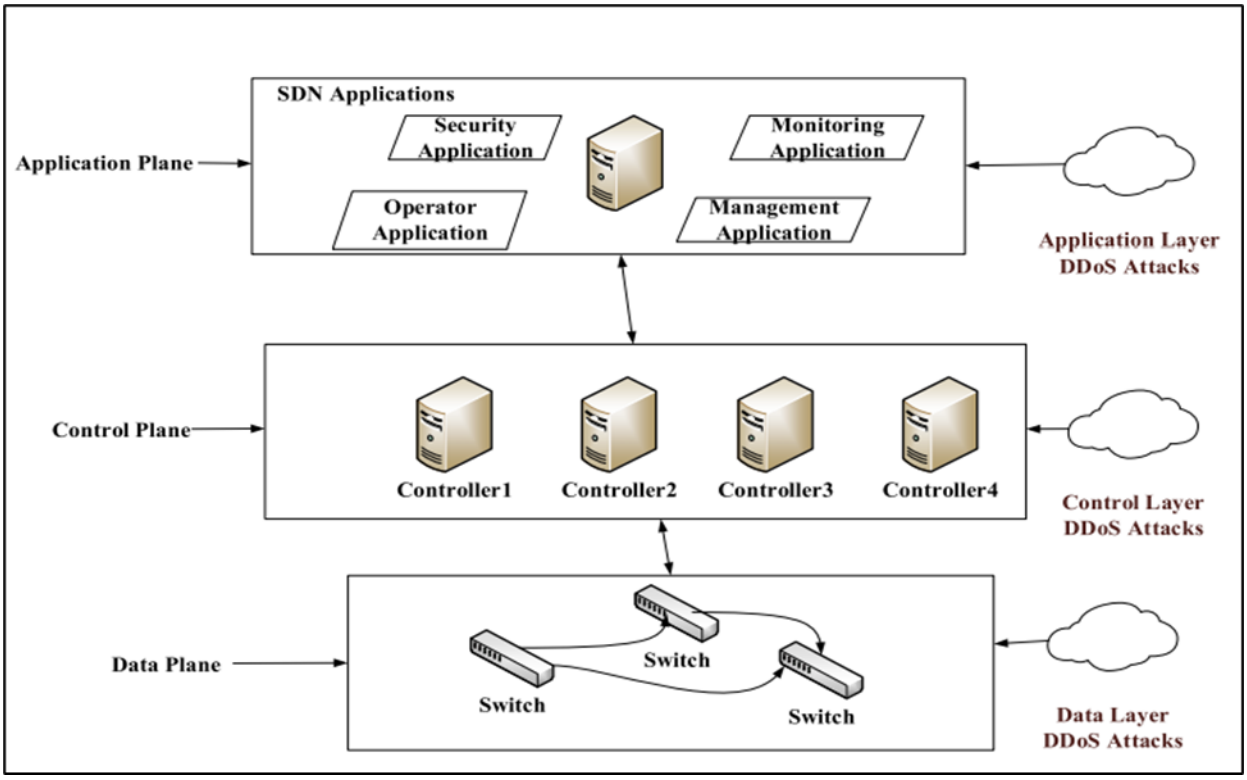

Figure 1.4: Cloud computing security attack

A Man-in-the-Middle (MitM) attack is a concerning security threat, particularly within Platform as a Service (PaaS). This type of attack occurs when an attacker or hacker attempts to intercept an ongoing conversation and inject false information to gain access to classified data that is being disclosed. To secure web-based applications, a Secure Socket Layer (SSL) is employed. SSL utilizes TCP to provide reliable end-to-end secure services through three main protocols: the Handshake protocol, the Change Cipher Spec protocol, and the Alert protocol. SQL injection is a common form of attack typically directed at Software as a Service (SaaS) platforms. In this type of attack, the assailant inserts malicious code into standard SQL code to gain unauthorized access to a database and extract confidential user data. In this scenario, the website inadvertently allows the attacker's input to be interpreted as SQL commands by the SQL Server, which can result in unauthorized access to the website's structure and data. Consequently, the attacker may make unauthorized modifications.

4.8 Example of Cloud Computing Security Technology Usage

Businesses and corporations, regardless of their size, are mandated to implement cloud computing security when using any cloud computing services in their operations. In addition to these organizations, critical sectors like the banking industry, exemplified by Bank Negara Malaysia's adoption of Google Cloud Security (Google Cloud, n.d.), the financial industry, and the e-commerce sector, must also prioritize cloud computing security. These sectors and businesses house a wealth of sensitive data, including but not limited to customer personal information.

