Journal of Applied Sciences, Information and Computing
Vol. 2, No. 1 (June, 2021)
School of Mathematics and Computing, Kampala International University

ISSN: 1813-3509 https://jasic.kiu.ac.ug

PRIVACY AND SECURITY CONCERNS IN THE ADOPTION OF CLOUD COMPUTING TECHNOLOGY

[1]Muhammad Muhammad Suleiman, [2]Surajo Sa'id, and [3]Rahama Babale Shu'aibu

[1]Department of Home & Rural Economics, School of Rural Technology and Entrepreneurship Development, Kano State Polytechnic, Kano Nigeria muhddkd@gmail.com

[2, 3]Department of Civil Engineering Technology, School of Technology, Kano State Polytechnic, Kano Nigeria [2]saidsurajo@yahoo.com, [3]rahamababale@yahoo.com

Abstract

In the field of computing, data security has always been a serious concern. It becomes considerably more severe in the cloud-computing technology environment because data is stored in several locations around the world. Users' biggest concerns about cloud technology are data privacy protection. Privacy and security protection are becoming more crucial for the future growth of cloud computing technology in government, industry, and business, even though numerous techniques on cloud computing themes have been researched in both academics and industries. In the cloud architecture, data security and privacy protection concern both hardware and software. This research will examine various security strategies, as well as problems from both software and hardware perspectives, for securing data in the cloud, to improve data security and privacy control in a reliable cloud environment. The article examines the most important security and privacy concerns surrounding cloud computing as they pertain to outsourcing elements of an organization's computing environment. It highlights areas of concern that require extra attention and offers the underlying information needed to make informed security decisions.

Keywords: Cloud Computing, Data Security and Privacy, Elasticity, Ubiquitous, NIST

1. Introduction

Cloud computing is a rapidly growing paradigm, but its unique characteristics heighten security and privacy concerns. The challenges and solutions to establishing a secure cloud computing environment are discussed in this article (Takabi and Joshi 2010). Although several researchers have attempted to describe cloud computing, there is currently no one, widely accepted definition (Takabi and Joshi 2010). Cloud computing encompasses both the applications that are supplied as services via the Internet as well as the hardware and software in the datacentres that supply such services (Takabi and Joshi 2010). There are four basic cloud delivery models, as drawn by NIST, Badger et al., 2011 cited in (Sen 2016), (Janseip 2015), Depending on who is providing cloud services. Cloud computing has been dubbed the "next generation" of computer paradigms. Both programmes and resources are supplied as services over the Internet in the cloud computing environment (Sun et al. 2014a), (Al-jaberi, Mohamed, and Ain 2015). Cloud computing is a set of hardware and software resources in data centres that deliver a variety of services across a network or the Internet to meet the needs of users (Takabi and Joshi 2010).

Cloud computing is a relatively new technology that allows customers to store and access computing resources and data over the Internet rather than from an expensive local hard disc. It helps to improve storage capacity by allowing customers to store their data in many cloud services, as well as save costs by eliminating the need to acquire an expensive machine with greater memory (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Al-jaberi et al. 2015). Cloud computing, according to the United States National Institute of Standards and Technology (NIST), is a technology that allows for ubiquitous, easy, on-demand network access to a shared pool of programmable computing resources (e.g., servers, networks, applications, storage, and services) that may be supplied and removed quickly with little administration work or contact from service providers (Sen 2016), (Sun et al. 2014a), (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Janseip 2015). While consumers are reaping the benefits of cloud computing, many are unaware that numerous hazards might result in significant financial loss. The majority of them had no idea how their cloud service provider managed their data or where it was stored (An, Y. Z. Zaaba, Z. F. Samsudin 2016). When consumers choose to use a cloud-computing service, they are entrusting their confidential data to a third party who assists them in storing and backing up their data or resources. Security specialists may pose questions like "Do you genuinely think the data is safe and secure when it is managed by a third party?" based on this. Moreover, "Do you have faith in the cloud service you use?" Because there is a lack of understanding while consumers are using the cloud service supplied by the cloud service provider, security risks and obstacles develop (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Virat, Molugu Surya Bindu, S . M Aishwarya, B. Dhanush, B. N. Kounte 2018), (Almarabeh and Majdalawi 2019).

