International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V71I4P106

Volume 71 Issue 4, 37-52, April 2023

Original Article

Security Challenges and Opportunities in IoT-Driven Cloud Computing: An In-Depth Review

Dilip Narayanan Ravindran

Infrastructure Security, Coinbase, US.

Received: 28 February 2023 Revised: 03 April 2023 Accepted: 14 April 2023 Published: 28 April 2023

Abstract *- The most economical, commercial, cultural, social, and governmental activities occur in cyberspace in today's digitally connected world. Yet, increased reliance on electronic technology exposes businesses to cyber threats that could harm their finances, military capabilities, or political standing. Despite numerous solutions being put forth to stop or lessen these attacks, researchers are still looking at the problems, benefits, and limitations of current techniques. The extensive use of cloud computing in industrial settings has brought about several positive effects. However, it has also generated security problems that conventional solutions might not be able to address adequately. Recent studies have concentrated on using artificial intelligence's deep learning to enhance security controls for cloud-based IoT devices to overcome these problems. This in-depth study examines the most recent developments in cloud-based IoT frameworks, applications, configurations, and security architectures and the division of cloud security problems into four groups. The paper outlines potential areas for future research for integrating cybersecurity in the cloud by outlining research gaps in IoT-based cloud infrastructure, discussing major security vulnerabilities in each domain, and presenting their limitations from a fundamental, artificial intelligence (AI), and deep learning (DL) point of view.*

Keywords *- Cyber security, Cloud computing, Internet of things, Attack prevention.*

1. Introduction

Cloud computing is a model that enables worldwide and immediate access to a network of shared computing resources that can be allocated and offered by a cloud service provider on demand [1]. A cloud infrastructure built on the Internet of Things (IoT) is a large network that includes several IoT-enabled applications and devices. Cloud computing infrastructure comprises data centers, connectivity infrastructure, real-time computation, and operational support. In the context of IoT, a cloud infrastructure encompasses principles and services for managing, securing, and connecting various IoT applications and devices. The cloud formed over the past ten years, and its variations are still emerging in the coming decade [2], [3]. IoT, or the Internet of Things, is seen as being the most prominent among these variants.

Nonetheless, alternative forms of cloud computing, such as service-oriented architectures, distributed cloud environments, data center operations, and management domains, rapidly adapt to the trend [4]. Based on the findings of a study conducted by the authors of [5], cloud computing has been identified as one of the top ten technology trends in 2020. It was reported that the cloud platform market experienced a growth of 17% in 2020.

Cloud Computing is a model allowing easy and widespread access to a shared pool of configurable computing resources, as defined by the National Institute of Standards and Technology (NIST). These resources may include networks, servers, storage, applications, and services that can be quickly provisioned and released with minimal management effort or interaction with the service provider.[6]. Cloud computing provides a platform that allows for high adaptability, flexibility, and cohabitation [7]. Figure 1 depicts a general cloud computing setting in which consumers may use the cloud from every supporting device in any location on Earth.

The NIST has identified five important character traits of cloud computing [6], namely: (1) measured service, (2) resource sharing, (3) continued growth, (4) connectivity, and (5) user-controlled provisioning. Cloud computing aims to provide various computing services, such as data centers, storage, database systems, network management, software, data analysis, and intelligence, through the internet. Users can select the kind and number of services they require. Traditional IT offerings have shifted to the cloud because of cost savings, convenience, flexible work scheduling, and fast information storage and retrieval. Cloud computing eliminates the need for businesses to purchase costly software as well as hardware to establish on-site data centers. Cloud computing automates various sectors by hosting programs and services

on remote computers. Many industries are now adopting this trend, which is growing with each passing year [8].

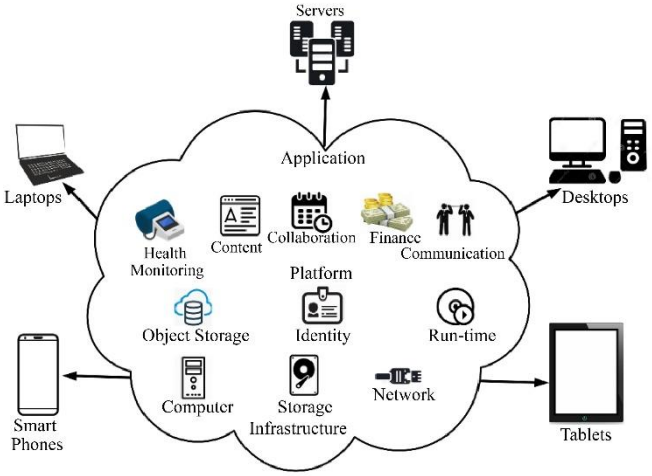

Fig. 1 General cloud computing setting

Cloud computing permits adaptability and frequent software and hardware updates for various industrial uses [9]–[11]. Moreover, the cloud enables users to make efficient utilization of network assets and offers a range of security solutions. These advantages demonstrate the huge potential of cloud computing. Cloud-related technologies offer numerous prospects for industry sectors and have the potential to unlock a variety of applications, solutions, utilities, platforms, and more that are possible in the future. Deep learning-based cloud computing can accommodate massive data volumes and learning algorithms. Its use can also enable deep learning models to attain overall effectiveness on a massive scale at a minimal cost by utilizing the processing power of a graphical processing unit. Any cloud-based approach's effectiveness heavily depends on giving cloud supervisors, software engineers, and end users the best experience possible.

Most importantly, cloud adoption is hampered by specific barriers such as sophistication, conformance, security, dependence, data confidentiality, governance, and cost [12]. Security is considered a significant challenge in cloud computing as applications and data can be situated at various levels depending on the selected cloud service architecture. As a result, security has been ranked as the top concern with cloud technology by researchers [13]. In 2020, Gartner identified four trends that affect the adoption of cloud computing, one of which is addressing related security and privacy concerns, particularly with the increasing prevalence of distributed cloud options [14].

The cloud provides the ability to distribute diverse data, resources, and virtual environments. A user in a typical software infrastructure of a corporation is restricted to the assets that are accessible to them (i.e., storage space, processing power, and hardware). However, a user can benefit from additional server capacity and expanded storage capacity in cloud computing as needed. In their current state, traditional approaches for user identity, authorization, and access control may not be suitable for cloud environments. Significant security concerns include external data storage, reduced user control, interconnected models, and architectures. Data protection is the main issue for safety and confidentiality in cloud-based systems. Each user's personal information will be at risk if this data gets compromised, leading to an increase in cybercrimes, and harming people, businesses, and governments.

Common security risks associated with cloud computing include cryptocurrency mining malware, distributed denial-of-service (DDOS) attacks, user account hijacking, and unauthorized access to sensitive information. According to Forbes [15], Skybox Security published a Security and Threat Report in the middle of 2019, with a significant rise in the number of exploits in cloud containers as the report's main finding. Threats to data in the cloud are greater than those to data in conventional storage systems. This is to make sure that cloud providers not only secure the cloud platform but as well as the customer data. The Oracle and KPMG Cloud Vulnerability Report 2019 found that 82% of cloud users had security incidents.[16]. Thus, ensuring cloud safety and privacy has become essential. According to research, security is the factor that cloud computing needed to flourish the most In 2011, the placement of data was identified as a security concern, leading to the emergence of various data security issues [18, 19, 20]. Researchers have also emphasized the importance of trust in cloud computing due to its close association with the reliability of cloud service providers. Consequently, the availability of trust value and proper trust management have been deemed critical. Trust is the most crucial factor since cloud computing has underlying security challenges. [21]. Cloud-based services are equally susceptible to the same data breaches that afflict conventional systems. It was emphasized that the integrity of the data kept there and the safety of cloud technology depended on the virtual environment machine's security. [22]

Smart IoT cloud systems are discussed in detail in [23], where the authors provide an analysis of five years' worth of research articles on customer-focused IoT cloud applications. This study also includes a security assessment of the IoT cloud infrastructure and offers a novel paradigm for evaluating security. [24] presents a paradigm for evaluating security and confidentiality issues in social networks based on cloud frameworks. Technological risks associated with cloud platforms for various types of cyberattacks are explored in [25].

A study carried out in [26] reported on triangulated research of cloud computing problems. The security concerns that now surround cloud computing were investigated in this tri-partite research. Because of these difficulties, the research also suggested consequences for adopting cloud computing.