For instance, the banking industry safeguards customer data such as account numbers and transaction details, while e-commerce businesses secure customer login credentials and order information. Protecting this vulnerable data is paramount to prevent data breaches and leaks, as a breach would compromise the fundamental principles of data security. Cloud computing security plays a pivotal role in safeguarding data from tampering since physical machines are no longer in play, and unauthorized access to machines becomes impossible. Additionally, it facilitates data backups and periodic patch updates, ensuring state-of-the-art security for companies (Hassija et al., 2019). These measures, in turn, enhance data integrity, one of the key facets of data security.

For businesses, corporations, and industries looking to implement cloud computing security, it's essential to understand that different Cloud Service Providers (CSPs) offer varying levels of cloud computing security and adhere to different cloud security frameworks. Three of the most prevalent cloud security frameworks are the Cloud Security Alliance (CSA), the National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO). These frameworks serve as checklists and self-assessment tools to establish robust security measures for systems (Hassija et al., 2019). It's crucial to recognize that cloud computing security isn't limited to businesses and industries alone; it's a concern that extends to individuals worldwide. Security should be treated as a matter of paramount importance by everyone, transcending the realm of IT and becoming a collective responsibility.

5. Discussion of the Impact

5.1 Benefits of Cloud Computing Security

To reap the advantages of cloud computing, your company should collaborate with cutting-edge private cloud computing providers without compromising security. Here are five benefits of a robust cloud computing security solution (Kumar, 2019, Kumar, K, et al., 2020):

a. Protection against DDoS Attacks

Distributed Denial of Service (DDoS) attacks are on the rise, and a top-tier cloud computing security strategy emphasizes methods to prevent excessive traffic from reaching a company's cloud servers. This involves thwarting, retaining, and dispersing DDoS attacks to mitigate risk.

b. Data Security

An effective cloud computing security solution encompasses established security protocols to safeguard sensitive data and transactions in an era marked by constant data breaches. This shields against unauthorized eavesdropping and interference during data transmission (Torkura et al., 2020).

c. Regulatory Compliance

Leading cloud computing security solutions assist companies in regulated industries by maintaining advanced systems for compliance and safeguarding personal and financial data (Rashid & Chaturvedi, 2019).

d. Flexibility

A cloud computing system provides the security required, whether you are scaling up or down. By expanding your cloud setup, you can prevent server downtime during peak traffic periods. After the peak, you can scale down to reduce costs (Rashid & Chaturvedi, 2019).

e. High Availability and Support

A best-practices cloud computing security plan ensures the continuous performance of a company's operations. This includes round-the-clock live monitoring, 365 days a year. Redundancies are integrated to ensure your business's website and applications remain accessible at all times (Rashid & Chaturvedi, 2019).

By engaging with cutting-edge private cloud computing providers and adopting a robust cloud computing security solution, your company can harness these benefits without compromising its security.

5.2 Issues limitations, and Challenges associated with Cloud computing security.

Security concerns in cloud computing are on the rise, and it's crucial to address these concerns based on cloud delivery and deployment approaches. Key decision-makers and organizations need to pay attention to some major security issues, as outlined by Radwan, T. et al. in 2019:

1. Insecure Application Programming Interfaces (APIs)

This security concern affects nearly all cloud service providers. Customers interact with, establish, manage, and monitor services through software interfaces and APIs. The use of insecure APIs and interfaces can jeopardize access to sensitive data, exposing organizations to various security risks and

vulnerabilities. To mitigate this risk, it's essential to implement highly secure access control measures such as authentication, encryption, and monitoring to prevent malicious interactions with these services and APIs.

2. Malicious Insiders

Malicious insiders pose a well-known threat that can impact any cloud delivery model, making them a concern for most organizations. The hiring process used by providers, the permissions granted to employees for accessing assets, and the oversight of their activities are often not transparent. Hackers may find this situation appealing as an opportunity to steal sensitive data or gain control over all cloud services without detection. A notable example is the case of Edward Snowden and the NSA. To ensure a secure cloud experience, compliance reporting, breach notification, and transparency into provider operations and procedures are essential.

3. Shared Technology Vulnerabilities

Infrastructure as a Service (IaaS) providers employ multi-tenancy, relying on shared infrastructure. However, the design of components like disk partitions, shared database services, CPU caches, Graphics Processing Units (GPUs), and other elements lacks robust separation properties for multi-tenant architecture. This design has exposed certain security vulnerabilities and flaws that can impact the entire system even when no customers are directly affected.

