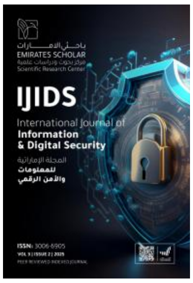

International Journal of Information & Digital Security
Vol 3 Issue 2 (2025)
Pages (4 - 18)

Available at
www.emiratesscholar.com

باحثي الامارات
EMIRATES SCHOLAR
مركز بحوث ودراسات
RESEARCH & STUDIES CENTER

Cyber Threats and Risk Mitigation Strategies for Cloud Systems and the Internet of Things

Driss Abbadi
Public Law, Politics, Economics, and Management Laboratory, Faculty of polydisciplinary, Taza, Sidi Mohamed Ben Abdellah University of Fès, Morocco
drissali@hotmail.fr

ARTICLE HISTORY

Received: 21 November 2025.
Accepted: 10 December 2025.
Published: 26 December 2025.

PEER - REVIEW STATEMENT:

This article was reviewed under a double-blind process by three independent reviewers.

HOW TO CITE

Abbadi , D. . (2025). Cyber Threats and Risk Mitigation Strategies for Cloud Systems and the Internet of Things. *International Journal of Information & Digital Security*, *3*(2), 4-18. https://doi.org/10.54878/fh5j6r80

ABSTRACT

As reliance on cloud computing and the Internet of Things (IoT) continues to grow, so too do the security risks that threaten the integrity of these systems. These systems are exposed to various threats, including cyberattacks targeting data stored in the cloud and attacks on devices connected within IoT environments. This study explores the emerging cybersecurity risks faced by cloud and IoT systems, focusing on effective strategies to mitigate these risks, such as encryption, multi-factor authentication, and continuous monitoring. The paper also examines the challenges of implementing these strategies, including technological complexities, legal concerns, and high costs. Lastly, the study reviews future trends in cloud computing and IoT security, with a particular emphasis on the increasing role of artificial intelligence and distributed computing to strengthen security and safeguard data.

Keywords: *Cybersecurity, cloud computing, Internet of Things, cyber threats, artificial intelligence, distributed computing.*

1. Introduction

The concept of cloud computing emerged in the 1960s, pioneered by John McCarthy, who predicted that computing would eventually be organized as a public utility. Its characteristics were first explored in 1966 by Douglas Parkhill in his book *The Challenge of Computer Utility*. The term 'cloud' itself originated from the field of communications, where telecom companies began offering virtual private network (VPN) services at a lower cost compared to dedicated point-to-point circuits, which were inefficient and wasted bandwidth. By using VPN services, companies were able to optimize network usage through better traffic balancing[1].

Today, cloud computing has expanded into a network of remote servers online for data storage and management, accessible anytime and from anywhere. Its costs are based on the 'pay-as-you-go' model[2]. The cloud offers services such as on-demand data storage and processing, while minimizing costs and reducing dependence on the user's infrastructure[**3**]. Cloud computing relies on models such as "Infrastructure as a Service" (IaaS), "Platform as a Service" (PaaS), and "Software as a Service" (SaaS) [**4**]. According to the National Institute of Standards and Technology (NIST), "cloud computing is a model that enables easy and on-demand access to configurable computing resources with minimal management effort[**5**] ". The institute also defines five key characteristics of cloud computing: on-demand services, resource sharing, broad network access, rapid elasticity, and pay-per-use[**6**].

There are three main cloud deployment models: the public cloud, which provides shared resources for all; the private cloud, which is dedicated to a single organization and offers higher security; and the hybrid cloud, which combines both public and private clouds[2]. In each model, there are five key parties: the Cloud Service Consumer (CSC), who receives the service and pays according to usage; the Cloud Service Provider (CSP), who offers these services; the Cloud Auditor, who evaluates the cloud services, performance, and security of applications; the Cloud Broker, who interacts between the cloud provider and the consumer to facilitate tasks; and finally, the Cloud Carrier, who provides the connectivity between both parties[5].

Cloud computing integrates technologies such as virtualization and distributed computing, enabling the storage of vast amounts of data and helping reduce service costs by sharing resources among users.It also offers benefits such as access anytime and anywhere, and a reduction in the need for infrastructure investment[5]. For these reasons, cloud computing has become an essential part of our daily lives, as we use it for email (like Yahoo and Google), social networks (like Facebook and Twitter), on-demand video services (like Netflix and Hulu), cloud storage (like Dropbox and Google Drive), collaboration tools (like Google Docs), and backup solutions (like Carbonite). Additionally, businesses leverage cloud computing to reduce costs and enhance performance, such as Reddit using Amazon EC2 for service, SmugMug for photo storage via Amazon S3, Mazda USA for advertisements through Rackspace, and HRLocker for HR solutions through Windows Azure[7].

The term "Internet of Things" was coined by Kevin Ashton in 1999 while working at Procter & Gamble[8]. It is a term that is not yet fully settled. The Internet of Things is almost equivalent to what is referred to as the "Internet of Everything" (according to Cisco/W3C), the "Physical Web" (according to Google), "Physical Computing" (according to Arduino), "Machine-to-Machine" (M2M), "Cyber-Physical Systems" (according to control theory terminology), or the "World-Size Web," a term coined by B. Schneier[9]. The Internet of Things is defined as a network of sensors and actuators embedded in physical objects, connected via both wired and wireless networks, and typically linked to the internet using the same Internet Protocol (IP) that connects the web. This concept has gained significant traction in recent years, primarily due to the emergence of cloud computing and big data[8].