Cloud computing can be thought of as a new computing typology that can provide on-demand services at a low cost. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) are the three well-known and widely used service models in the cloud paradigm (Al-jaberi et al. 2015). A cloud service provider delivers software with associated data, which consumers can access via web browsers (Al-jaberi et al. 2015). PaaS is a service model in which a service provider provides consumers with a set of software programmes that can accomplish specified tasks. In an IaaS, the cloud service provider provides virtual machines and storage to users to help them increase their business capabilities (Sun et al. 2014a), (Sen 2016), (Al-jaberi et al. 2015).

In IT, data security has always been a big concern. Because data is distributed across multiple machines and storage devices, including servers, PCs, and other mobile devices such as wireless sensor networks and smartphones, data security becomes especially important in the cloud-computing environment. Cloud computing data security is more difficult than data security in traditional information systems. To encourage users and businesses to utilise cloud computing, users' security concerns must first be addressed for the cloud environment to be trusted. The creation of a trustworthy atmosphere is a must if people are to have faith in such technologies (Sun et al. 2014a).

The functions of cloud computing are examined first before the data security challenges are highlighted. On-demand service is another term for cloud computing. A cloud service provider provides and manages services in the cloud-computing environment. The cloud provider makes all services available over the Internet, while end-users use the services to meet their business needs and then pay the service provider appropriately (Sun et al. 2014a), (Almarabeh and Majdalawi 2019).

Data and networking storage are the two primary types of functions provided by the cloud-computing environment. Consumers of cloud services do not need anything in the cloud-computing environment; they can access their data and complete their computer chores just by connecting to the Internet. Clients have no idea where the data is stored or which computers are performing the computations during data access and processing (Sun et al. 2014a).

When it comes to data storage, data safety and security are the most important components in winning user trust and successfully using cloud technologies. In the sphere of cloud computing research, several data protection and security solutions have been presented (Sun et al. 2014a). Data protection techniques, on the other hand, need to be improved further. Cloud computing services are available across the full computing spectrum. Nowadays, organisations and businesses are relocating and expanding their operations by utilising cloud computing to reduce costs. This can help free up additional personnel to focus on strategic differentiation and make the corporate division of labour more obvious (Sun et al. 2014a). The cloud is growing continuously because it could provide high-performance computational services at cheaper rates. Famous IT On the Internet, firms including Microsoft (http://azura.microsoft.com), Amazon (http://amazon.com), Google (https://cloud.google.com), and Rackspace (http://rackspace.com), have offered cloud services (Sun et al. 2014a), (Muthulakshmi and Venkatesulu 2019), (Sharma, Vaidya, and Khan 2013).

Cloud computing can save an organisation time and money, but trusting the system is more important because the real asset of any organisation is its data, which it shares in the cloud to access the services it requires by storing it either directly in a relational database or indirectly in a relational database through an application. When it comes to trusting the system, cloud computing has many characteristics that require specific consideration. The data protection and prevention strategies utilised in the system determine the system's overall trustworthiness(Sun et al. 2014b). Researchers have tested and introduced a variety of tools and approaches for data security and prevention to gain and remove the trust barrier, but there are still gaps that need to be filled by making these techniques better and effective (Sun et al. 2014a). There are many different interpretations of security. Confidentiality, the prohibition of illegal disclosure of information, integrity, the prevention of unlawful change or deletion of information, and availability, the prevention of unauthorised withholding of information, are all aspects of security (Sun et al. 2014a), (Sun et al. 2014b).

Resource security, resource management, and resource monitoring are all key concerns in cloud computing. There are now no standard norms and standards for deploying applications in the cloud, and standardisation control in the cloud is lacking. Numerous unique strategies have been created and applied in the cloud; nevertheless, due to the dynamic nature of the cloud environment, these techniques fall short of assuring complete security. In this paper, the fundamental concerns of data security, governance, and management with relation to cloud computing control cited in (Sun et al. 2014a). Sun et al. cited in (Sun et al. 2014a) The key security, privacy, and trust challenges in the current cloud computing environment have been emphasised, assisting users in recognising the tangible and intangible hazards associated with its use. Security, privacy, and trust, according to the authors, are three significant potential risks in cloud computing. In the current era of the long-awaited idea of computing as a utility, security is crucial. Safety methods, cloud server monitoring or tracing, data confidentiality, and avoiding malevolent insiders' illicit actions and service hijacking are the four subcategories (Sun et al. 2014a).