Also, writers in [27] provided another thorough examination of a security problem by comparing the risks that cloud platforms face and some detection and mitigation approaches presently in use. Moreover, [28] observed the practical application of algorithms for processing encrypted queries in a high-capacity cloud-based system for a real-time situation. The multi-dimensional average failure cost, characterized as a quantifiable security risk valuation model against the safety issues raised by these researchers, was proposed by [1] in 2016. They also suggested suitable defenses to address the noted security issues.

This paper addresses privacy and security issues in IoT cloud computing, building upon previous research in the field. This research gives a comprehensive survey of IoT cloud architecture, services, configurations, and security models. Previous studies have either discussed security challenges in general or concentrated on a small number of elements. The study outlines four main categories for grouping IoT cloud security issues: data, network and service, apps, and people-related security risks. The study also identifies and examines the most recent developments and patterns in IoT cloud-based threats. The general constraints of AI, particularly DL, are explained and assessed together with each security concern group. The paper also examines technological issues that have been raised in the literature as well as potential future developments in cloud computing and cybersecurity.

The structure of this article is as follows: In Section 2, essential background information regarding cloud-based IoT architecture and services is presented. Section 3 comprehensively reviews previous studies on cloud-based IoT security concerns and attacks. The limitations and challenges of cloud computing are discussed in Section 4. The paper then proceeds to present future research directions in Section 5. The conclusion of the study is presented in Section 6.

2. Cloud-Based IoT Architecture and Services

In recent years, IoT and cloud computing have become the most widely used technologies [29]. According to current trends, the rate of development of digital technologies is predicted to be phenomenal, and the amalgamation of the technologies mentioned above can lead to efficient resource management. This section offers a succinct outline of present cloud architectures, types of clouds, deployment models, and correlated attacks before delving into the subject of security issues and challenges. A brand-new DDoS attack dubbed economic denial of sustainability (EDOS) has arisen in the IoT-based cloud computing era [30]. Using the server-shared monitoring service as an illustration, EDoS may be described as an increase in the wear of flexible packaging (something cloud server). EDOS (Economic Denial of Sustainability) attacks are a type of cyber-attack that aim to exhaust the resources of a targeted system or network by consuming significant amounts of network bandwidth or computing resources. These attacks significantly threaten cloud computing and IoT environments, where multiple devices and systems rely on a shared network and computing resources. EDOS attacks can disrupt cloud services and cause significant downtime, resulting in financial losses and reputational damage to the affected organizations. Furthermore, these attacks can also have severe consequences on IoT devices, which may rely on cloud-based resources and services. Therefore, it is crucial to implement robust security measures, such as intrusion detection systems, firewalls, and access control mechanisms, to prevent EDOS attacks and mitigate their impact on cloud and IoT environments [31].

2.1. Enabling Cloud-Based IoT Architecture

The Internet of Things (IoT) and cloud computing have been integrated, and cloud-based IoT architecture has emerged as a result. This design has several advantages in terms of scalability, flexibility, and data processing capabilities. The effective processing, storing, and analysis of data are made possible by cloud-based IoT architecture, enabling seamless integration of IoT devices, data, and services with cloud-based resources. With the help of this architecture, businesses can handle massive amounts of IoT data, carry out advanced analytics, and derive insightful information for decision-making.

The architecture of the cloud-based IoT has been covered in several research publications in various aspects. For instance, Wu's studies suggested a cloud-based IoT architecture that uses edge computing to enable real-time processing and analysis of IoT data [32]. They emphasized the significance of effective data processing at the edge for enhancing responsiveness and reducing latency in IoT applications. A cloud-based IoT architecture using machine learning techniques for predictive analytics was introduced in a different study by Wang et al. to optimize resource allocation and boost energy efficiency in IoT systems [33]. To achieve the best performance and resource utilization, they underlined the need for intelligent resource management in cloud-based IoT design.

To tackle both small and large-scale business issues, cloud architecture combines various cloud resources, such as data centers, software features, services, and apps. With the help of cloud architecture, end users should be able to access their data and apps with high bandwidth, security, and on-demand adaptability [34]–[37]. Cloud architecture often lays out the elements and relationships between those components. A few essential components of a general cloud architecture are as follows: In that sequence, the list includes local client data and resources, cloud data and resources, software components and services, and middleware.

Cloud computing has become a popular choice for organizations and individuals to store and access data. There are four types of cloud architecture classified in Figure 2.

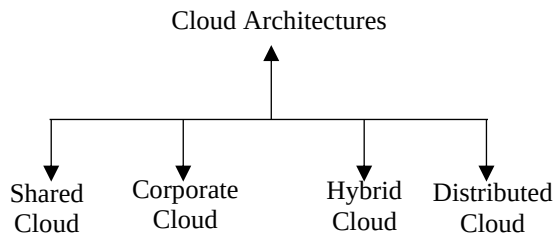

Fig. 2 Various types of cloud architectures

2.1.1. Shared Cloud

A shared cloud is a type of multi-tenant cloud owned and operated by different organizations, and many individuals and organizations use these resources simultaneously. The main issues with this kind of cloud are the allotment of resources, ownership authentication, shared access control, and cloud data protection from attackers. Many entities and organizations instantaneously use these shared resources, infrastructures, and networks. Google, Amazon, and Microsoft are a few of the popular shared cloud providers. Collaborative clouds provide numerous benefits, including dependability, distance neutrality, cost modeled on consumption, economical pricing, exceptional scalability, and adaptability. However, shared clouds also have some disadvantages, such as minor customization and low security [38].

2.1.2. Corporate Cloud

A corporate cloud is a type of single-tenant cloud, usually controlled by a single entity, and is created with that company's needs in mind. Security is critical in corporate clouds, as compared to other cloud environments. It is a sort of cloud technology created with that organization's needs in mind. Organizations can better manage their data by using corporate cloud storage, which makes it more subject to legal requirements for compliance. The infrastructure's management and hosting can be done internally or by a third-party service [39]. The infrastructure is owned and run by the same company. In corporate cloud solutions, the infrastructure is either managed or used by the organization, or the cloud service or infrastructure provider supplies it. Compared to conventional cloud environments, corporate cloud environments place a higher priority on security. Identification of users and vendors, as well as managing security-related concerns, are simpler than in a shared cloud. Using a corporate cloud has benefits [38].

2.1.3. Hybrid Cloud

A hybrid cloud architecture links a corporate cloud to one or even more shared clouds. This connects and centrally manages several cloud platforms with controllable and adaptable workloads. As an illustration, a business can control security between personal and shared clouds, preserving sensitive information in the first and general data in the second. Hybrid cloud security is more reliable than shared cloud security. The advantages of a hybrid cloud are adaptability, scalability, security, and cost-efficiency. However, hybrid clouds have limitations such as networking issues and security compliance [38].

2.1.4. Distributed Cloud

A system that combines numerous cloud computing environments—either public or private—is referred to as a distributed cloud architecture. These clouds are occasionally referred to in the literature as "community clouds," whether or not they are related or linked together. Organizations can use assets and amenities from many cloud providers in distributed cloud environments, offering them flexibility and options in their cloud infrastructure strategy [40], [41].

When opposed to a shared cloud, using a distributed cloud architecture has advantages in terms of security since it allows businesses to divide their data and workloads across several clouds, minimizing the danger of a single point of failure. Sharing resources is another significant benefit, as businesses may maximize their use of the cloud by utilizing various cloud providers according to their unique needs, such as price, performance, or location [42].

Distributed cloud environments could also have certain drawbacks in any case. Because different cloud providers may have varied levels of control and administration over security measures, they might not be as secure as a corporate cloud. To provide uniform administration across various clouds while managing and administering a distributed cloud environment, governing policies and procedures may be necessary. This can complicate and burden the management of the cloud system as a whole.

In achieving an effective and secure cloud implementation, the decision to implement a distributed cloud architecture should consider the unique needs and considerations of the company, including elements like security, resource optimization, and administrative rules. To safeguard their data and workloads in a distributed cloud environment, enterprises should install appropriate safeguards, such as encryption, authentication, and access control systems. The distributed cloud infrastructure should also undergo routine monitoring and audits to maintain compliance with security rules and standards.