Other concepts related to the Internet of Things have emerged, such as the "Internet of Everything" (IoE), which is an extension of IoT encompassing people, processes, data, and things. Another is the

"Internet of Nano Things" (IoNT), where devices communicate on the nanoscale. There is also the "Internet of Mission-Critical Things" (IoMCT), used in critical tasks such as rescue operations and battlefields. Lastly, the "Internet of Mobile Things" (IoMT) refers to communication between devices via sensors embedded in mobile phones[10]. However, the most widely used term remains the Internet of Things (IoT).

Today, IoT has become an integral part of our daily lives[8], aiming to connect "things" to enhance industries, automate processes, and develop services. Its common applications include smart cities, smart homes, remote healthcare, asset tracking, smart grids, and smart agriculture[11]. This technology contributes to cost reduction in fields such as transportation, energy, and education, while supporting the growth of modern industries in automation and artificial intelligence[8].

However, concerns about privacy and security remain the largest barrier to adopting cloud computing and IoT technologies. These two technologies have radically changed how businesses, governments, and consumers interact with data and internet-connected devices. As reliance on these systems increases, so do the risks associated with cyber threats that jeopardize security and data privacy. These risks include data breaches, attacks on connected devices, and insecure applications that can put data at risk. Consequently, the issue addressed in this article involves analyzing emerging threats in cloud computing and IoT environments and presenting effective strategies to mitigate the associated risks.

1.1.Importance of the Topic

As the reliance on cloud computing and the Internet of Things (IoT) continues to grow, so do the security risks that threaten the integrity of these systems. These systems offer numerous benefits, such as flexibility in accessing data and facilitating communication between various devices, but they also expose users and data to a wide range of threats. These threats include cyberattacks targeting data stored in the cloud and attacks on devices connected within IoT environments.

Protecting data and ensuring the security of cloud and IoT systems require effective strategies, such as encryption, multi-factor authentication, and continuous monitoring. However, these strategies are not without challenges, including technological complexities, legal concerns, and the high costs associated with their implementation.

The importance of this study increases as organizations and individuals continue to rely on these complex systems, making it essential to explore innovative and effective solutions to secure this digital environment. It also highlights future trends in cloud computing and IoT security, with a focus on the growing role of distributed computing in enhancing security and safeguarding data

1.2. Research Problem

As reliance on cloud computing and the Internet of Things (IoT) continues to grow, a range of security risks emerge that threaten the integrity of these systems. Despite the significant benefits offered by these technologies, such as ease of access to data and improved device communication efficiency, cloud systems and IoT devices are increasingly vulnerable to cyberattacks that could lead to data breaches or disruption of critical operations.

One of the key challenges facing these systems is how to protect the data stored in the cloud and ensure the security of devices connected within IoT environments. There is an urgent need to develop effective strategies to combat various threats, such as cyberattacks, breaches, and malware, in addition to challenges in implementing security technologies such as encryption, multi-factor authentication, and continuous monitoring.

The research problem lies in clearly identifying these security risks and understanding how they impact cloud computing and IoT systems, while exploring the best strategies and technologies to address these threats effectively. The study also aims to derive future trends in security for these systems.

1.3. Research Questions

-What are the main security risks currently threatening cloud computing and Internet of Things (IoT) systems?

-How do cyberattacks impact data stored in the cloud and devices connected within IoT environments?

-What effective strategies can be implemented to protect data and ensure the security of cloud systems and IoT devices?

-What are the future trends in cloud computing and IoT security, and how can security be enhanced using advanced technologies like distributed computing?

1.4. Objectives of the Study

The aim of this study is to identify and analyze the primary security risks threatening cloud computing and Internet of Things (IoT) systems, and to understand the impact of cyberattacks on data stored in the cloud and devices connected within IoT environments. The study also seeks to explore effective strategies for protecting data and ensuring the security of cloud systems and IoT devices, while evaluating the technological, legal, and financial challenges associated with implementing these strategies. Additionally, the study aims to analyze future trends in cloud computing and IoT security, with a focus on providing best practices for implementing security strategies in cloud systems and IoT devices across various industrial and commercial sectors.

1.5. Methodology of the Study

This study will adopt a descriptive-analytical approach to examine the security risks threatening cloud computing and Internet of Things (IoT) systems. It will focus on the importance of developing innovative security strategies that leverage modern technologies such as encryption and multi-factor authentication to enhance security in these systems, enabling them to effectively combat emerging cyber threats. The study will use both theoretical and practical analysis through a literature review, as well as gathering data from cybersecurity experts through surveys and interviews.

1.6. Research Framework

This study on "Cyber Threats and Risk Mitigation Strategies for Cloud Systems and the Internet of Things" is divided into two main sections:

The first section focuses on the cybersecurity threats faced by cloud computing and IoT systems in the context of modern technological trends. This section reviews the latest developments in cloud computing and IoT, identifying key security risks such as data breaches, cyberattacks targeting sensitive data, and unauthorized access to connected devices. It also discusses vulnerabilities in cloud infrastructure and IoT environments that could be exploited by attackers, along with the potential consequences of these risks on privacy, data integrity, and public safety.

The second section addresses strategies for mitigating these cybersecurity risks in cloud and IoT systems. This section explores innovative technical solutions aimed at enhancing the security of these technologies, including the use of encryption, multi-factor authentication, and real-time monitoring systems.

2. Cybersecurity Threats in Cloud Systems and the Internet of Things

With the increasing reliance on modern technologies like cloud computing and the Internet of Things (IoT), cybersecurity threats have become an escalating concern. These systems, which significantly contribute to enhancing business efficiency and services, also open the door to a wide range of security risks that threaten data privacy and the safety of connected devices. In this context, it is important to study the cybersecurity threats associated with these systems and understand how to effectively counter them.