Concisely, data privacy, data protection, data availability, data location, and secure transmission are the most important challenges in cloud data security. Threats, data loss, service disruption, outside malicious assaults, and multitenancy difficulties are among the security challenges in the cloud (Sun et al. 2014a). Chen and Zhao cited in (Sun et al. 2014a) looked at privacy and data security challenges in cloud computing, focusing on privacy protection, data separation, and cloud security. Data security concerns are mostly at the SPI (SaaS, PaaS, and IaaS) level, and data sharing is a major barrier in cloud computing. We will examine several security techniques and challenges for data storage privacy and security protections in the cloud computing environment in this study (Chen and Zhao 2012), (Sinjilawi, AL-Nabhan, and Abu-Shanab 2014).

2. Related Work

The following categories accounted for the vast majority of the examined research articles (Shirazi and Iqbal 2017);

a. Cloud threats and vulnerabilities

b. Cloud privacy, compliance, audit, legal, and trust issues

c. Organizational challenges in implementing a cloud solution

d. Concerns and challenges around cloud security are addressed with solutions and recommendations.

A survey of various connected literature is provided below.

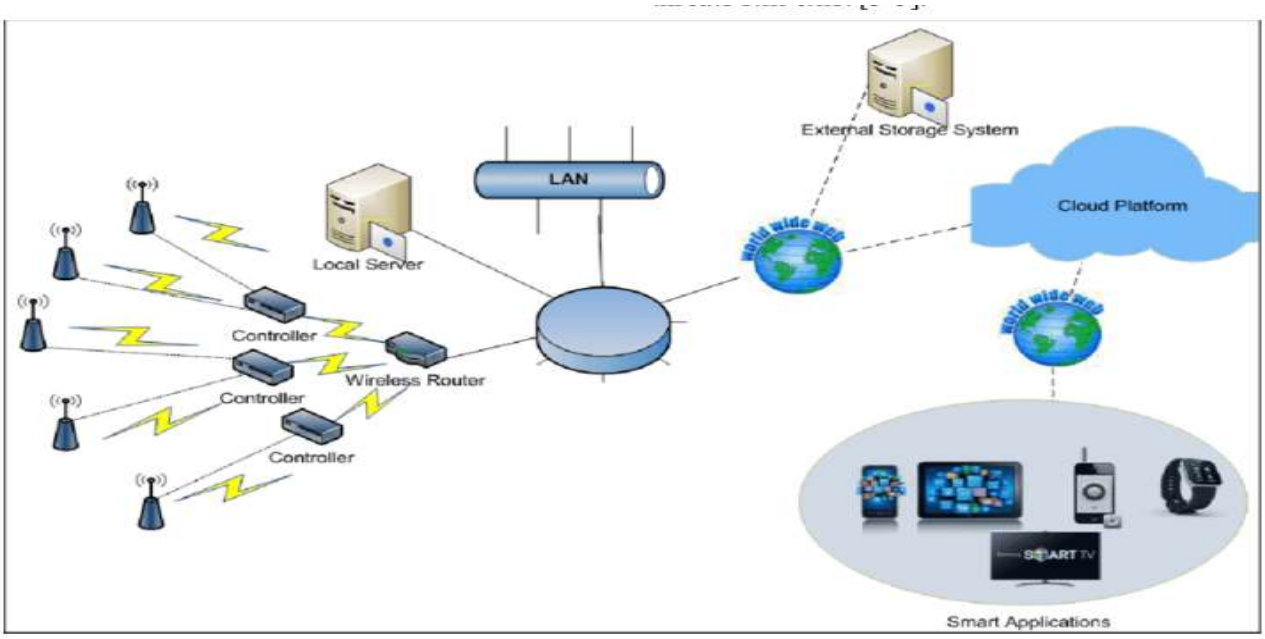
DiaaSalama et al cited in (Muthulakshmi and Venkatesulu 2019) presented a new hybrid cryptography technique This design incorporates both symmetric and asymmetric algorithms, such as (AES and Blowfish). The key objective of this combination is to raise the level of security. In the encryption and decryption process, the MD5 hashing function is employed to hash the key, allowing several persons to process at the same time. Acqueela G Palathingal et al cited in (Muthulakshmi and Venkatesulu 2019) proposed combining encryption and steganography technologies to improve cloud storage security. The idea behind this method is to encrypt data and store it behind graphics. It is stored in the cloud as an image, and from the attacker's perspective, it is a picture since the data is protected. The image was downloaded by the authenticated user, who then decrypted the file with the provided key to obtain the original data behind the image cited in (Muthulakshmi and Venkatesulu 2019).