To summarize, each cloud architecture type has unique advantages and disadvantages. The decision regarding which architecture to use will depend on factors such as the required storage capacity, accessibility, performance, and security needs of both the user and the organization.

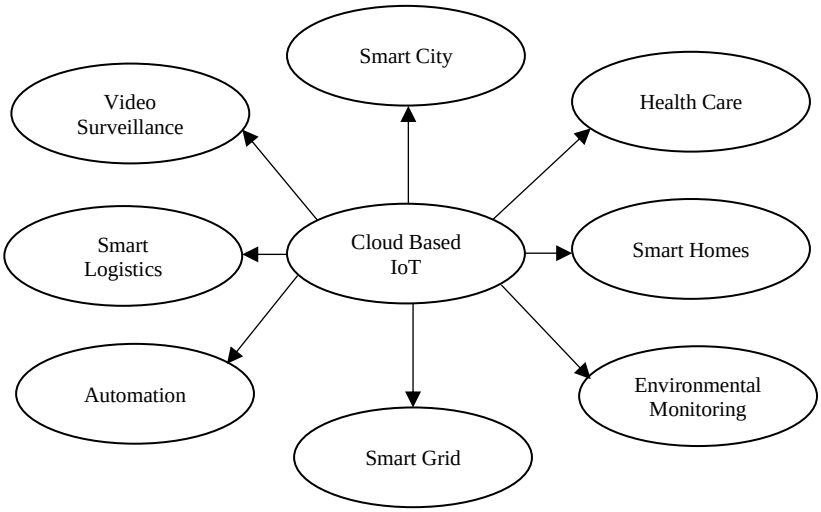

Fig. 3 Various Cloud-based Services in IoT

Corporate clouds, for instance, provide thorough control over the user experience, are more reliable, and have higher security, whereas shared clouds are less reliable and more vulnerable to cyberattacks. Although hybrid clouds combine the finest aspects of both, they also present special networking and security challenges. Although distributed cloud architectures offer better security than shared clouds, they must be managed according to governance principles.

2.2. Cloud-Based IoT Services

The combination of cloud computing and IoT technologies has allowed for the creation of powerful and scalable applications that provide numerous benefits, such as increased reliability, security, and performance. While IoT devices enable real-time data collection and monitoring, the cloud provides a flexible and cost-effective infrastructure for storing and processing data from IoT devices. Cloud-based IoT services can be easily scaled up or down based on the application's needs, allowing cost-effective on-demand scaling. As a result, cloud-based IoT applications have received considerable attention in recent years. They are increasingly being deployed in various domains, including smart cities, healthcare, smart homes, smart grids, and industrial automation. Figure 3 depicts the various services of cloud-based IoT services.

2.2.1. Smart City Concept

Smart city implementation significantly depends on dependable and widespread wireless connectivity. Information and communication technologies (ICT) that are used to create, implement, and promote sustainable practices make up a smart city. The Internet of Things (IoT), a technology that includes tying machines and items together in a network to send data, is one important technology that enables smart city applications. The cloud greatly aids the introduction of IoT-based services in smart cities. Smart cities can effectively gather, store, process, and analyze large amounts of data from numerous sources, including sensors, devices, and systems, to gain insights and make decisions for enhancing urban services, infrastructure, and sustainability. This is done by utilizing cloud-based IoT services.

According to research, cloud-based IoT services greatly impact smart cities. For instance, Rauf et al. offered an IoT-based framework for smart city applications that used cloud computing for data processing and storage. The framework made it possible to monitor environmental factors, including temperature, humidity, and air quality, in real time, enhancing the sustainability of urban areas [88]. Another study by Gubbi et al. emphasized the value of cloud computing in the context of IoT for applications related to smart cities, highlighting the scalability, flexibility, and cost-effectiveness of cloud-based services in supporting IoT installations in urban settings [44].

Moreover, cloud-based IoT services provide chances for collaboration and innovation across many smart city stakeholders. For instance, Botta et al. proposed a cloud-based IoT platform to enable smart city services, including traffic management, waste management, and energy management. This platform would incorporate data from many sources, including sensors, social media, and citizen feedback. To promote innovation and co-creation of urban services, the platform enabled data sharing and collaboration across various entities, including city officials, service providers, and people [45].

By offering scalable, adaptable, and affordable solutions for data storage, processing, and analysis, cloud-based IoT services play a significant role in enabling smart city applications. With real-time monitoring, data-driven decision-making, innovation, and collaboration among various stakeholders, cloud-based IoT services in smart cities can potentially improve urban services, infrastructure, and sustainability. Many studies have emphasized the importance of cloud computing in the context of IoT for applications related to smart cities, highlighting the advantages and

opportunities provided by cloud-based services in creating and implementing smart city solutions.

2.2.2. Cloud Implementation in the Healthcare Sector

Cloud-based by providing remote patient monitoring, real-time data collecting, and enhanced healthcare outcomes, IoT services have completely transformed the healthcare sector. Even when patients are not physically present in the same area as their healthcare provider, IoT-embedded devices such as wearables, remote monitoring tools, and sensors can capture patient data such as heart rate, blood pressure, glucose levels, and other vital indicators. Specialists and other healthcare professionals can remotely monitor and track patients' health problems thanks to real-time data transmission to the cloud.

With quick interventions and individualized treatment plans now possible because of the availability of this real-time patient data, healthcare delivery has undergone a radical change. IoT device data can be analyzed on the cloud by specialists, giving them important information about the health of their patients. This makes it possible for more precise diagnostics, proactive chronic illness treatment, and prompt emergency intervention. In addition, cloud-based IoT technologies have made telemedicine and virtual healthcare possible, removing geographical constraints and expanding access to healthcare services by enabling patients to obtain medical consultations and care remotely.

Several research articles have recognised the importance of cloud-based IoT services in healthcare. For instance, Azimi et al., published in the Journal of Medical Internet Research (JMIR), showed how IoT-based remote monitoring can enhance the quality of care for elderly patients [46]. Another study carried out by Riaz et al. gave a thorough overview of various IoT-based healthcare applications, such as remote patient monitoring, telemedicine, and personalized healthcare [47].

In conclusion, cloud-based IoT services have enabled remote patient monitoring, real-time data collecting, and virtual healthcare, leading to substantial breakthroughs in healthcare. Improved healthcare outcomes, individualized treatment plans, and expanded access to healthcare services have all been made possible by the capacity to gather and analyze patient data from IoT devices in the cloud. Cloud-based IoT services are anticipated to be crucial in altering healthcare delivery and enhancing patient care as technology continues to advance.

2.2.3. Smart Homes

Implementations of smart homes are growing in popularity because of the comfort and convenience they provide to homeowners. These systems use cloud-based services and Internet of Things (IoT) technologies to build a linked ecosystem inside the house. Using smartphone applications or other linked devices, smart home systems often enable users to monitor and manage various house features, including lighting, heating, security, and entertainment. The basic objective of smart home systems is to increase living comfort while lowering costs through resource efficiency.

IoT services provided by the cloud are essential for implementing smart homes. These services enable connections between smart home sensors and gadgets and the cloud, which processes, examines, and stores data. Using smartphone applications or other user interfaces, real-time monitoring and control of home functions are now possible, thanks to cloud-based services, which offer the computing power, storage, and scalability required to handle the massive amounts of data generated by smart home devices.

Academic literature has extensively covered research in cloud-based IoT services for smart home deployments. Using IoT devices, cloud computing, and data analytics, for instance, the authors of a paper by A. Ali et al. suggested a cloud-based architecture for smart homes to enable intelligent decision-making for energy management in such houses [48]. The real-time monitoring and control of house appliances by the authors demonstrated how well their suggested architecture reduced energy consumption in smart homes.

A cloud-based framework for smart house automation was developed in a different study by Saneep et al. [49]. This framework uses IoT technologies to enable the interconnection of smart home devices, cloud computing, and data analytics. The authors presented a thorough architecture using cloud-based data processing, analysis, and storage services. They covered the advantages of doing so for effective control and administration of smart home systems.

The creation of a cloud-based IoT infrastructure for smart houses that permits remote monitoring and management of home activities through smartphone applications was also the focus of a study by S. H. Tayef et al. [50]. By practical trials, the authors proved the viability of their platform and presented a flexible and adaptable architecture that integrates multiple smart home devices, cloud computing, and data analytics.