5.3 Future Potential Cloud Computing Security

While there are numerous advantages to using the cloud, it also introduces new security threats and challenges. Organizations leveraging cloud computing technology can bolster their defenses with cutting-edge security technologies. Here are some of the most crucial cloud security technologies currently in development, as reported by Read Write in 2022:

5.3.1 Extended Detection and Response (XDR)

XDR technology is a unified incident response and security platform that allows data from various proprietary components to be collected and interconnected. Notably, these solutions offer built-in integration at the platform level, eliminating the need to purchase and integrate multiple disparate tools. Public cloud workloads face various security issues, including misconfigurations, unsecured APIs, insider threats, and unauthorized access. XDR addresses these challenges in the following ways:

Securing identity management: XDR technologies enable data collection from numerous cloud settings. In cases of suspicious activity on privileged accounts, XDR solutions can promptly alert security personnel. Analyzing massive cloud logs: Cloud workloads generate extensive log volumes, making manual analysis cumbersome. XDR tools can process cloud logs and utilize AI algorithms to identify potential risks. Analyzing network flows: Public cloud networks are often complex, making it challenging to detect threats. XDR tools scrutinize traffic across the entire cloud ecosystem and employ intelligent analysis to identify network security incidents. They can even respond automatically by isolating infected systems through network segmentation.

5.3.2 Web Application and API Protection (WAAP)

Web applications and application programming interfaces (APIs) are critical components of cloud environments, designed to be accessible from the Internet. Consequently, these technologies have access to sensitive data and credentials, rendering them prime targets for cybercriminals. Unlike traditional firewalls, which safeguard the network layer, Web Application and API Protection (WAAP) technology focuses on protecting traffic at the application layer. WAAP solutions are typically deployed on the public side of web applications, at the network's edge. Key features of WAAP solutions include:

Next-Generation Web Application Firewall (Next-Gen WAF): This protects against malicious bots, advanced rate limiting, safeguards for microservices and APIs, and defense against account takeovers (ATO). Detection of unauthorized access to customer accounts: WAAP can help identify unauthorized access to customer accounts via authentication APIs or the customer authentication process used within apps (Torkura et al., 2020). These advanced cloud security technologies are crucial for organizations seeking to fortify their cloud security posture.

5.4 Benefits of IoT Security

IoT devices must incorporate secure hardware, software, and communication protocols to function reliably. Appliances such as refrigerators and manufacturing robots are susceptible to compromise if adequate IoT security measures are not in place. Malicious hackers can gain control over these devices, jeopardizing their functionality and potentially stealing the user's digital data.

Implementing robust IoT security offers several advantages, including:

1. Enhancing operational efficiency and cost savings by leveraging reliable device data for decision-making.
2. Enabling monetization through accurate assessments of product usage and material consumption, backed by verifiable data.
3. Facilitating the adoption of new business models like 'product as a service' and 'pay-per-use' by ensuring the security and control of features.
4. Allowing companies to activate or deactivate features, facilitating upselling to clients while preventing fraud.
5. Providing a competitive edge to customers by adding security to their IoT devices.
   Safeguarding the valuable intellectual property of IoT devices through secure processing, safe storage, white box cryptography, and advanced software obfuscation (Laghari et al., 2021).

5.5 Issues limitations, and Challenges associated with IoT security

Confidentiality, integrity, and availability represent fundamental security objectives in any system, and the IoT is no exception. IoT faces unique challenges that complicate the implementation of security measures. One significant challenge is the inherent diversity among IoT nodes, each with distinct methods of connecting to the internet and varying levels of built-in protection. In the subsequent discussion, we will delve into the issues, limitations, and challenges that exist at each layer of the IoT ecosystem (Laghari et al., 2021)

a. Perception Layer

IoT nodes are typically located outdoors, exposing them to physical threats and the risks of natural disasters. These factors make IoT nodes susceptible to physical attacks, as attackers can tamper with device components if they have physical access. In many applications, IoT devices need to be mobile, which further increases their vulnerability to potential assaults. This layer predominantly consists of RFID sensors and wireless sensor networks, both of which face security challenges such as information leakage, replay attacks, clone attacks, and man-in-the-middle attacks. Additionally, these nodes are often limited in terms of storage capacity and computational capabilities, rendering them susceptible to various types of attacks. Replay attacks, for example, compromise the confidentiality of this layer by replicating or replaying device information. Timing attacks involve attackers analyzing encryption time. Malicious nodes can introduce fraudulent data into this layer, threatening data integrity and increasing the risk of Denial of Service (DoS) attacks. To mitigate these security challenges, encryption, steganography, access control, and authentication measures can be employed (Zikria et al., 2021; Almusaylim, Jhanjhi, & Alhumam, 2020, Zahra, F., Jhanjhi et al., 2022)

b. Network layer

This layer is a prime target for a range of security threats, including eavesdropping, denial-of-service (DoS) attacks, unauthorized access, destruction, viruses, and Man-in-the-Middle attacks. Attackers can analyze network traffic and eavesdrop to compromise the security of the IoT. The increased remote access and data exchange in IoT systems heighten the probability of such attacks. Securing the key exchange is crucial to prevent these security breaches. IoT communication introduces novel security challenges as it primarily occurs between machines, not humans. These machines do not adhere to conventional security protocols and exchange critical data. Malicious actors can exploit IoT devices to collect extensive user information. Hence, safeguarding both IoT devices and networks is of paramount importance. While existing network protocols offer effective security mechanisms, they do not fully account for the heterogeneity inherent in IoT. Objects in the IoT ecosystem must be aware of the current network status and respond to anomalous activities that jeopardize security. Effective protocols and software solutions play a crucial role in securing IoT data (Zikria et al., 2021; Jabeen et al., 2023).