Mohammad et al cited in (Muthulakshmi and Venkatesulu 2019) Data Encryption and Decryption Using K-NN Machine Learning was proposed. The author focused his efforts in this paper on reducing the time and power necessary for encryption and decryption. Initially, the author divides the cloud-stored data into typical sensitive and very sensitive categories. The user receives authentication based on the sensitive level. The AES-256 algorithm is utilised for very sensitive data, and the RSA (Rivest Shamir Adleman) technique is used to encrypt the key of AES 256. The AES (advanced encryption standard)-192 algorithm is used for normal sensitive data (Muthulakshmi and Venkatesulu 2019).

DhuratëHyseni et al cited in (Muthulakshmi and Venkatesulu 2019) In Cloud Computing, an advanced model to Improve the Safety of Sensitive Data was proposed. The method is primarily intended for businesses and organisations. This solution includes key management and access rights systems that are both efficient. It is segmented before encryption, and the combination of decryption and correction yields a successful result. The attacker fails to join all of the segmented files in this case (Muthulakshmi and Venkatesulu 2019). Hitesh Marwaha & Rajeshwar Singh et al cited in (Muthulakshmi and Venkatesulu 2019) Data Sanitization and AES based on MAC addresses were proposed. This procedure is based on locating sensitive data before sending it to the cloud and using a mac address dependant AES technique for non-sensitive data. Sanitization does not show sensitive data as it is because of this mathematical approach to data. That is, it deceives the attackers into believing it is non-sensitive data cited in (Muthulakshmi and Venkatesulu 2019).

3. The Concept of Cloud Computing

Cloud computing is a new commercial infrastructure paradigm that promises to decrease or eliminate the need for high-cost hardware, software, and network infrastructures to be maintained in-house. It also lowers or eliminates the expensive expense of hiring technical personnel to sustain these infrastructures and run in-house IT solutions. Cloud computing has quickly evolved from a widely debated concept with many ambiguous concepts and implications to an emerging computing paradigm that allows numerous services to be supplied to interested users at lower costs and bigger profits (Al-jaberi et al. 2015), (Chen and Zhao 2012). As a result, a formal definition and description of Cloud Computing and its needs must be established (Al-jaberi et al. 2015), (Sharma et al. 2013), (Sinjilawi et al. 2014).



Source: (Muthulakshmi and Venkatesulu 2019): **Basic Architecture of Cloud Computing**

Cloud computing and resource sharing are both beneficial to small and medium-sized businesses. Small businesses do not need to purchase all of the services. They use it for their needs and pay for it on a per-use basis. It is well known in the business for providing low-cost, dependable services. It is currently used in important fields such as e-transactions, e-commerce, e-billing, e-banking, and e-mail. Due to the growing number of capabilities, a large number of users are turning to cloud computing as a key component of their organisation. This increases the amount of network traffic between users and cloud servers. Online data transfer is the most important requirement for these services. Third-party service providers are quietly increasing in the business (Sharma et al. 2013), (Sinjilawi et al. 2014). This raises security and privacy concerns among users, particularly in the case of data leakage or loss. The majority of clients store their critical data in cloud storage, which provides the highest level of protection, yet various dangers still exist (Muthulakshmi and Venkatesulu 2019), (Sharma et al. 2013), (Shirazi and Iqbal 2017).

Cloud computing is defined as "a collection of hardware and network resources that pool the computing power of several computers to deliver a variety of web-based applications." “Cloud computing is a model for enabling convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction,” according to the US National Institute of Standards and Technology (NIST) (Takabi and Joshi 2010), (Chen and Zhao 2012). Effective cloud computing technology in an enterprise can result in higher-quality and more efficient apps and services, as well as improved levels of end-user satisfaction (Takabi and Joshi 2010), (Chen and Zhao 2012), (Shirazi and Iqbal 2017), (Suleiman et al. 2020), (Sharma et al. 2013).