Lastly, by providing the required data infrastructure for processing, storage, and analysis, cloud-based IoT services play a significant role in enabling the adoption of smart homes. Smart home devices and sensors can be seamlessly integrated with cloud-based services, allowing for real-time monitoring and management of house processes via mobile apps or other user interfaces. As a result of the study in this area, homeowners now have more comfort and convenience thanks to various architectures and frameworks that effectively manage and control smart home devices via cloud-based services.

2.2.4. Smart Electricity Grids

Smart grids are becoming more and more common because of their ability to improve energy consumption efficiency, reduce greenhouse gas emissions, and facilitate the integration of renewable energy sources. The cloud-based delivery of IoT services is necessary to implement smart grids. By utilizing cloud computing technology, smart grids can collect and analyze massive amounts of data from various sources, such as smart meters, renewable energy sources, and weather sensors. These data are then used to optimize the electrical grid's stability, resilience, and energy utilization.

Real-time control and monitoring of the smart grid are also made possible by cloud-based IoT services, giving grid managers the ability to address any potential problems immediately. To minimize widespread outages, for instance, the system can instantly isolate the afflicted area in the event of a localized failure and reroute power. Moreover, energy storage systems can be managed by cloud-based IoT services, which can assist the grid to be balanced and boost the incorporation of clean energy sources.

The implementation of cloud-based IoT services in smart grid systems has been investigated in several studies. M. Yalpanian et al., for instance, called for a cloud-based IoT platform to control distributed energy resources in smart grids [51]. The platform employs machine learning algorithms to improve energy consumption and lower expenses. Data is gathered from numerous sources, including smart meters and renewable energy sources. A cloud-based IoT system was created by Khan et al. for the real-time monitoring and management of the smart grid [52]. The system incorporates some sensors and devices to gather data, which is then processed and analyzed using cloud computing technologies.

In conclusion, the development of smart grids is made possible by cloud-based IoT services. Smart grids can gather and analyze enormous volumes of data, optimize energy use, and boost the dependability and resilience of the power system by using cloud computing technology. Studies investigating the usage of cloud-based IoT services in smart grid installations have shown how they can potentially transform the energy industry.

2.2.5. Industrial Automation

Industrial automation has completely changed the manufacturing sector by increasing productivity, lowering costs, and integrating IoT devices and cloud computing. Smart factories can link industrial equipment like machines, robots, and humans using IoT automation devices, which helps to optimize production processes. Automation devices can gather and transfer data to the cloud for real-time analytics, which can be used to monitor and improve industrial operations, thanks to cloud-based IoT services [53].

IoT automation tools can increase safety in industrial settings in addition to increasing productivity. For instance, sensors may be used to identify unsafe situations and warn workers, and robots can be deployed to carry out risky activities, lowering the likelihood of accidents. Manufacturers may reduce downtime and boost productivity by adopting cloud-based IoT services to monitor their facilities and respond to real-time problems remotely.

The advantages of cloud-based IoT services in industrial automation have been underlined in numerous study studies. The authors of [53] presented a cloud-based Internet of Things (IoT) framework for industrial automation to increase overall productivity and lower expenses. A similar cloud-based IoT system for quality assurance in manufacturing was proposed in a paper by S. V. Lakshami [54]. This system uses cloud computing to monitor and improve production processes continuously. These studies show how cloud-based IoT services have the potential to change the industrial sector by allowing smart factories that can improve safety, save costs, and optimize production processes.

3. Security Concerns and Attacks in Cloud-based IoT System

Cloud service providers are often thought to be in charge of cloud security. However, in recent years, an increasing number of firms have moved their operations, data, and applications to the cloud [55]. Cyberattacks' priorities have altered as a result, and they now consider cloud services to be a more profitable target [56]. Figure 6 provides a picture of the cloud system's components, assaults, and loopholes that can be examined to find new points of weakness. The biggest concern when participating in cloud services is security threats in cloud computing. It is because third-party vendor stores and process the user's information without the user's awareness. Defective identification, leaked credentials, account hijacking, data theft, and other problems are possible.

Despite the fact, the numerous advantages of IoT systems, security concerns and attacks are critical issues that must be addressed. Security threats to IoT systems can arise from the numerous interconnected devices that communicate with each other, making it difficult to guarantee the security of every device in the network. One possible security threat is the unauthorized access of sensitive information from IoT devices. Attackers may use different methods to access an IoT device, such as hacking or phishing attacks. Once they gain access, they can manipulate the device and its data, which can have serious consequences. Additionally, IoT devices can be attacked to create botnets, a network of devices controlled remotely by an attacker to launch attacks on other devices or systems.

Fig. 4 Cloud computing-associated threats, attacks, and components

To address these security concerns, researchers have proposed several solutions. One approach is implementing encryption and authentication techniques to secure data communication between IoT devices and cloud servers. Other solutions include intrusion detection and prevention systems, firewalls, and multi-factor authentication mechanisms to protect against unauthorized access. For example, a study by A. Al-Fuqaha et al. proposed a security framework for IoT systems that includes several security measures, such as authentication, authorization, and access control [57].

Another study by A. Abbas et al. proposed a blockchain-based security framework for IoT systems to ensure data integrity and confidentiality [58]. These studies demonstrate the importance of addressing security concerns and implementing robust security measures in IoT systems to prevent attacks and ensure data confidentiality, integrity, and availability. Figure 4 highlights various cloud computing-associated threats, attacks, and associated components.

The most significant cloud-based assaults on IoT systems are highlighted in the following section. The prevention methods used to lessen similar attacks in the past few years are also mentioned here.

3.1. Data Theft

The dangers of data theft in cloud computing and their effects on IoT devices have been emphasized in some studies. S. E. Gendi et al. highlighted security concerns in cloud computing that could influence IoT devices in their study, and they suggested a security framework to reduce these risks [59]. The security issues related to cloud-based IoT applications were also examined in a study by Khan et al., and a security architecture was suggested to handle these risks [60]. These findings underline how crucial it is to preserve sensitive data and prevent data theft by guaranteeing the security of IoT devices and cloud settings.

Data theft in cloud computing has become a major concern due to the potential impact on the security of IoT devices. As more and more devices connect to the cloud, the amount of sensitive data stored and processed in cloud environments has increased significantly. Any breach of this data can have severe consequences, including financial loss, damage to reputation, and even physical harm.

The system's complexity is one of the main obstacles to preventing data theft in cloud systems. Vulnerabilities in cloud computing are difficult to find and fix because of the numerous layers of hardware, software, and networking involved. Moreover, data theft can happen as a result of human mistakes or carelessness. Therefore, it is critical to have appropriate security processes in place to guard against such occurrences.

The dangers of data theft in cloud computing have been reduced using various methods and solutions, including encryption, access restriction, and intrusion detection systems. These precautions are not infallible, though, and theft is still possible. It is crucial to avoid data theft and safeguard sensitive information to maintain vigilance and constantly check the security of cloud environments and IoT devices.

3.2. Loss of User Data

Data loss presents a significant risk in cloud computing, especially for Internet of Things (IoT) devices that depend on cloud-based computing and storage resources. Data loss can happen for several causes, including hardware or software failure, virus assaults, or natural disasters. Data loss in a cloud environment can have serious repercussions, including monetary losses and reputational harm to the company.

The significance of establishing appropriate data loss prevention mechanisms in cloud-based IoT systems has been highlighted by many studies. In a study, Agarwal et al. suggested a data loss prevention framework for cloud-based IoT systems that made use of machine learning methods to recognize and stop data loss [61]. In a similar study, M. E. Hussain suggested a data loss prevention solution for cloud storage services, including encryption methods to safeguard sensitive data [62]. These studies show the potential of utilizing cutting-edge technology to stop data loss in cloud-based IoT systems.

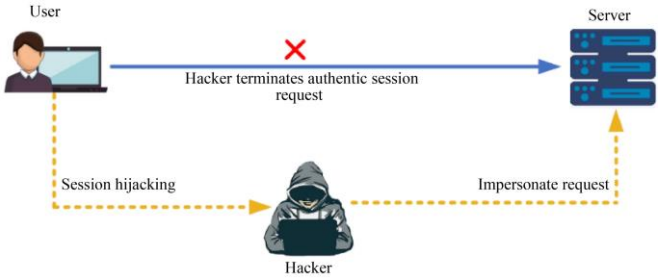

Fig. 5 Basic illustration of account takeover attack

Having a solid backup and recovery plan in place is just as important as putting data loss prevention measures in place. Regular backups of important data should be part of this strategy, as should a disaster recovery plan that may be used in the event of a data loss incident. Organizations can lessen the effects of data loss events and guarantee the continuity of their operations by putting these procedures in place.