2.1. Cybersecurity Threats in Cloud Systems

In recent years, the number of people using cloud services has significantly increased, with vast amounts of data being stored in cloud computing environments. As a result, data breaches in cloud services have risen annually, as hackers constantly seek to exploit vulnerabilities in cloud infrastructure. In this research, we analyze actual attacks on the cloud to review the methods used by hackers against cloud computing systems and ways to prevent these malicious activities**[3]**. The main cybersecurity threats in cloud computing are:

2.1.1. Breaches: These are among the most significant threats facing cloud systems, as they can lead to data leaks or unauthorized access to sensitive information. The low cost of cloud computing services has drastically changed our daily lives; most mobile companies now offer free cloud services for a limited time. However, the security issues related to these services make us vulnerable to cyberattacks. Hackers use various techniques to breach cloud systems and gain illegal access to the data stored within, exposing sensitive information to theft for criminal purposes**[3]**. According to DataLossDB, 1,047 data breaches were recorded in 2012, compared to 1,041 breaches in the previous year, including incidents like the Epsilon data leak and the theft of information from Stratfor. Hackers may also exploit the massive computing power of the cloud to launch attacks on other networks, as seen in the attack on the PlayStation network using Amazon EC2 servers. Therefore, it is crucial to understand cloud security threats in order to provide more secure services for users**[7].**

2.1.2.Cyberattacks on Application Programming Interfaces (APIs): APIs represent a major vulnerability that attackers can exploit to access data stored in the cloud. API traffic is among the most active on the internet today**[12]**, with over 22,000 searchable APIs on ProgrammableWeb. These interfaces provide a link between connected systems and are faster and more powerful compared to traditional models. However, they are also more difficult to protect, which increases the security risks for organizations**[13].**

Reports indicate a 400% increase in attacks on APIs, leading to sensitive data leaks and significant financial losses. According to a Salt Security report, 31% of customers experienced data breaches in Q1 of 2023 due to vulnerabilities in APIs. It is expected that U.S. companies will incur losses ranging from $12 billion to $23 billion as a result of these breaches, while many organizations are still unaware of the number of APIs or security vulnerabilities they contain**[14].**

APIs are susceptible to their own unique risks and are prime targets for attackers due to their open nature to the public or third parties. While cybersecurity aims to reduce the attack surface of a network, APIs, by their nature, significantly increase this surface if not carefully designed. From an attacker's perspective, APIs are an easier target because they directly expose numerous points that can be exploited, reducing the time needed to discover vulnerabilities within the network. The increasing use of microservices architectures, as opposed to monolithic structures, is a key factor in the intensified reliance on APIs, which necessitates more stringent practices to maintain network security according to the 'zero trust' principle**[12]**.

The risks associated with APIs include a range of security vulnerabilities such as broken authorization, weak authentication, insecure network connections, insufficient training for development teams, and various issues regarding access control and permissions. Among these vulnerabilities, the Broken Object Level Authorization (BOLA) flaw stands out, which allows unauthorized users to access sensitive objects and data, posing a significant threat to system integrity. Additionally, poor API inventory management can lead to the leakage of outdated or unprotected data, making it easier for attackers to breach it. Other threats to APIs include issues like attacks related to broken authentication or unrestricted resource consumption, which may cause service outages or severe damage to the infrastructure**[12]**.

Although some of these risks can be mitigated through continuous security patches and specialized training, research indicates that designing APIs carefully and thoughtfully is the primary step to reduce security threats and enhance protection against the increasing number of attacks**[12]**.

2.1.3. Data Threats: Data is considered a vital asset in any business, and its leakage or corruption can lead to a loss of trust in the company and the collapse of its operations. With the increasing reliance on cloud computing in various business sectors, protecting data in the cloud environment has become critically important. Data in the cloud faces security threats throughout its lifecycle, from creation and storage to use, sharing, archiving, and destruction. During the storage and archiving phase, known as static data, it may be more vulnerable to breaches, while during the transit phase, or data in motion, it is exposed to eavesdropping and attacks as it travels over the internet**[5].**

This highlights the importance of using techniques like encryption to ensure data confidentiality and protect it from risks during transit across networks. Furthermore, the core principles of security in cloud computing, such as confidentiality, integrity, and availability (the CIA triangle), are essential factors that contribute to protecting data from unauthorized access, tampering, and ensuring its availability without disruption. Authentication, authorization, and non-repudiation are key aspects of access control, ensuring that only authorized individuals can access data and perform associated actions**[5]**..

In the cloud computing environment, data is stored on infrastructure owned by the cloud service provider, exposing it to additional threats compared to enterprise systems that store data in a controlled, on-premises environment. This is especially true for public clouds, which rely on the internet and are more exposed to risks due to their openness. According to the shared responsibility model, the cloud service provider is responsible for securing the infrastructure, while businesses are responsible for securing their data and ensuring its confidentiality and integrity of access **[5].**

2.1.4. Security Challenges in Authentication and Access Control (AAC): Authentication and access control (AAC) is the process of verifying a user's identity to ensure secure access to cloud resources. In enterprise computing, credentials are typically stored on servers like Active Directory (AD) or Lightweight Directory Access Protocol (LDAP). In a private cloud, authentication is implemented similarly using a Virtual Private Network (VPN), while in a public cloud, the connection relies on the internet, exposing authentication to greater security vulnerabilities due to the aggregation of resources and the use of multiple devices by different users**[5].**