c. Application Layer

The absence of standardized regulations governing application interaction and development leads to various security vulnerabilities. The proliferation of authentication systems makes it challenging to guarantee data privacy. This layer is responsible for traffic management, making it susceptible to Denial of Service (DoS) attacks. The increasing number of connected devices and the volume of generated data can result in an application overload for data analysis, impacting service availability. When developing IoT applications, it is essential to consider user interaction and data generation (Zikria et al., 2021)

5.6 Future Potential IoT Security

Unification and Optimization

When IoT devices rely on protocols originally designed for the Internet, their performance and efficiency are hindered. For instance, protocols like HTTP pose challenges for IoT devices with limited computational capabilities. Additionally, the use of WIFI protocols can lead to significant energy

consumption. Due to technical constraints, some of the IoT communication protocols cannot easily interconnect or switch between them. As a result, there is a pressing need to update or extend existing IoT protocols to enable seamless communication between different IoT devices. The development of a new Wi-Fi type with lower power consumption is currently in progress (Ismail & Islam, 2020; Chaurasiya et al., 2023).

6. Conclusion

Confidentiality, Integrity, and Availability (CIA) form the fundamental building blocks of a robust security system recommended for IoT systems. The implementation of confidentiality in IoT ensures that messages exchanged between senders and receivers remain secure and protected from malicious or unauthenticated users. This, in turn, guarantees the security of communication networks and the messages transmitted between various IoT devices. Moving Integrity, serves to safeguard the content of communications between senders and recipients, ensuring that they remain untampered with by potential adversaries. Integrity checks can be conducted for every node involved in the message exchange process within an IoT system.

Availability is another crucial aspect of IoT security. It ensures that malicious users cannot disrupt or degrade the quality of communication or services provided by IoT systems or network infrastructure. To enhance physical layer security, it's advisable to employ lightweight cryptographic algorithms. Cryptographic algorithms and protocols are essential as they encrypt data during transmission, securing the resources of IoT devices. For network layer security, implementing measures such as communication security and identity authentication is essential to thwart unauthorized nodes. While contemporary cloud computing services have strong security measures in place, the primary threat comes from insider intruders. Implementing user activity monitoring and logging is a best practice to protect cloud computing services. This approach allows companies to track user access, making it easier to detect any unauthorized access or data breaches. Furthermore, cloud computing companies can actively monitor activities within their cloud computing security services, preempting potential threats and fortifying their defenses against future attacks.

7. References

[1] Ahmed, H., Nasr, A. A., Abdel-Mageid, S., & Aslan, H. K. A survey of IOT security threats and defenses. *International Journal of Advanced Computer Research*, **9**(45), 325–350. https://doi.org/10.19101/ijacr.2019.940088 (2019).

[2] Aletabi, H., & Abdallah, M. A. Proposed Cloud Quality Model (IaaSQual) for "Infrastructure as a Service (IaaS)" from User's Perspective. *2023 International Conference on Information Technology (ICIT)*. https://doi.org/10.1109/icit58056.2023.10225894 (2023).

[3] Aliahmadi, A., Nozari, H., & Ghahremani-Nahr, J. Big Data IoT-based Agile-Lean logistic in pharmaceutical industries. *International Journal of Innovation in Management Economics and Social Sciences*, **2**(3), 70–81. https://doi.org/10.52547/ijimes.2.3.70 (2022).

[4] Almusaylim, Z. A., & Jhanjhi, N. Z. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wireless Networks*, **25**(6), 3193–3204. https://doi.org/10.1007/s11276-018-1712-5 (2018).

[5] Almusaylim, Z. A., Alhumam, A., & Jhanjhi, N. Z. Proposing a Secure RPL based Internet of Things Routing Protocol: A Review. *Ad Hoc Networks*, **101**, 102096. https://doi.org/10.1016/j.adhoc.2020.102096 (2020).

[6] Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., & Jhanjhi, N. Z. Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things. *IEEE Explore*. https://doi.org/10.20944/preprints202007.0476.v1 (2020).

[7] Almusaylim, Z. A., Jhanjhi, N. Z., & Alhumam, A. Detection and Mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. *Sensors*, **20**(21), 5997. https://doi.org/10.3390/s20215997 (2020).

[8] Almuayqil, S. N., Humayun, M., Jhanjhi, N. Z., Almufareh, M. F., & Javed, D. Framework for improved sentiment analysis via random minority oversampling for user tweet review classification. Electronics, **11**(19), 3058 (2022).