3.3. Account Takeover

IoT devices are impacted by account takeover, also known as service traffic hijacking, a critical security issue in cloud computing. Cybercriminals or hackers who illegally access sensitive data about accounts and services commit this kind of attack. Hackers may broadcast, use, or sell private information like financial records, credit card details, and personal photographs. This can result in identity theft, financial loss, and reputational harm for those involved, whether people or organizations. Moreover, such an assault may lead to exploiting IoT devices and other cloud-based services. Figure 5 illustrates the strategy adopted by a hacker for an account takeover attack.

Several security mechanisms, including strong passwords, two-factor authentication, and encryption approaches, have been suggested in the literature to avoid account or service traffic hijacking. For example, Zhao et al. suggested a secure architecture for cloud-based IoT systems that used encryption techniques to safeguard data transmission and access [63]. The use of two-factor authentication and access control techniques was also recommended in a study by A. Al-Fuqaha et al. to improve the security of cloud-based IoT systems [57]. These findings highlight the importance of implementing strong security controls to guard against account or service traffic hijacking in cloud-based IoT systems. Furthermore, It is advised to verify whether the service provider performs background checks on employees with physical access to the server to improve security in cloud computing and IoT systems. Also, it's critical to disable IP addresses from which cloud apps can be accessed and to have a solid authentication mechanism for clients of cloud applications. Users can select IP ranges in some cloud applications to restrict access to the corporate network or VPN.

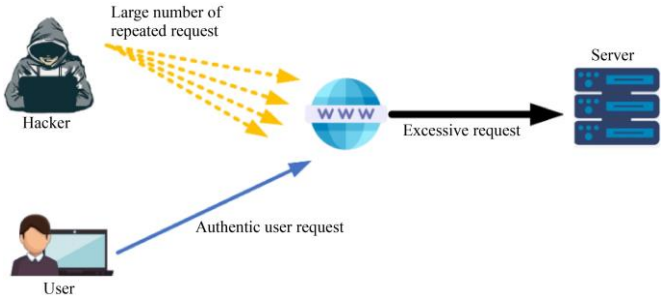

Fig. 6 Basic illustration of the DoS attack

3.4. Denial of Service (DoS) Attack

Attacks that cause a denial of service (DoS) pose a severe security risk for cloud computing and may also affect IoT systems. A DoS attack involves flooding a system with numerous requests to prevent it from operating normally. This overloads the system's resources and prevents legitimate users from accessing it, as illustrated in Figure 6. One or more sources can carry out this attack, which can seriously impact major monetary losses, reputational harm, and even legal repercussions.

Due to its extensive distribution and size, the IoT is particularly susceptible to DoS assaults. If an IoT device is the target of a successful DoS attack, vital infrastructure services like healthcare, transportation, and energy could be affected. DoS attacks on IoT devices can also result in the loss of sensitive data, such as financial or personal health records, endangering the security and privacy of users.

Security measures like firewalls, intrusion detection and prevention systems, and network segmentation can be put in place to stop DoS assaults. Moreover, IoT devices and cloud systems can be properly configured, patched, and updated to improve security and lower the possibility of successful DoS assaults.

Research has been done to examine how DoS attacks affect cloud computing and IoT systems and to suggest practical mitigation strategies. For instance, a study by A. Jamalipour et al. examined the effects of DoS assaults on IoT systems and offered a novel strategy for identifying and countering these attacks [64]. This strategy makes use of machine learning techniques. Similarly, a subsequent study by Niyamtiga et al. suggested a revolutionary strategy combining edge computing with blockchain technology to enable effective and secure data communication in the Internet of Things systems, thereby lessening the impact of DoS assaults [65].

3.5. Malicious Insider Attack

Malicious insiders pose a significant security risk to cloud computing and can also influence IoT devices. These insiders are those who have been granted permission to enter the system but deliberately misuse their rights to hurt others. As the attacker is a legitimate user with access to the system's data

and services, this kind of attack is difficult to identify. Insiders with malicious intent can interrupt system operations, change sensitive data, and cause severe financial losses and reputational harm.

Due to the sheer volume of connected devices and the scattered architecture of the system, the IoT is particularly susceptible to hostile insider assaults. Successful malicious insider attacks on IoT devices have the potential to compromise user privacy and security by disrupting vital infrastructure services like healthcare, transportation, and electricity and by causing the loss of sensitive data like financial or personal health records.

Security measures like access restriction, monitoring, and auditing can be implemented to thwart hostile insider assaults. Also, the danger of insider threats can be reduced by conducting adequate background checks and vetting workers with administrative access. Employees who receive regular security training will be more aware of security concerns and more likely to report any suspicious conduct.

It has been studied how hostile insider assaults affect IoT and cloud computing systems and how to mitigate the risks effectively. For instance, a study by Zhao et al. developed a unique method that makes use of blockchain technology to improve IoT device security and guard against harmful insider assaults [66]. In a similar research, Kim et al.'s article also suggested an intrusion detection system that employs machine learning methods to identify insider threats in cloud computing systems [67].

3.6. Phishing Attacks

Phishing, or impersonating a reliable entity in cyberspace, is the most popular term for a cyber-attack involving fooling people into disclosing sensitive information like usernames, passwords, and credit card numbers. This type of attack can negatively affect IoT devices and are a major risk in cloud computing. To trick the victim into disclosing critical information like passwords, credit card numbers, or other personal information, the attacker will send deceptive emails, texts, or other forms of communication. Once the attacker has this knowledge, they can use it to log into the victim's cloud account, where they can steal sensitive information or commit other crimes.

Because IoT devices frequently lack adequate security protections and are more vulnerable to infiltration, phishing assaults are particularly concerning for IoT devices. Suppose an IoT device is the target of a successful phishing attack. In that case, sensitive data may be compromised, unauthorized users may get access to the device, or the attacker may even have full control over the device.

Users must be alert and take precautions to prevent phishing attempts, such as double-checking links before clicking on them, refraining from sending sensitive information over email and reporting any suspicious activity to the proper authorities. By limiting access to dangerous files and filtering incoming emails, cloud-based email systems can also help identify and thwart phishing attacks.

Several research studies have explored the impact of phishing attacks on cloud computing and IoT systems and proposed mitigation techniques. For instance, a study by Salahdine et al. proposed a machine learning-based approach to detect phishing attacks in cloud environments [68]. Similarly, another study by P. Velmurugan et al. proposed a framework for enhancing security in IoT devices by implementing advanced encryption and authentication techniques to prevent phishing attacks [69].

3.7. Cloud-based Malware Attack

Cyberattacks are known as cloud malware injection attacks (CMIAs), targeting cloud computing infrastructure to access sensitive data stored in the cloud. Cross-site scripting and SQL injection attacks, which take advantage of flaws in cloud service providers like OpenStack, are two typical types of CMIA. The security of IoT devices, which frequently depend on cloud computing services to store and process data, can be severely impacted by CMIAs. A successful CMIA attack can weaken the security of IoT devices, allowing the attacker to steal confidential data, gain unauthorized access to the device, or even take full control of it. Critical infrastructure services like healthcare, transportation, and electricity may suffer as a result, which might be quite dangerous.

An attacker who uses a malware injection attack seeks to introduce harmful applications and services into the cloud [70]. To carry out this assault, the attacker employs various techniques while keeping the cloud model in mind. The attacker starts by creating a malicious service application module or virtual machine instance on its own, then tries to add it to the cloud. The attackers then attempt to turn it into a legitimate instance, divert the legitimate user's requests to the malicious service application, and run the malicious code [71]. The attacker tries to exploit the cloud platform to operate, access user data, resources, and data, and change data. IoT relies on cloud computing since it is widely used and admired worldwide for data and resource storage. One such attack uses IoT devices' factory default login details to infect them with the Mirai malware.