Password-based authentication alone does not provide sufficient security in a public cloud, as it can be compromised through attacks such as brute force, dictionary attacks, or phishing. Therefore, cloud service providers (CSPs) should adopt more secure authentication methods, such as tokens instead of passwords. Additionally, authentication in the cloud is not limited to users alone but also extends to machines that need authorization to perform operations like backups, system patching, and updates. Since cloud applications are accessed via multiple devices, it is crucial to use robust authentication methods such as RSA tokens, one-time passwords, or biometric recognition to ensure the authenticity of the identity and make effective risk-based decisions for access management**[5].**

2.1.5. Denial of Service Attacks: The cloud computing model offers on-demand, fully managed, and flexible computing resources and systems to organizations. However, attacks on cloud components can result in immense losses due to their value for both cloud service providers and their users. One category of attacks is Distributed Denial of Service (DDoS) attacks, which can have severe consequences including degraded customer experience, service interruptions, and, in extreme cases, complete service shutdowns and widespread economic failure. Developments in the Internet of Things (IoT) and network connectivity have facilitated the execution of DDoS attacks, which have grown in size, frequency, and intensity**[6]**

2.2. Cybersecurity Threats in the Internet of Things (IoT): The Internet of Things (IoT) is witnessing significant development in connectivity between various devices, ranging from household appliances to industrial sensors, which is transforming the way we live and work**[15]**. Every country has critical infrastructure that provides essential services such as communications, energy, banking, transportation, and water management, with strategies for managing these infrastructures differing across sectors. As reliance on IoT solutions increases, these infrastructures are being connected to the internet**[16]**. With the growth in the number of these infrastructures, malicious entities seeking to exploit vulnerabilities to threaten our interconnected lives have also increased**[15]**. The adoption and implementation of IoT pose risks to personal security, safety, and privacy, making cybercrimes easier on a large scale and leading to threats such as Distributed Denial of Service (DDoS) attacks that threaten the underlying internet infrastructure**[17]**. Cybercrime can exploit IoT technology to endanger human life, as IoT devices generate vast amounts of data that need to be responsibly processed to maintain integrity and security. Consequently, both devices and their data become susceptible to cybercrimes at every layer of the IoT**[17]**.

Risks are being introduced into industrial sectors such as transportation, energy, and manufacturing, with the emergence of new attack surfaces and an increased likelihood of damage. Furthermore, the risks and damages resulting from the Industrial Internet of Things (IIoT) can spread across organizations and interconnected sectors, leading to systemic risks. Aspects of this shift in the risk landscape are not addressed by current cybersecurity approaches, leaving gaps in security capabilities**[18].**

Security poses a major challenge in the Internet of Things, as devices are often unprotected, making them vulnerable to attacks. In the future, sectors like healthcare and daily life will heavily rely on sensors, making tampering with them a direct threat to human life, such as disabling pacemakers or causing car accidents. Additionally, eavesdropping on IoT data could lead to blackmail or leaking sensitive information**[11].**

Cyberattacks can threaten the security function of a device or control system in several ways, such as disabling it when needed or hijacking it to appear as though it is functioning correctly while it is actually compromised. Manipulating the system can generate false alarms or improperly activate safety functions, leading to equipment damage or endangering lives. Even if the device is still operational, it may become inaccessible or trigger alarms requiring maintenance**[19].**

The threats associated with Internet of Things (IoT) devices are numerous, including unauthorized access due to weak authentication mechanisms or the absence of secure access controls, which allows attackers to breach devices. Data breaches also emerge as a problem due to inadequate encryption and insecure data storage, exposing sensitive information to risks. Additionally, devices can be compromised by malware that turns them into botnets for launching DDoS attacks. Physical attacks, such as tampering or theft, also threaten the integrity of the devices. Other threats include supply chain vulnerabilities such as counterfeit components or tampered firmware, along with privacy issues related to the collection of personal data**[15].**

At the device level, vulnerabilities may include insecure software, weak authentication, and lack of encryption, while network-related vulnerabilities involve improper segmentation and unencrypted data transmission. Regarding cloud systems, insecure APIs or weak data security in storage could put the system at risk. Finally, human factors like poor user habits, such as using weak passwords or failing to regularly update devices, make them more susceptible to attacks**[15].**

Cyberattacks on IoT systems and critical infrastructures vary and involve several advanced threat techniques. Prominent attacks include the injection of malicious software such as viruses and ransomware (e.g., WannaCry), phishing aimed at obtaining sensitive data from victims via untrusted sources, with spear-phishing being the most common in critical infrastructures. Hacking is carried out using techniques like brute force attacks and Man-in-the-Middle (MITM) attacks. DDoS attacks target networks by excessively increasing traffic, while SQL injection attacks focus on stealing or modifying data from databases. Physical attacks involve direct tampering with devices, and Advanced Persistent Threats (APTs) involve covert network intrusions that progress through stages such as initial penetration, establishing a foothold, privilege escalation, internal reconnaissance, lateral movement, and maintaining persistence within the system. As the number of connected devices grows, security vulnerabilities increase, making critical infrastructures more vulnerable to attacks aimed at obtaining ransom or stealing sensitive data**[16].**

Although cloud computing has well-known characteristics, its security state remains complex and must be appropriately addressed in order for businesses to benefit from cloud services more efficiently**[20].**

3. Cybersecurity Risk Mitigation Strategies in Cloud and the Internet of Things

The importance of cloud computing and Internet of Things (IoT) technologies is rapidly increasing in our contemporary world, as they form the foundation for many vital sectors such as healthcare, transportation, and energy, enhancing connectivity and integration between devices and networks. With the expansion of the use of these technologies, cybersecurity threats emerge as one of the greatest challenges that could threaten data security and system integrity. The risks associated with cyberattacks, whether through malware injection, phishing, or advanced persistent attacks, require effective strategies to mitigate their impacts and protect critical infrastructures. In this section, we will discuss the key cybersecurity risk mitigation strategies for cloud computing and IoT, focusing on the importance of adopting advanced security solutions that keep pace with the evolution of these technologies and ensure the security and protection of data from potential threats.