[9] Alohali, Bashar, Vasilakis and Moscholios, I. (2018). more author) A Secure Scheme for Group Communication of Wireless IoT Devices. [online] **1**, 18–20. Available at: https://eprints.whiterose.ac.uk/141752/1/csndsp_IoT_2018.pdf [Accessed 1 Jun. 2022] (2018).

[10] Alouffi, B. et al. A systematic literature review on Cloud computing security: Threats and mitigation strategies. *IEEE Access*, **9**, 57792–57807. https://doi.org/10.1109/access.2021.3073203 (2021).

[11] Alruwaili, B. A. A. A. M., Humayun, M., & Jhanjhi, N. Z. Proposing a Load Balancing Algorithm For Cloud Computing Applications. *Journal of Physics*, **1979**(1), 012034. https://doi.org/10.1088/1742-6596/1979/1/012034 (2021).

[12] Alshammari, M. O., Almulhem, A. A., & Jhanjhi, N. Z. Internet of Things (IoT): Charity automation. *International Journal of Advanced Computer Science and Applications*, **8**(2), https://doi.org/10.14569/ijacsa.2017.080222 (2017).

[13] Awotunde, J. B., & Misra, S. Feature extraction and Artificial Intelligence-Based Intrusion Detection model for a secure internet of things networks. In *Lecture notes on data engineering and communications technologies*, 21–44, https://doi.org/10.1007/978-3-030-93453-8_2 (2022).

[14] Azrour, A., Mabrouki, J., Guezzaz, A. and Kanwal, A. Internet of Things Security: Challenges and Key Issues. Available at: https://www.researchgate.net/publication/354601482_Internet_of_Things_Security_Challenges_and_Key_Issues (Accessed: 28 May 2022) (2021).

[15] Basavaraju, P. H., Lokesh, G. H., Mohan, G., Jhanjhi, N. Z., & Flammini, F. Statistical channel model and systematic random linear network coding based qos oriented and energy efficient uwsn routing protocol. Electronics, **11**(16), 2590 (2022).

[16] Bollinadi, M., Damera, V. Cloud Computing: Security Issues and Research Challenges. Available at: https://www.jncet.org/Manuscripts/Volume-7/Issue-11/Vol-7-issue-11-M-12.pdf (Accessed: 27 May 2022) (2017).

[17] Chaurasiya, S. K., Biswas, A., Nayyar, A., Jhanjhi, N. Z., & Banerjee, R. DEICA: A differential evolution-based improved clustering algorithm for IoT-based heterogeneous wireless sensor networks. *International Journal of Communication Systems*, **36**(5). https://doi.org/10.1002/dac.5420 (2023).

[18] Diro, A. et al. Lightweight Authenticated-Encryption scheme for internet of things based on Publish-Subscribe communication. *IEEE Access*, **8,** 60539–60551. https://doi.org/10.1109/access.2020.2983117 (2020).

[19] Dong, S., Abbas, K. and Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access*, [online] **7,** 80813–80828, doi:10.1109/ACCESS.2019.2922196 (2019).

[20] Exabeam. *Cloud Security: Principles, Solutions, and Architectures - Exabeam*. [online] Available at: https://www.exabeam.com/explainers/cloud-security/cloud-security-principles-solutions-and-architectures/ [Accessed 31 May 2022] (2022).

[21] George, S. and George H. *Serverless Computing: the Next Stage in Cloud Computing's Evolution and an Empowerment of a New Generation of Developers.* Available at: https://www.researchgate.net/publication/350580133_Serverless_Computing_the_Next_Stage_in_Cloud_Computing's_Evolution_and_an_Empowerment_of_a_New_Generation_of_Developers (Accessed: 28 May 2022) (2021).

[22] Gill, S. H. et al. Security and privacy aspects of cloud Computing: A Smart Campus case study. *Intelligent Automation and Soft Computing*, **31**(1), 117–128. https://doi.org/10.32604/iasc.2022.016597 (2022).

[23] Gill, S. S., Cabral, A., Fuller, S., Chen, Y., & Uhlig, S. Facilitating an online and sustainable learning environment for cloud computing using an action research methodology. In *Advances in higher education and professional development book series*, 43–70, https://doi.org/10.4018/978-1-6684-6172-3.ch003 (2023).

[24] Google Cloud. (n.d.) *Bank Negara (Malaysia)*. Available at: https://cloud.google.com/security/compliance/bank-negara-malaysia (Accessed: 27 May 2022).

[25] Gopi, R. et al. Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimedia Tools and Applications*, **81**(19), 26739–26757. https://doi.org/10.1007/s11042-021-10640-6 (2021).

[26] GSM Association. *IoT Security Guidelines Endpoint Ecosystem.* Available at: https://www.gsma.com/iot/wp-content/uploads/2020/03/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf (Accessed: 29 May 2022) (2020).