It is essential to stop Cloud Malware Injection Attacks (CMIAs) to keep cloud-based systems secure. Organizations should ensure that their software and applications are updated with the most recent security patches and upgrades to prevent these threats. Additionally, they should put strong access controls in place, such as regular access authorization reviews and multi-factor authentication, and encrypt sensitive data in transit and at rest. It is important to find any weaknesses in the system and to undertake regular security audits. End users

should also receive training on how to spot and report suspicious activity, including phishing scams and other social engineering techniques frequently employed in CMIA attacks.

3.8. Open Port Attack

In a port scanning attack, an attacker searches for open ports on a system or network to find potential security holes that can be used to launch additional assaults. Because several virtual machines are running on the same physical hardware in cloud computing settings, a single vulnerability in one of the virtual machines might potentially expose the entire cloud architecture.

Attacks that use port scanning may be pertinent in the context of the Internet of Things (IoT). IoT devices are frequently connected to the internet and are susceptible to port scanning attacks if they are not properly secured. For instance, a hacker may search a home router for open ports and use a flaw to access connected IoT devices like security cameras or smart thermostats. An IoT device can be used as a launching pad for additional assaults or as a botnet component for DDoS attacks after an attacker can access it [72], [73].

Businesses and organizations can put in place a variety of defense techniques to stop port scanning attacks. One strategy is to install a powerful firewall to control port visibility and prevent unauthorized access to the network. An alternative method is using TCP wrappers to restrict server access based on IP addresses and domain names. Frequent system audits can also assist in locating security flaws and vulnerabilities that attackers may exploit.

Lastly, port scanning attacks pose a significant risk to IoT and cloud computing infrastructures. Strong firewalls, TCP wrappers, and routine system audits are preventive measures that can help reduce the hazards brought on by port scanning attacks.

3.9. Botnet Attacks

Attacks by botnets are a serious risk to cloud-based systems and are becoming more of an issue in the IoT space. In this kind of assault, an attacker takes control of a network of compromised computers or devices and uses it to carry out harmful operations, including distributed denial of service (DDoS), spamming, data theft, and phishing attacks [74]. Cloud services can be used to create botnets, which are challenging to identify and stop since they can immediately activate and work nonstop [75].

It is crucial to maintain software updated and closely monitor the network for any indications of unusual activity to prevent botnet assaults [74]. Aside from monitoring failed login attempts, businesses must also be alert to any changes in traffic patterns or odd network behavior [75]. Using bot defense systems that dependably screen out malicious requests to gain access to websites and APIs while allowing access to legitimate requests from clients or partners can help identify and prevent botnet assaults, which also require advanced detecting abilities [76].

In the IoT space, where the number of connected devices is increasing exponentially and securing these devices is getting harder, a study by Pokhrel et al. emphasizes the significance of botnet attacks [77]. According to network flow parameters and classification of network traffic as either botnet or non-botnet traffic, the study suggests a machine learning-based framework for botnet identification in IoT devices.

In summary, botnet assaults are becoming a bigger problem in the IoT space and seriously threaten cloud-based systems. Businesses must maintain current software, regularly monitor the network, and be alert to any changes in traffic patterns or unexpected network behavior if they want to prevent botnet assaults. Moreover, sophisticated detection abilities are needed to recognize and stop botnet attacks. This can be done by utilizing bot protection tools and frameworks built on machine learning or deep learning for botnet detection in IoT devices.

4. Obstacles and Restrictions of Cloud Computing

IoT has many benefits for users, but it also raises issues with security and privacy. Managing data collection, access control, and privacy become critical issues in cloud-based IoT architecture when IoT devices transfer private data to vendors or third parties. Although methods like access control, encryption, and privacy protection can be useful, they are not always enough. The vast volume of data gathered, major vulnerabilities, and a lack of encryption are the causes of the hazards and difficulties associated with the rise of the IoT. IoT device proliferation raises issues about data privacy. While confidentiality, availability, and database integration are fundamental data security features in the public cloud development paradigm, authentication, authorization, and non-repudiation are key properties when accessing IoT data on the cloud [78], [79].

Organizations have benefited from cloud computing by making use of its enhanced cloud infrastructures, better effectiveness, improved work throughput, and lower cost. Traditional cloud infrastructures must be reevaluated and related security risks addressed in light of improvements in 5G, IoT infrastructures, smart mobile devices, and intelligent AI-based data analytics platforms.

4.1. Preserving the Privacy, Security, and Accessibility of Data (PSA)

Cloud computing faces challenges in maintaining availability, integrity, and confidentiality. Data collected from IoT devices must be protected from unauthorized access.

Confidentiality is crucial before uploading data to cloud servers through any insecure media[80], [81].

4.2. Elements of Application Security

Software application security is a significant challenge and critical vulnerability in information security [82]. Cloud computing brings diversity to the list of associated vulnerabilities, as millions of programming lines are behind in developing applications written in different languages by various programmers.

4.3. Challenges posed by COVID-19 or similar pandemics

Remote working models adopted by many industries have forced the excessive use of cloud resources due to the safety concerns surrounding COVID-19. It will be challenging for the cloud computing industry if a similar situation arises shortly [83].

4.4. Constraints of Computational Resources

IoT provides users with some benefits but also presents privacy and security issues. With cloud-based IoT architecture, controlling data collection, access control, and privacy becomes a critical concern when IoT devices transfer sensitive data to vendors or third parties. Though they can be useful, methods like access control, encryption, and privacy protection are not always enough. IoT expansion entails risks and difficulties because of the vast amounts of data generated, significant vulnerabilities, and a lack of encryption [84], [85]. With more IoT devices, data privacy worries grow. While accessing IoT data on the cloud, authentication, permission, and non-repudiation are crucial qualities. In contrast, confidentiality, availability, and database integration are fundamental data security aspects in the public cloud development model.

4.5. Categorization of Security Issues

To provide security with the least amount of expense and effort, cloud computing involves the classification of information assets and the handling of security issues according to the related classification level. It might be difficult to categorize information when numerous users and organizations share it. Organizations responsible for cloud security must deal with concerns such as data duplication, quick threat detection, lowered access control, and regulatory compliance [86], [87].

5. Future Scope

In conclusion, this research highlights the importance of addressing security and privacy issues in cloud computing systems. They are becoming increasingly essential for data storage and processing in modern technologies such as IoT, smart cities, and the 5G internet. Researchers may focus on different logical control techniques to improve cloud security, including reviewing and analyzing existing security models and addressing authenticity, encryption, multi-tenancy, and security of virtual machines. Resource sharing in cloud computing infrastructures must also be studied to ensure inclusive cloud system security.

The future direction of cloud computing includes implementing blockchain technology to enhance data security and storage methods. Blockchain-based cloud log security can make cloud systems unbreachable, increasing users' trust in a cloud environment. Authentication mechanisms using blockchain technology will also make it difficult for insiders to access user login credentials. Federated learning techniques, which can train algorithms on multiple decentralized servers using local data without sharing, can be used to achieve strong privacy in cloud computing. Additionally, optimization strategies can be utilized to enhance algorithm training efficiency while addressing privacy concerns and statistical heterogeneity.

6. Conclusion

The use of cloud computing has changed how businesses and organisations function, yet it has additionally increased security threats that jeopardize the data's safety. Though cloud technology has provided businesses with the adaptability and scale they need to compete in an industrial world that is changing quickly, it has also exposed their data to security threats. The deployment models, cloud architecture, and common assaults have all been covered in this study. We divided cloud security concerns into four groups and discussed the related problems in each category. Also, we have outlined difficulties that must be overcome, such as restrictions that have emerged in the fields of AI and DL concerning cloud computing.

According to the survey, hackers' creative hacking methods and technology breakthroughs are increasing security threats in the cloud. To guarantee the security and privacy of data in the cloud, it is essential to create new security approaches and enhance those that already exist. Cloud service providers and end users must work together to address cloud security. It is crucial to take a thorough approach to cloud security that considers all facets of the cloud computing environment, including network security, access management, and data encryption. Further research is urgently needed in areas like blockchain-based cloud security, federated learning for the cloud, and authentication systems to increase cloud security, as this article has shown.