3.1. Sustainable Security Strategies for Cloud Systems

Although cloud computing continues to grow in popularity, usability, and acceptance, issues related to data protection, data privacy, and other security concerns pose a significant barrier in the field of cloud computing**[4]**. Therefore, it has become essential for companies to adopt comprehensive and clear security policies that include data classification and the identification of sensitive data, along with creating policies for access, archiving, and destruction. Identity and Access Management (IAM) also plays an important role in protecting data integrity and reducing security risks. Ultimately, while cloud computing provides flexibility and high availability of infrastructure, it requires the implementation of integrated security measures to ensure the protection of data from potential security threats that may affect business operations**[5]**.

Securing cloud services has become essential due to the high demand for cloud services given their various applications. It has been observed that the security factor in cloud computing is the most important element, as it significantly impacts cloud operations. Cloud computing security strategies include formal, informal, and technical strategies. These strategies include confidentiality, integrity, availability, privacy, compliance, trust, incident response, governance, and security awareness strategies**[21].**

This strategy is implemented through techniques, the most notable of which are:

3.1.1. Encryption: Encryption algorithms are considered the most common solution used to ensure data security in cloud computing. One of the challenges related to encryption in cloud computing is key security; this method prevents encrypted data from being compromised and ensures that only authorized users can access the keys. Rivest et al. proposed a practical public key system called RSA. This algorithm uses two keys:

the public key, which is used to encrypt plaintext published to the public, and the private key, which is used to decrypt the encrypted text and is known only to the data owner. The RSA encryption algorithm has been widely used to ensure privacy and maintain the confidentiality of data. Despite this usage, many attacks make the use of this algorithm ineffective, particularly when the factor is used below the required level. This allows numerical analysis attacks to achieve their results efficiently, affecting the performance of this algorithm**[22]**.

3.1.2. Multi-Factor Authentication (MFA): Multi-factor authentication (MFA) is a security procedure that uses additional layers to verify the user's identity and enhance data security beyond the traditional username and password. MFA relies on requiring two or more methods of verification, such as something the user knows (password), something the user has (like a bank card or mobile device), and something that is the user (such as biometric data like fingerprints). With these multiple layers, it becomes difficult for hackers to access accounts even if they obtain the traditional login details, as more data is required that only the user possesses. Thus, MFA provides an effective and fast way to enhance account security without burdening the user with remembering more information**[23].**

Multi-factor authentication (MFA) relies on three main types of factors to enhance security: knowledge factors, possession factors, and inherence factors. Knowledge factors include what the user knows, such as passwords, PINs, and security questions. Possession factors rely on something the user owns, such as connected or standalone tokens, which can be used for authentication by simply presenting the token. Inherence factors are related to the user's own characteristics, such as fingerprints, facial recognition, and retina scans, which are biometric methods that do not require the user to remember or carry something but simply interact with the device. By combining these different types of factors, the security level is significantly increased, as each additional factor strengthens the verification capability in protecting accounts and data from attackers**[23].**

3.1.3. Continuous Monitoring: Continuous monitoring tools and analysis are essential for the early detection of threats and providing effective protection against cyberattacks. One of the most prominent of these tools is the Intrusion Detection System (IDS), which works by monitoring events occurring in the network or system and analyzing them to detect any abnormal activity that may indicate an attack or security breach. These systems detect potential violations that may breach security policies or involve the illegal use of the system. Additionally, systems such as the Intrusion Prevention System (IPS) and Security Information and Event Management (SIEM) systems are used in continuous security monitoring, providing comprehensive information and detailed analytics of system performance. These tools rely on advanced techniques to detect suspicious patterns and interactions that could represent a threat, helping to take proactive measures to prevent attacks before they escalate**[24].**

The Intrusion Detection System (IDS) is used to monitor suspicious activities and traffic in the network, analyzing logs to detect threats or abnormal activities and alerting the network administrator when any threat is detected. IDS is divided into two types: Host-based IDS (HIDS), which is deployed on a single device to monitor local activities, and Network-based IDS (NIDS), which monitors activities across the network. IDS can also be classified into two types based on the detection method: signature-based detection, which relies on matching known attack patterns, and anomaly-based detection, which detects threats by identifying deviations from normal activity patterns**[25].**

The Intrusion Prevention System (IPS) is a security system used to monitor the network and detect abnormal activities, preventing them from reaching the network by taking defensive actions such as reporting, blocking, or quarantining the activities. IPS is divided into two types: Network-based IPS (NIPS), which monitors network traffic, and Host-based IPS (HIPS), which monitors personal computer traffic. IPS relies on various techniques to detect threats, such as signature-based analysis, which compares traffic with known attack signatures, and anomaly-based analysis, which detects suspicious activities by comparing actual activity with normal behavior**[25].**

While an Intrusion Detection System (IDS) is a program that automates the detection of intrusions, the Intrusion Prevention System (IPS) is a program that includes all the capabilities of an IDS and can also attempt to stop potential incidents**[24].**