[27] Hassija, V. et al. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, **7,** 82721–82743, doi:10.1109/access.2019.2924045 (2019).

[28] Hassija, V. et al. A survey on IOT security: Application areas, security threats, and solution architectures. *IEEE Access*, **7,** 82721–82743. https://doi.org/10.1109/access.2019.2924045 (2019).

[29] Humayun, M., Alsaqer, M., & Jhanjhi, N. Z. Energy optimization for smart cities using IoT. *Applied Artificial Intelligence*, **36**(1). https://doi.org/10.1080/08839514.2022.2037255 (2022).

[30] Humayun, M. et al. Privacy protection and energy optimization for 5G-Aided industrial internet of things. *IEEE Access*, **8,** 183665–183677, https://doi.org/10.1109/access.2020.3028764 (2020).

[31] Humayun, M. et al. Privacy protection and energy optimization for 5G-Aided industrial internet of things. *IEEE Access*, **8,** 183665–183677. https://doi.org/10.1109/access.2020.3028764 (2020).

[32] Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, **22**(1), 105–117, https://doi.org/10.1016/j.eij.2020.05.003 (2021).

[33] Humayun, M., Jhanjhi, N. Z., Hamid, B., & Ahmed, G. Emerging smart logistics and transportation using IoT and blockchain. *IEEE Internet of Things Magazine*, **3**(2), 58–62, https://doi.org/10.1109/iotm.0001.1900097 (2020).

[34] Humayun, M. et al. Software-as-a-service security challenges and best practices: A multivocal literature review. Applied Sciences, **12**(8), 3953 (2022).

[35] Humayun, M., Jhanjhi, N. Z., & Almotilag, A. Real-time security health and privacy monitoring for Saudi highways using cutting-edge technologies. Applied Sciences, **12**(4), 2177 (2022).

[36] Hussein, A. H. Internet of things (IOT): Research challenges and future applications. *International Journal of Advanced Computer Science and Applications*, **10**(6). https://doi.org/10.14569/ijacsa.2019.0100611 (2019).

[37] Ibm.com. *What is Cloud Security? Cloud Security Defined | IBM*. [online] Available at: https://www.ibm.com/topics/cloud-security#:~:text=CSPM%20addresses%20these%20issues%20by,mitigation%2C%20and%20digital%20asset%20management. [Accessed 31 May 2022] (2019).

[38] Hussain, I. et al. "Health Monitoring System Using Internet of Things (IoT) Sensing for Elderly People," 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2022, 1-5, doi: 10.1109/MACS56771.2022.10023026 (2022).

[39] Jabeen, T. et al. An intelligent healthcare system using IoT in wireless sensor network. *Sensors*, **23**(11), 5055. https://doi.org/10.3390/s23115055 (2023).

[40] Jurcut, A., Pasika, R. & Lina, X. *Introduction to IoT Security*. Available at: https://www.researchgate.net/publication/336406296_Introduction_to_IoT_Security (Accessed: 27 May 2022) (2019).

[41] Kaspersky. *What is Cloud Security?* [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security [Accessed 31 May 2022] (2022).

[42] Kaspersky. (n.d.) What is Cloud Security? Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security (Accessed: 27 May 2022).

[43] Khattak, S. B. A., Nasralla, M. M., Farman, H., & Choudhury, N. Performance evaluation of an IEEE 802.15.4-Based thread network for efficient Internet of things communications in smart Cities. *Applied Sciences*, **13**(13), 7745. https://doi.org/10.3390/app13137745 (2023).

[44] Kumar, R., & Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, **33,** 1–48 https://doi.org/10.1016/j.cosrev.2019.05.002 (2019).

[45] Kumar, K., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). A Survey of The Design and Security Mechanisms of The Wireless Networks and Mobile Ad-Hoc Networks. In IOP Conference Series: Materials Science and Engineering, **993**(1), 012063, IOP Publishing (2020).

[46] Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. Retracted article: A review and state of art of internet of things (IOT). *Archives of Computational Methods in Engineering*, **29**(3), 1395–1413. https://doi.org/10.1007/s11831-021-09622-6 (2021).

[47] Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, **12**(9), 157. doi:10.3390/fi12090157 (2020).

[48] Leong, Y. R., Tajudeen, F. P., & Yeong, W. C. Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. *Universal Access in the Information Society*. https://doi.org/10.1007/s10209-022-00937-0 (2022).

[49] Levin, M. *The Rising IoT Threat to the Agriculture Industry and the Global Food Supply*. Available at: https://www.f5.com/labs/articles/threat-intelligence/the-rising-iot-threat-to-the-agriculture-industry-and-the-global-food-supply (Accessed: 27 May 2022) (2020).