References

[1] Mouna Jouini, and Latifa Ben Arfa Rabai, "A Security Framework for Secure Cloud Computing Environments:," *International Journal of Cloud Applications and Computing*, vol. 6, no. 3, pp. 32–44, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[2] Aqsa Mohiyuddin et al., "Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System," *International Journal of Fuzzy Systems Volume*, vol. 24, no. 2, pp. 1203–1215, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Rabia Abid et al., "An Optimised Homomorphic CRT-RSA Algorithm for Secure and Efficient Communication," *Personal and Ubiquitous Computing,* 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Arfa Arslaan Ikram et al., "Mobile Cloud Computing Framework for Securing Data," *2021 44th International Conference on Telecommunications and Signal Processing (TSP)*, Brno, Czech Republic, IEEE, pp. 309–315, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Gartner Top 10 Strategic Technology Trends, 2020. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020

[6] Peter Mell, and Timothy Grance, "*The NIST Definition of Cloud Computing*," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-145, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[7] Aakriti Sharma, Bright Keshwani, and Pankaj Dadheech, "Authentication Issues and Techniques in Cloud Computing Security: A Review," *SSRN Journal*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Mostafa Ghobaei-Arani et al., "ControCity: An Autonomous Approach for Controlling Elasticity Using Buffer Management in Cloud Computing Environment," *IEEE Access*, vol. 7, pp. 106912–106924, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," *IEEE Access*, vol. 9, pp. 8820–8834, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Thar Baker et al., "Intention-Oriented Programming Support for Runtime Adaptive Autonomic Cloud-Based Applications," *Computers & Electrical Engineering*, vol. 39, no. 7, pp. 2400–2412, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mohammed Al-khafajiy et al., "COMITMENT: A Fog Computing Trust Management Approach," *Journal of Parallel and Distributed Computing*, vol. 137, pp. 1–16, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Tian Xia et al., "CSPM: Metamodel for Handling Security and Privacy Knowledge in Cloud Service Development," *International Journal of Systems and Software Security and Protection*, vol. 12, no. 2, pp. 68–85, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] John R. Vacca, *Cloud Computing Security: Foundations and Challenges,* CRC Press, 2016. [Google Scholar] [Publisher Link]

[14] 4 Trends Impacting Cloud Adoption in 2020, Gartner. [Online]. Available: https://www.gartner.com/smarterwithgartner/4-trends-impacting-cloud-adoption-in-2020

[15] Jeb Su, Why Cloud Computing Cyber Security Risks are on the Rise: Report, Forbes. [Online]. Available: https://www.forbes.com/sites/jeanbaptiste/2019/07/25/why-cloud-computing-cyber-security-risks-are-on-the-rise-report/

[16] Preeti Mishra et al., "VMProtector: Malign Process Detection for Protecting Virtual Machines in Cloud Environment," *Advances in Computing and Data Sciences*, *Communications in Computer and Information Science,* Singapore: Springer Singapore, vol. 1045, pp. 360–369, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, and Saleh A. Wasimi, "A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing," *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833–851, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[18] David Teneyuca, "Internet Cloud Security: The Illusion of Inclusion," *Information Security Technical Report*, vol. 16, no. 3–4, pp. 102–107, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[19] Noriswadi Ismail, "Cursing the Cloud (or) Controlling the Cloud?," *Computer Law & Security Review*, vol. 27, no. 3, pp. 250–257, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nancy J. King, and V.T. Raja, "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud," *Computer Law & Security Review*, vol. 28, no. 3, pp. 308–319, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[21] Patrick Ryan, and Sarah Falvey, "Trust in the Clouds," *Computer Law & Security Review*, vol. 28, no. 5, pp. 513–521, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[22] Rashmi, Dr.G.Sahoom, and Dr.S.Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions," *International Journal on Cloud Computing: Services and Architecture*, vol. 3, no. 4, pp. 1–11, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[23] Fei Chen et al., "IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-oriented Applications," *ACM Computing Surveys*, vol. 54, no. 4, pp. 1–36, 2022. [CrossRef] [Publisher Link]