3.1.4. Data Partitioning Across Different Providers: Distributed data processing in the cloud is a vital method for effectively managing and analyzing large volumes of data, where complex tasks are broken down into smaller parts to be processed in parallel across a network of cloud servers. This helps optimize resource usage and reduce processing time. Distributed data processing involves several strategies for scalable data partitioning, such as**:[26]**

-Hash-Based Partitioning: This method distributes data based on a pre-defined hash key, ensuring a balanced load distribution;

-Range-Based Partitioning: Data is divided based on specific categories, such as predefined time periods, making it suitable for searching across certain ranges;

-Key-Based Partitioning: This partitions data based on the properties of data keys, useful when access to data requires examining specific attributes;

-Dynamic Partitioning: This method allows adjustments in partitions based on changes in load, data distribution, or resource availability, offering flexibility to adapt to changing needs;

-Content-Based Partitioning: Data is distributed based on its content, which helps accelerate the retrieval of similar data. This is commonly used in distributed file systems and search engines.

To mitigate security challenges related to Policy-Based Access Control (AAC), several effective approaches can be followed, such as implementing a unified access policy wherever possible, and using multi-factor authentication to manage identity and access efficiently. Additionally, biometric authentication, which is more secure than single sign-on, can be adopted. Furthermore, the RSA encryption system can be utilized to support various authentication models such as two-factor authentication and adaptive authentication. Implementing Intrusion Detection Systems (IDS) and firewalls, along with network segmentation and cloud layers, also contributes to enhancing data protection. Third-party identity management solutions such as "Azure Active Directory," "Okta," and "McAfee Cloud Identity Manager" provide robust options for securing access. Finally, using open standards like SAML and OAuth for exchanging authentication and authorization data between different systems is recommended**[5]**.

3.1.5. Firewalls and Network Segmentation: Firewalls simply act as gatekeepers for network traffic. They evaluate data packets sent across the network based on predefined security rules to determine which packets are safe and which may pose potential threats. When a data packet is considered harmful, the firewall blocks its passage, protecting the network from potential damage. In the context of Internet of Things (IoT) devices, firewalls play a critical role. As demonstrated in our tests, these devices can be vulnerable to attacks such as Denial of Service (DoS) attacks, where an attacker floods the device with unnecessary requests, making it unresponsive. In such cases, firewalls are an effective tool for mitigating threats. By detecting abnormal data flows, a firewall can block the attacker's IP address, preventing further requests from reaching the targeted device and protecting it from a potential DoS attack**[27].**

DDoS Attacks are considered criminal offenses in many countries around the world, with these attacks carrying legal liability both at the criminal and civil levels, potentially leading to fines or imprisonment. Under laws like the U.S. Computer Fraud and Abuse Act, a DDoS attack is a federal crime, with penalties that could include several years of imprisonment. Countries like the UK, Germany, and France have stringent laws against these attacks, imposing severe penalties on those involved. For example, in Germany, penalties can reach up to 10 years in prison, while in the UK, the penalties may reach 12 months and up to 10 years in certain cases. Other countries like China, Australia, South Africa, and Brazil treat these crimes similarly, with attackers facing prison sentences ranging from 5 to 10 years. Many countries also adopt additional legislation like the Budapest Convention, which provides a legal framework to deal with cybercrimes at the international level. With the increasing threat of DDoS attacks, more countries are expected to adopt stricter laws and penalties to combat these crimes and protect cybersecurity**[6].**

3.2. Sustainable Security Strategies for IoT Systems

Cyberattacks on the Internet of Things (IoT) and Industrial Internet of Things (IIoT) have increased, making it essential to implement robust cybersecurity protocols to support functional safety and protect safety-related solutions in buildings and industrial processes. With the growing reliance on automation and network connectivity of devices, the security risks associated with internet connectivity have become a top priority for stakeholders such as product designers, building managers, and owners. To ensure functional safety, it is crucial to ensure that devices and systems responding to operator inputs operate correctly, as any inaccurate response could pose a risk. To mitigate these risks, it is necessary to expand the design and testing lifecycle of systems to include cybersecurity assessments, ensuring that all IoT and IIoT devices and systems are designed and tested according to recognized cybersecurity standards**[19].**

There are various methods to mitigate the effects of cyberattacks on critical infrastructure dependent on IoT. These methods include several technologies to reduce risks and enhance security**[16]**. Some of the most important strategies are: **access control**, which determines who can access resources and data, **encryption** to protect data traffic from attackers, and **authentication** to ensure that devices only respond to authorized commands. These authentication systems, based on passwords, rely on techniques such as encryption using public keys, zero-knowledge protocols, and isolation through sandboxing to reduce vulnerabilities**[28].**

Regular remote security updates are also crucial to update systems and protect them from security vulnerabilities. Physical security of devices must also be ensured to prevent tampering and unauthorized access, and any backdoors that attackers might exploit should be avoided. For mass-produced devices, it is preferable to use unique login credentials rather than default passwords to reduce the chances of hacking. These combined measures contribute to protecting devices and networks from increasing threats**[16].**

There are also other measures that limit cyberattacks on devices, such as:

3.2.1. Quick IP Address Switching: If Denial of Service (DoS) attacks are among the major threats facing IoT systems, techniques such as quick IP address switching provide an effective means of mitigating these attacks. By changing the IP addresses of servers and clients in real-time, the server's destination is hidden, making it more difficult for attackers to identify their targets. Automatic IP address switching relies on "Moving Target Defenses" (MTD) technology, which randomly changes network properties, preventing attackers from creating a fixed list of targets. Research has shown that this technique is effective in countering scanning attacks, which usually precede DDoS and other network attacks. By making the targets invalid within a short time frame, it disrupts malicious attempts by attackers**[29].**