[50] Logesswari, S., Jayanthi, S., KalaiSelvi, D., Muthusundari, S. & Aswin, V. A study on cloud computing challenges and its mitigations. Materials Today: Proceedings. [online] doi:10.1016/j.matpr.2020.10.655 (2020).

[51] Lutz, É., & Coradi, P. C. Applications of new technologies for monitoring and predicting grains quality stored: Sensors, Internet of Things, and Artificial Intelligence. *Measurement*, **188,** 110609. https://doi.org/10.1016/j.measurement.2021.110609 (2022).

[52] Malviya, A., & Dwivedi, R. K. A comparative analysis of container orchestration tools in cloud computing. *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*. https://doi.org/10.23919/indiacom54597.2022.9763171 (2022).

[53] Micheal, T. and Bose, S. *A Study of Threat Analysis of Lot Networks Using Artificial Neural Network.* Available at: https://ijariie.com/AdminUploadPdf/A_Study_of_Threat_Analysis_of_Lot_Networks_Using_Artificial_Neural_Network_ijariie13943.pdf (Accessed: 27 May 2022) (2018).

[54] Mikova, T. *Cyber Attack on Ukrainian Power Grid.* Available at: https://is.muni.cz/th/uok5b/BP_Mikova_final.pdf (Accessed: 27 May 2022) (2018).

[55] Muzammal, S. M., Murugesan, R. K., & Jhanjhi, N. Z. Introducing Mobility Metrics in Trust-based Security of Routing Protocol for Internet of Things. *IEE Explore*. https://doi.org/10.1109/nccc49330.2021.9428799 (2021).

[56] Muzammal, S. M., Murugesan, R. K., & Jhanjhi, N. Z. A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches. *IEEE Internet of Things Journal*, **8**(6), 4186–4210, https://doi.org/10.1109/jiot.2020.3031162 (2021).

[57] Muthukkumar, R. et al. A genetic algorithm-based energy-aware multi-hop clustering scheme for heterogeneous wireless sensor networks. PeerJ Computer Science, **8,** e1029 (2022).

[58] Amara, N., Zhiqui, H. & Ali, A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 244-251, doi: 10.1109/CyberC.2017.37 (2017).

[59] Nawaz, A. Feature engineering based on hybrid features for malware detection over Android framework. Turkish Journal of Computer and Mathematics Education (TURCOMAT), **12**(10), 2856-2864 (2021).

[60] Nizetic, S., Solic, P., Lopez, D. and Patrono, L. *Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future*. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7368922/ (Accessed: 27 May 2022) (2020).

[61] Ogonji, M. M., Okeyo, G., & Wafula, J. M. A survey on privacy and security of Internet of Things. *Computer Science Review*, **38,** 100312. https://doi.org/10.1016/j.cosrev.2020.100312 (2020).

[62] Oracle. (n.d.). What is IoT? Available at: https://www.oracle.com/internet-of-things/what-is-iot/ (Accessed: 28 May 2022).

[63] Panchiwala, S., & Shah, M. A comprehensive study on critical security issues and challenges of the IOT World. *Journal of Data, Information and Management*, **2**(4), 257–278, https://doi.org/10.1007/s42488-020-00030-2 (2020).

[64] Patel, H. (2018, June 5). 1. How IoT works? - Harshali Patel - Medium. *Medium*. https://medium.com/@patelharshali136/1-how-iot-works-7ef9b471b8a2 (2018).

[65] Pratomo, A. B. (2023, September 29). *Implementation of Internet of things (IoT) technology in air pollution monitoring in Jakarta: Quantitative analysis of the influence of air quality change and its impact on public health in Jakarta*. https://wsj.westscience-press.com/index.php/wsnt/article/view/225 (2023).

[66] Radwan, T., Azer, M.A. & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. International Journal of Computer Applications in Technology, **55**(2), 158, doi:10.1504/ijcat.2017.082865 (2017).

[67] Rahman, A., & Subriadi, A. P. Software as a Service (SaaS) Adoption Factors: Individual and Organizational Perspective. *2022 2nd International Conference on Information Technology and Education (ICIT&E)*. https://doi.org/10.1109/icite54466.2022.9759891 (2022).

[68] Rajeswari, N. *Overview of Cloud Computing and Its Types*. Available at: https://www.researchgate.net/publication/354683300_OVERVIEW_OF_CLOUD_COMPUTING_AND_ITS_TYPES (Accessed: 27 May 2022) (2019).

[69] Rao, A.R. & Clarke, D. (2020). Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet of Things*, [online] **10,** 100079. doi:10.1016/j.iot.2019.100079 (2020).

[70] Rashid, A., & Chaturvedi, A. Cloud computing characteristics and services a brief review. *International Journal of Computer Sciences and Engineering*, **7**(2), 421–426, https://doi.org/10.26438/ijcse/v7i2.421426 (2019).