[24] Patruni Muralidhara Rao, and Pedada Saraswathi, "Evolving Cloud Security Technologies for Social Networks," *Security in IoT Social Networks*, *Elsevier,* pp. 179–203, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Reza Montasari et al., "Cloud Computing Security: Hardware-Based Attacks and Countermeasures," *Digital Forensic Investigation of Internet of Things (IoT) Devices*, *Advanced Sciences and Technologies for Security Applications,* Cham: Springer International Publishing, pp. 155–167, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] M. A. Khan, "A Survey of Security Issues for Cloud Computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11–29, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[27] Deepak Puthal et al., "Cloud Computing Features, Issues, and Challenges: A Big Picture," *2015 International Conference on Computational Intelligence and Networks*, *IEEE,* pp. 116–123, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[28] Faisal Shahzad, Waheed Iqbal, and Fawaz S. Bokhari, "On the use of Cryptdb for Securing Electronic Health Data in the Cloud: A Performance Study," *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, Boston, MA, USA: IEEE, pp. 120–125, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[29] M. Anuradha et al., "IoT Enabled Cancer Prediction System to Enhance the Authentication and Security Using Cloud Computing," *Microprocessors and Microsystems*, vol. 80, p. 103301, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[30] Marco Antonio Sotelo Monge, Jorge Maestre Vidal, and Gregorio Martínez Pérez, "Detection of Economic Denial of Sustainability (Edos) Threats in Self-Organizing Networks," *Computer Communications*, vol. 145, pp. 284–308, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[31] Madarapu Naresh Kumar et al., "Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing Using in Cloud Scrubber Service," *2012 Fourth International Conference on Computational Intelligence and Communication Networks*, IEEE, pp. 535–539, 2012. [CrossRef] [Google Scholar] [Publisher Link]
[32] Yulei Wu, "Cloud-Edge Orchestration for the Internet of Things: Architecture and AI-Powered Data Processing," *IEEE Internet of Things Journal,* vol. 8, no. 16, pp. 12792–12805, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[33] Jun-Bo Wang et al., "A Machine Learning Framework for Resource Allocation Assisted by Cloud Computing," *IEEE Network*, vol. 32, no. 2, pp. 144–151, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[34] Afia Naeem et al., "DARE-SEP: A Hybrid Approach of Distance Aware Residual Energy-Efficient SEP for WSN," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 611–621, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[35] Abdul Rehman Javed et al., "Green5G: Enhancing Capacity and Coverage in Device-to-Device Communication," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1933–1950, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[36] Swarna Priya R.M et al., "Load Balancing of Energy Cloud Using Wind Driven and Firefly Algorithms in Internet of Everything," *Journal of Parallel and Distributed Computing*, vol. 142, pp. 16–26, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[37] Rana Zeeshan Ahamad et al., "Interference Mitigation in D2D Communication Underlying Cellular Networks: Towards Green Energy," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 45–58, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[38] B. Kezia Rani, B. Padmaja Rani Dr., and A. Vinaya Babu Dr, "Cloud Computing and Inter-Clouds – Types, Topologies and Research Issues," *Procedia Computer Science*, vol. 50, pp. 24–29, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[39] Tinankoria Diaby, and Babak Bashari Rad, "Cloud Computing: A Review of the Concepts and Deployment Models," *International Journal of Information Technology and Computer Science*, vol. 9, no. 6, pp. 50–58, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[40] Mohammad Babar et al., "Cloudlet Computing: Recent Advances, Taxonomy, and Challenges," *IEEE Access*, vol. 9, pp. 29609–29622, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[41] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[42] Lu Shen et al., "CloudS: A Multi-cloud Storage System with Multi-level Security," *Algorithms and Architectures for Parallel Processing*, Lecture Notes in Computer Science, Cham: Springer International Publishing, vol. 9530, pp. 703–716, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[43] S. Karthikeyan, T. Poongodi, "Secure and Optimized Communication in the Internet of Things using DNA Cryptography with X.509 Digital Attributes," International Journal of Engineering Trends and Technology, vol. 71, no. 3, pp. 1-8, 2023. [CrossRef] [Publisher Link]
[44] Jayavardhana Gubbi et al., "Internet of Things (Iot): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[45] Alessio Botta et al., "Integration of Cloud Computing and Internet of Things: A Survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[46] Iman Azimi et al., "Internet of Things for Remote Elderly Monitoring: A Study From User-Centered Perspective," *Journal of Ambient Intelligence and Humanized Computing,* vol. 8, no. 2, pp. 273–289, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[47] S. M. Riazul Islam et al., "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[48] A. R. Al-Ali et al., "A Smart Home Energy Management System Using IoT and Big Data Analytics Approach," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 4, pp. 426–434, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[49] Faraz Doja et al., "A Comprehensive Framework for the IoT-Based Smart Home Automation Using Blynk," *Information and Communication Technology for Competitive Strategies,* Lecture Notes in Networks and Systems, Singapore: Springer Nature Singapore, vol. 401, pp. 49-58, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[50] Mohammad Asadul Hoque, and Chad Davidson, "Design and Implementation of an IoT-Based Smart Home Security System," *International Journal of Networked and Distributed Computing*, vol. 7, no. 2, pp. 85-92, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[51] Mostafa Yalpanian et al., "BIOT: A Blockchain-Based IoT Platform for Distributed Energy Resource Management," *Silicon Valley Cybersecurity Conference*, Communications in Computer and Information Science, Cham: Springer International Publishing, vol. 1383, pp. 134–147, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[52] Fahad Khan et al., "IoT Based Power Monitoring System for Smart Grid Applications," *2020 International Conference on Engineering and Emerging Technologies*, IEEE, pp. 1-5, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[53] Jacques Jansen, and Alta van der Merwe, "A Framework for Industrial Internet of Things," *Responsible Design, Implementation and Use of Information and Communication Technology*, Lecture Notes in Computer Science, Cham: Springer International Publishing, pp. 138–150, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[54] S. Venkata Lakshmi et al., "Role and Applications of IoT in Materials and Manufacturing Industries – Review," *Materials Today: Proceedings*, vol. 45, pp. 2925–2928, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[55] Abdul Rehman Javed et al., "Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291–4300, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[56] Waqas Ahmed et al., "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 115932–115950, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[57] Ala Al-Fuqaha et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[58] Asad Abbas et al., "Blockchain-Assisted Secured Data Management Framework for Health Information Analysis Based on Internet of Medical Things," *Personal and Ubiquitous Computing*, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[59] Sherif El-Gendy, and Marianne. A. Azer, "Security Framework for Internet of Things (IoT)," *2020 15th International Conference on Computer Engineering and Systems*, IEEE, pp. 1–6, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[60] Naqash Azeem Khan, Azlan Awang, and Samsul Ariffin Abdul Karim, "Security in Internet of Things: A Review," *IEEE Access*, vol. 10, pp. 104649–104670, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[61] Er. Garima Agrawal, and Dr. Samta Jain Goyal, "Survey on Data Leakage Prevention through Machine Learning Algorithms," *2022 International Mobile and Embedded Technology Conference*, IEEE, pp. 121–123, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[62] Mohammad Equebal Hussain, and Rashid Hussain, "Cloud Security as a Service Using Data Loss Prevention: Challenges and Solution," *Internet of Things and Connected Technologies*, Lecture Notes in Networks and Systems, Cham: Springer International Publishing, vol. 340, pp. 98–106, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[63] Yao Zhao, Zhenjiang Zhang, and Jian Li, "A Secure Edge-Cloud Computing Framework for IoT Applications," *Smart Grid and Internet of Things*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Cham: Springer International Publishing, vol. 354, pp. 70-78, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[64] Abbas Jamalipour, and Sarumathi Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," *IEEE Internet of Things Journal,* vol. 9, no. 12, pp. 9444–9466, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[65] Baraka William Nyamtiga et al., "Blockchain-Based Secure Storage Management with Edge Computing for IoT," *Electronics*, vol. 8, no. 8, p. 828, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[66] Yanqi Zhao et al., "Blockchain-Based Auditable Privacy-Preserving Data Classification for Internet of Things," *IEEE Internet Things Journal*, vol. 9, no. 4, pp. 2468–2484, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[67] Hyunjoo Kim et al., "Design of Network Threat Detection and Classification Based on Machine Learning on Cloud Computing," *Cluster Computing*, vol. 22, no. S1, pp. 2341–2350, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[68] Fatima Salahdine, Zakaria El Mrabet, and Naima Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, pp. 250–255, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[69] P. Velmurugan et al., "An Advanced and Effective Encryption Methodology Used for Modern Iot Security," *Materials Today: Proceedings*, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[70] Sara Afzal et al., "URLdeepDetect: A Deep Learning Approach for Detecting Malicious URLs Using Semantic Vector Models," *Journal of Network and Systems Management*, vol. 29, no. 3, p. 21, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[71] Suman Sansanwal, and Nitin Jain, "Security Attacks in Cloud Computing: A Systematic Review," *2021 Third International Conference on Inventive Research in Computing Applications*, *IEEE,* pp. 501–508, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[72] Ahmed Sallam, Ahmed Refaey, and Abdallah Shami, "On the Security of SDN: A Completed Secure and Scalable Framework Using the Software-Defined Perimeter," *IEEE Access*, vol. 7, pp. 146577–146587, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[73] Azidine Guezzaz et al., "A Distributed Intrusion Detection Approach Based on Machine Leaning Techniques for a Cloud Security," *Intelligent Systems in Big Data, Semantic Web and Machine Learning*, Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, vol. 1344, pp. 85–94, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[74] Ali Muhammad, Muhammad Asad, and Abdul Rehman Javed, "Robust Early Stage Botnet Detection using Machine Learning," *2020 International Conference on Cyber Warfare and Security (ICCWS)*, IEEE, pp. 1–6, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[75] Abdul Rehman Javed et al., "Ensemble Adaboost Classifier for Accurate and Fast Detection of Botnet Attacks in Connected Vehicles," *Emerging Telecommunications Technologies*, vol. 33, no. 10, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[76] Neha Agrawal, and Shashikala Tapaswi, "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3769–3795, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[77] Satish Pokhrel, Robert Abbas, and Bhulok Aryal, "IoT Security: Botnet detection in IoT using Machine Learning," 2021. [CrossRef] [Google Scholar] [Publisher Link]
[78] Abdul Rehman Javed et al., "Alphalogger: Detecting Motion-Based Side-Channel Attack Using Smartphone Keystrokes," *Journal of Ambient Intelligence and Humanized Computing*, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[79] Abdul Rehman Javed et al., "Betalogger: Smartphone Sensor-based Side-channel Attack Detection and Text Inference Using Language Modeling and Dense MultiLayer Neural Network," *ACM Transactions on Asian and Low-Resource Language Information Processing,* vol. 20, no. 5, pp. 1–17, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[80] Md. Ashfakul Islam, and Susan V. Vrbsky, "Transaction Management with Tree-Based Consistency in Cloud Databases," *International Journal of Cloud Computing*, vol. 6, no. 1, pp. 58-78, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[81] Jun Tang et al., "Ensuring Security and Privacy Preservation for Cloud Data Services," *ACM Computing Surveys*, vol. 49, no. 1, pp. 1–39, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[82] Seungwon Shin et al., "Rosemary: A Robust, Secure, and High-performance Network Operating System," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 78–89, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[83] Sudakshina Mandal, and Danish Ali Khan, "A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic," *2020 International Conference on Smart Electronics and Communication*, IEEE, pp. 837–842, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[84] Abdul Rehman Javed, and Zunera Jalil, "Byte-Level Object Identification for Forensic Investigation of Digital Images," in *2020 International Conference on Cyber Warfare and Security (ICCWS)*, IEEE, pp. 1–4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[85] Maryam Hina et al., "SeFACED: Semantic-Based Forensic Analysis and Classification of E-Mail Data Using Deep Learning," *IEEE Access*, vol. 9, pp. 98398–98411, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[86] Abdul Rehman Javed et al., "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU," *IEEE Transactions on Network Science and Engineering,* vol. 8, no. 2, pp. 1456–1466, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[87] Mohit Mittal et al., "Analysis of Security and Energy Efficiency for Shortest Route Discovery in Low-Energy Adaptive Clustering Hierarchy Protocol Using Levenberg-Marquardt Neural Network and Gated Recurrent Unit for Intrusion Detection System," *Emerging Telecommunications Technologies*, vol. 32, no. 6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[88] Abdul Rauf, Riaz Ahmed Shaikh, and Asadullah Shah, "Security and Privacy for IoT and Fog Computing Paradigm," *2018 15th Learning and Technology Conference (L&T)*, IEEE, pp. 96–101, 2018. [CrossRef] [Google Scholar] [Publisher Link]