4. Essential Characteristics of Cloud Computing

According to NIST, distributed computing has five distinct features, which are listed below:

a. **Measured Service**: Cloud frameworks gives pay as scrutinize administration, which screens and control asset utilization to give straightforwardness to both client and specialist co-op (Suleiman et al. 2020).

b. **Broad Network Access**: Any gadget, for example, cell phones, PC, workstations, and so forth can be utilized to get to the assets accessible over the web (Suleiman et al. 2020).

c. **On-demand Self-Service**: A cloud's endorser can get to assets, for example, registering abilities, stockpiling, and so on whenever required without a need for specialist co-op (Suleiman et al. 2020).

d. **Resource Pooling**: Computing assets can be gotten to by more than each client in turn utilizing a multitenant design. In any case, clients are inexperienced with the specific area of the gave asset however on account of a more significant level of deliberation, for example, the datacentre area may be determined (Suleiman et al. 2020), (Sharma et al. 2013)

e. **Rapid Elasticity**: The administrations of distributed computing are flexible to the point that one can include assets when required and discharge them once they finish. Furthermore, assets are open to clients in boundless amounts whenever (Suleiman et al. 2020), (Sharma et al. 2013).

5. Cloud Computing Application, Security and Privacy Issues

Understanding cloud computing's security and privacy threats, as well as providing efficient and effective solutions, is vital to its success. Although cloud computing allows users to minimise start-up expenses, lower operational costs, and boost agility by obtaining services and infrastructure resources as needed, their unique architectural features also create many security and privacy hitches (Takabi and Joshi 2010), (Sharma et al. 2013).

Threats, vulnerabilities, and risks, while sometimes misunderstood, are almost a ubiquitous phenomenon in Cloud Computing services and computation processes. These concepts must be defined as carefully as possible, keeping in mind that they are connected. Bhowmik cited in (Bhadra 2020), (Masud, Yong, and Huang 2012) describes the concepts as follows. A threat is defined as an incident that has the potential to harm a system. It can jeopardise the system's dependability by jeopardising the confidentiality, availability, and integrity of data stored in the system. Threats can be malicious, such as the purposeful change of sensitive data, or they can be unintentional, such as the deletion of a file or a problem caused by an incorrect calculation. Vulnerability is defined as "certain vulnerabilities or defects in a system (hardware, software, or process) that a threat could exploit to harm the system." It refers to security defects that represent a threat to a system and increase the likelihood of a successful attack. Finally, risk refers to ‘the ability of a threat to exploit vulnerabilities and thereby causing harm to the system. Risk occurs when threat and vulnerability overlap. It is the prospect of a threat to materialize’. Common threats to any computing system are eavesdropping (capturing data packets for sensitive information), fraud (altering data to make an illegitimate gain), theft (stealing trade secret or data financial gain), sabotage (disrupting data integrity, DoS), an external attack (inserting a malicious code or worm) (Masud et al. 2012), (Bhadra 2020). Dahbur describes a countermeasure and proposes an equation for the interrelationship between them: Risk=Vulnerability x Threat x Impact x Likelihood (e.g. strong authentication mechanism, computer antivirus software, or information security awareness). It can be a policy, method, software configuration, or hardware device that removes vulnerability or minimises the possibility that a threat agent will be able to exploit the vulnerability (Shirazi and Iqbal 2017), (Sharma et al. 2013), (Bhadra 2020).

5.1 Application Issues

The cloud service provider should monitor and maintain the cloud regularly to guarantee that it is secure and free of dangerous code that has been uploaded to the cloud by hackers or attackers with the intent of stealing sensitive information or even damage the information of specific users (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

5.2 Cloud Privacy Issues

Cloud privacy is a critical aspect of cloud infrastructure. There are numerous rules and regulations in place to protect data and information privacy (Chandna, Singh, and Choudhary 2020). To ensure the security of the data users saves in their cloud model, the cloud computing service provider must implement their policies. They must ensure that they are aware of who is accessing the data stored in the cloud and that authorised personnel can only maintain the cloud service model. Cloud computing security should be addressed on both the supplier and user sides (Sun et al. 2014a). Users should not tamper with the data of other users, so the cloud service provider should provide a good layer of security protection for them. Cloud computing is a good approach to save money and get additional storage if and only if both the provider and the user take care of security. According to him, legislative change is necessary to secure sensitive data in the cloud because one of the most difficult aspects of cloud computing is ensuring that consumers trust the privacy and security of their data (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Janseip 2015), (Chandna et al. 2020).

5.3 Data Privacy

An individual's or a group's ability to seclude themselves or information about themselves and selectively reveal them is known as privacy. The elements of privacy include (Sun et al. 2014a), (Chen and Zhao 2012), (Chandna et al. 2020).

a. When: a subject may be more anxious about the disclosure of current or future information than information from the past (Sun et al. 2014a), (Chandna et al. 2020).

b. How: While a user may feel at ease if his or her friends can explicitly request his or her information, he or she may not appreciate alerts that are given automatically and regularly (Chandna et al. 2020).

c. Extent: rather than an exact spot, a user's information may be reported as an ambiguous region (Chandna et al. 2020).