[71] Rayapuri, B. A Survey of Security and Privacy in Mobile Cloud Computing. Available at: https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=4427&context=masters_theses (Accessed: 29 May 2022) (2018).

[72] ReadWrite. The Future of Cloud Security: 2022 and Beyond. [online] Available at: https://readwrite.com/the-future-of-cloud-security-2022-and-beyond/ [Accessed 27 May 2022] (2021).

[73] ResearchGate. (n.d.). *(PDF) IoT Security, Privacy, Safety and Ethics*. [online] Available at:https://www.researchgate.net/publication/332859761_IoT_Security_Privacy_Safety_and_Ethics.

[74] Saeed, S., Jhanjhi, N. Z., Naqvi, M., Humayun, M., & Ahmed, S. Ransomware: A Framework for Security Challenges in Internet of Things. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. https://doi.org/10.1109/iccis49240.2020.9257660 (2020).

[75] Sangkaran, T., Abdullah, A., & JhanJhi, N. Z. Criminal network community detection using graphical analytic methods: A survey. EAI Endorsed Transactions on Energy Web, **7**(26), e5-e5 (2020).

[76] Sankar, S. et al. Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. *Transactions on Emerging Telecommunications Technologies*, **32**(8). https://doi.org/10.1002/ett.4171 (2020).

[77] Sathish, K., Vealey, T., Harshit, S. Security in Internet of Things: Challenges, Solutions and Future Directions. Available at: https://www.researchgate.net/publication/301281714_Security_in_Internet_of_Things_Challenges_Solutions_and_Future_Directions (Accessed: 27 May 2022) (2016).

[78] Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. Machine Learning Approaches for Load Balancing in Cloud Computing Services. *2021 National Computing Colleges Conference (NCCC)*. https://doi.org/10.1109/nccc49330.2021.9428825 (2021).

[79] Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. Load balancing techniques in cloud computing environment: A review. *Journal of King Saud University - Computer and Information Sciences*, **34**(7), 3910–3933. https://doi.org/10.1016/j.jksuci.2021.02.007 (2022).

[80] Sharma, M., Gupta, R., & Acharya, P. Adoption and forecasting of technology: modeling the dynamics of cloud adoption using a system approach. *Journal of Enterprise Information Management*. https://doi.org/10.1108/jeim-05-2023-0232 (2023).

[81] *Smart Home Dashboard Sketch Freebie*. (n.d.). https://www.sketchappsources.com/free-source/4387-smart-home-dashboard-sketch-freebie-resource.html

[82] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. A survey on the internet of things (IOT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191–1221, https://doi.org/10.1109/comst.2019.2962586 (2020).

[83] Sumina, V. 26 Cloud Computing Statistics, Facts & Trends for 2022. Available at: https://www.cloudwards.net/cloud-computing-statistics/ (Accessed: 27 May 2022) (2022).

[84] Susilo, B. and Sari, R.F. Intrusion Detection in IoT Networks Using Deep Learning Algorithm. *Information*, [online] **11**(5), 279. doi:10.3390/info11050279 (2020).

[85] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. IOT privacy and security: Challenges and solutions. *Applied Sciences*, **10**(12), 4102. https://doi.org/10.3390/app10124102 (2020).

[86] Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. CloudStrike: Chaos Engineering for Security and resiliency in cloud infrastructure. *IEEE Access*, *8*, 123044–123060. https://doi.org/10.1109/access.2020.3007338 (2020).

[87] Wahab, A., Ahmad, O., Muhammad, M. & Ali, M. A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, **8**(7). doi:10.14569/ijacsa.2017.080768 (2017).

[88] Wojcicki, K., Bieganska, M., Paliwoda B. & Gorna J. *Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review*. Available at: https://www.researchgate.net/publication/358924343_Internet_of_Things_in_Industry_Research_Profiling_Application_Challenges_and_Opportunities-A_Review (Accessed: 29 May 2022) (2022).

[89] Yu, R., Xue, G., Kilari, V.T. and Zhang, X. Deploying Robust Security in Internet of Things. *2018 IEEE Conference on Communications and Network Security (CNS)*. [online] doi:10.1109/cns.2018.8433219 (2018).

[90] Zahra, F. T. et al. Protocol-Specific and sensor Network-Inherited attack detection in IoT using machine learning. *Applied Sciences*, **12**(22), 11598. https://doi.org/10.3390/app122211598 (2022).

[91] Zikria, Y. B., Ali, R., Afzal, M. K., & Kim, S. W. Next-generation internet of things (IOT): Opportunities, challenges, and solutions. *Sensors*, **21**(4), 1174. https://doi.org/10.3390/s21041174 (2021).

[92] Zahra, F. et al. Rank and wormhole attack detection model for RPL-based internet of things using machine learning. Sensors, **22**(18), 6765 (2022).