3.2.2. Intrusion Detection Systems (IDS): Designing a robust, lightweight, and high-performance Intrusion Detection System (IDS) is an effective solution for ensuring the security of IoT environments**[16].**

Intrusion Detection Systems (IDS) are software or hardware systems that monitor and analyze events in a network or system to detect intrusion attempts, such as breaches of confidentiality, integrity of the system, or bypassing security mechanisms. With the rise of network attacks, these systems have become essential for the security infrastructure of organizations, as intrusions occur due to attacks from the internet or attempts by authorized users to gain unauthorized privileges[30]. IDS are crucial for detecting attacks after the attacker has infiltrated the system. IDS techniques vary into four main types: **signature-based IDS**, which compares threats with stored signatures in a database but may fail to detect new attacks; **anomaly-based IDS**, which uses machine learning techniques to detect unknown attacks but may generate false alarms; **host-based IDS**, which monitors malicious activities on the host device but is limited to detecting activities within that device only; and finally, **stack-based IDS**, which monitors data packets before they reach higher layers based on the OSI layer model, providing early protection before the data is processed by applications or operating systems[16].

In IoT environments, Intrusion Detection and Prevention Systems (IDS/IPS) can offer effective protection against cyberattacks, such as the **ARP spoofing attack**. In this attack, the attacker associates their MAC address with the IP address of a legitimate user on the network. By monitoring ARP traffic, an IDS/IPS system can detect abnormal patterns between IP and MAC addresses, indicating a spoofing attack. Upon detection, the IPS system can block or isolate the malicious traffic, restricting the intrusion and protecting the network from threats[27].

4. Conclusion

In conclusion, cybersecurity threats in cloud and IoT systems remain some of the most significant challenges faced by organizations in the digital age, with risks continuously increasing as reliance on these technologies grows across various sectors. Addressing these threats requires advanced risk mitigation strategies, including the use of modern security tools, as well as raising security awareness and training employees. Despite significant progress in protective strategies, security vulnerabilities persist, prompting companies to intensify efforts in updating security solutions and increasing investments in this area.

As risks continue to grow, it is essential to adopt new concepts in cybersecurity, such as adopting a holistic security approach across all systems and connected devices. This also requires considering new topics, such as security in quantum computing environments and the impact of next-generation AI technologies on network security. The future holds numerous challenges and opportunities, requiring organizations to remain in a constant state of readiness to adapt to ever-evolving threats.

5. Recommendations

Here are some important recommendations to counter cyber threats and enhance the security of cloud and IoT systems:

-Invest in Security Training and Awareness: Organizations should invest in training employees on the latest cybersecurity practices and how to identify potential attacks. Security awareness within the organization is one of the key foundations for combating cyberattacks.

-Enhance Encryption and Data Protection: Organizations should adopt advanced encryption techniques to protect data during transmission and while at rest. It is also essential to ensure that all devices connected to the network use strong encryption protocols to prevent information leakage.

-Adopt a Multi-Layered Security Approach: Organizations should implement multi-layered security strategies, including intrusion detection systems (IDS) and advanced anti-malware systems, in addition to firewalls, to provide multiple defenses against attacks.

-Regularly Update Systems: Companies should regularly update software systems and connected devices to ensure protection from security vulnerabilities. Continuous updates play a critical role in addressing new security gaps.

-Regularly Review and Assess Risks: Organizations must regularly assess risks through security audits and penetration testing to identify vulnerabilities and potential issues. This contributes to enhancing the organization's preparedness against future attacks.

-Leverage Artificial Intelligence: Using artificial intelligence and big data analytics can significantly enhance an organization's ability to detect attacks and analyze suspicious behaviors in real-time, leading to quicker and more effective responses.

-Adopt Secure Cloud Solutions: Cloud service providers should be selected based on their adherence to the highest cybersecurity standards, such as end-to-end encryption, and compliance with globally recognized security laws and regulations.

-Improve Identity and Access Management: It is crucial for companies to use identity and access management solutions to ensure that each device or user only receives the permissions necessary for their role. Implementing methods such as Multi-Factor Authentication (MFA) will contribute to enhanced security.

-Enhance Physical Security of Devices: Since IoT devices can be vulnerable to breaches if physically accessed, it is important to secure devices well and equip them with tamper-resistant mechanisms.

-Continuous Monitoring and Data Analysis: It is crucial to continuously monitor data and activities within systems using advanced analysis tools to ensure early threat detection and prevent attacks before they have a significant impact on the system.

References

[1]-Bang A, Bairagi SWI. Cloud computing: History, architecture, security issues. Int J Advent Res Comput Electron. 2015 Mar 28;Special Issue National Conference "CONVERGENCE 2015":103. Available from: https://tinyurl.com/bd2z96cf.

[2]-Suganya M, Sasi Prabha T. A comprehensive analysis of data breaches and data security challenges in cloud environment. SSRN. 2022 May 18. Available from: https://tinyurl.com/2d6hznpm.

[3]-Mozumder DP, et al. Cloud computing security breaches and threats analysis. Int J Sci Eng Res. 2017 Jul;8(1):1287. Available from: https://tinyurl.com/4m2pp7ru.

[4]-Nandgaonkar A, Kulkarni P. Encryption algorithm for cloud computing. Int J Comput Sci Inf Technol. 2016;7(2):983-9. Available from: https://tinyurl.com/yckbjn8s.

[5]-Kumar R. Exploring data security issues and solutions in cloud computing. Procedia Comput Sci. 2018;125:691-7. Available from: doi:10.1016/j.procs.2017.12.089.

[6]-Bhardwaj A, et al. Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Comput Sci Rev. 2021 Feb;100033:1. Available from: doi:10.1016/j.cosrev.2020.100332.

[7]-Chou TS. Security threats on cloud computing vulnerabilities. Int J Comput Sci Inf Technol. 2013 Jun;5(3):79-80. Available from: doi:10.5121/ijcsit.2013.5306.

[8]-Duncan B, Whittington M. Cyber security for the cloud and the Internet of Things: How can it be achieved? Eng Technol Ref. 2017 Jun;1:10.1049/etr.2017.0001. Available from: https://doi.org/10.1049/etr.2017.0001.

[9]-Baccell E. Internet of Things (IoT) societal challenges & scientific research fields for IoT. Inria; November 2021. p. 11. Available from: https://tinyurl.com/bhderjk5.

[10]-Bodduna R, et al. A review on the different types of Internet of Things (IoT). J Adv Res Dyn Control Syst. 2019 Jan;11(1):154. Available from: https://tinyurl.com/2p88mdr9.

[11]-De Donno M, et al. Sustainable security for Internet of Things. In: Proceedings of the 2019 International Conference on Smart Applications, Communications and Networking (SmartNets); 2019; p. 1. Available from: doi: 10.1109/SmartNets48225.2019.9069776.

[12]-McKinley Sconiers-Hasan. Application Programming Interface (API) Vulnerabilities and Risks. Carnegie Mellon University; June 2024. Available from: https://doi:10.1184/R1/25282342.

[13]-Giese G. Think like a hacker: reducing cyber security risk by improving API design and protection. Cyber Security: A Peer-Reviewed Journal. 2020;4(1):48-57. Available from: https://tinyurl.com/j5anv8yy.

[14]-Qazi FA. Application Programming Interface (API) Security in Cloud Applications. EAI Endorsed Transactions on Cloud Systems. 2023 Oct 17;7(23):1-2. Available from: https://doi:10.4108/eetcs.v7i23.3011.

[15]-Dheeneswaran D, Thara L. Cybersecurity threats in the Internet of Things (IoT): A comprehensive analysis. Int Res J Modernization Eng Technol Sci. 2023 Sep 9;1776. Available from: https://tinyurl.com/299nu9cd.

[16]-Daş R, Gündüz MZ. Analysis of Cyber-Attacks in IoT-based Critical Infrastructures. Int J Inf Secur Sci. 2019 Dec 26;122. Available from: https://tinyurl.com/2k26a2sx.

[17]-Rana P, Patil BP. Cyber security threats in IoT: A review. J High Speed Networks. 2023;29:109-111. Available from: https://doi:10.3233/JHS-222042.

[18]-Axon L, et al. Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda. Digit Threats Res Pract. 2022 Dec 5;3(4):34. Available from: https://doi.org/10.1145/3503920.

[20]-Safhi A, et al. Major Security Threats and Attacks that Facing Cloud Computing with the Main Defence Strategies. Commun Math Appl. 2022;13(1):315-329. Available from: doi:10.26713/cma.v13i1.1973.

[21]-Olushola OB. Strategies for Securing Cloud Services. IOSR J Comput Eng (IOSR-JCE). 2019 Dec 31;22(1):13. Available from: doi:10.9790/0661-2201031319.

[22]- Ghassan Sabeeh Mahmood, et al. A secure cloud computing system by using encryption and access control model. J Inf Process Syst. 2019 Jun;15(3):538-49. doi: 10.3745/JIPS.03.0117. Available from: https://doi.org/10.3745/JIPS.03.0117. p. 542.

[23]- Williamson J, Curran K. The role of multi-factor authentication for modern day security. Semiconductor Sci Inf Devices. 2021 Apr;3(1):16. Available from: doi: https://doi.org/10.30564/ssid.v3i1.3152.

[24]-Azhagiri M, et al. Intrusion detection and prevention system: Technologies and challenges. Int J Appl Eng Res. 2015;10(87):1. Available from: https://tinyurl.com/mrya8zak.

[25]-Younus ZS, Alanezi M. A survey on network security monitoring: Tools and functionalities. Mustansiriyah J Pure Appl Sci. 2023;1(2):60. doi: 10.47831/mjpas.v1i2.33. Available from: https://doi.org/10.47831/mjpas.v1i2.33.

[26]-Ponnusamy S, Gupta P. Scalable data partitioning techniques for distributed data processing in cloud environments: A review. IEEE Access. 2017;1-2. doi: 10.1109/ACCESS.2024.3365810. Available from: https://doi.org/10.1109/ACCESS.2024.3365810.

[27]-Demolinis R. Impact and mitigation of cyberattacks on IoT devices: A lens on smart home. Master of Science Thesis, University of Turku, Department of Computing; 2023 Aug. p. 83. Available from: https://tinyurl.com/2vmf5avt.

[28]-Jyotiyana JP, Mishra A. Secure authentication: Eliminating possible backdoors in client-server endorsement. Procedia Comput Sci. 2016;85:607. doi: 10.1016/j.procs.2016.05.227. Available from: https://doi.org/10.1016/j.procs.2016.05.227.

[29]-Xu X, et al. An adaptive IP hopping approach for moving target defense using a light-weight CNN detector. Security and Communication Networks. 2021;1. doi: 10.1155/2021/8848473.

Available from: https://doi.org/10.1155/2021/8848473.

[30]-Bace R, Mell P. Intrusion detection systems. National Institute of Standards and Technology; 2001. p. 5. Available from: https://tinyurl.com/3mc2c2px.