End-user context and privacy must be safeguarded and used correctly in trade. Privacy in organisations comprises the implementation of laws, methods, standards, and processes for the management of personally identifiable information (Janseip 2015), (Chandna et al. 2020).

The privacy concerns vary depending on the cloud context and can be categorised into four subcategories (Chandna et al. 2020):

a. How to give consumers control over their data when it's stored and processed in the cloud while avoiding data theft, malicious usage, and illegal resale (Chandna et al. 2020)?

b. How to avoid data loss, leakage, and unauthorised modification or fabrication in a jurisdiction and consistent state, where copying user data to many suitable locations is a common choice (Chandna et al. 2020)?

c. Who is in charge of ensuring that legal obligations for personal information are met (Chandna et al. 2020)?

d. To what extent are cloud subcontractors involved in processing that can be identified, checked, and verified (Chandna et al. 2020)?

6. Data Security and Privacy Challenges

Cybercrime on the internet is not only on the rise, but it is also becoming more sophisticated and targeted (Chen and Zhao 2012), (Younis, Kifayat, and Merabti 2014). Cybercrime knows no borders, and cybercriminals are attacking businesses all around the world for a variety of financial, political, and even personal motives. According to a 2016 data breach research done by IBM and the Ponemon Institute, the average cost of a data breach is $4, with the cost of each stolen record increasing from $154 in 2015 to $158 in 2016 (Shirazi and Iqbal 2017). We have offered some examples of the most well-known data breaches in recent years to highlight the financial, privacy, and social implications of a data breach. The occurrences listed below are only a few of the numerous that occur daily around the world. A data breach's repercussions can have a long-term impact on individuals and businesses. Clients lose faith in organisations that have experienced a data breach, which can lead to a loss of revenue (Chen and Zhao 2012), (Younis et al. 2014). Because so many businesses have begun to move their services to the cloud, hackers have found cloud systems to be an appealing target. As a result, while shifting services to the cloud, businesses need to be extra vigilant about security and privacy (Shirazi and Iqbal 2017), (Virat, Molugu Surya Bindu, S . M Aishwarya, B. Dhanush, B. N. Kounte 2018).

6.1 Cloud Security Issues

Because users can store all of their common, private, or even sensitive data on the cloud, which can be viewed by anyone, anytime, data at rest is a big issue in cloud computing. Data theft is a relatively typical problem that cloud service companies face nowadays (Chen and Zhao 2012). Furthermore, some cloud service providers do not even provide their server due to cost and flexibility. There are also occurrences such as data loss, which can be a major issue for users. For example, the server may be unexpectedly shut down, resulting in data loss for users. Furthermore, data may be damaged or corrupted because of a natural disaster. As a result, one of the security concerns in cloud computing is the physical location of data (Sun et al. 2014a), (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Chen and Zhao 2012).

According to Gartner cited in (Chen and Zhao 2012), users should inquire about seven key safety issues before choosing a cloud vendor: privileged user access, regulatory compliance, data placement, data segregation, recovery, investigative support, and long-term viability. Forrester Research Inc., quoted in (Chen and Zhao 2012), assessed the security and privacy procedures of several of the biggest cloud providers (such as Salesforce.com, Amazon, Google, and Microsoft) in three important areas in 2009. Difficulties of security and privacy, as well as legal and contractual issues. The Cloud Security Alliance (CSA), as cited in (Chen and Zhao 2012), is bringing together solution providers, non-profits, and individuals to discuss existing and future best practices for cloud information assurance. The CSA has identified thirteen security domains for cloud computing cited in (Chen and Zhao 2012).

Subashini and Kavitha cited in (Chen and Zhao 2012) made an investigation of cloud computing security issues from the cloud computing service delivery models (SPI model) and give a detailed analysis and assessment method description for each security issue cited in (Chen and Zhao 2012). Mohamed Al Morsy, John Grundy and Ingo Müller explored the cloud computing security issues from different perspectives, including security issues associated with cloud computing architecture, service delivery models, cloud characteristics and cloud stakeholders cited in (Chen and Zhao 2012). Chen et al cited in (Chen and Zhao 2012) believed that two aspects are to some degree new and essential to the cloud: the complexities of multi-party trust considerations and the ensuing need for mutual auditability. They also point out some new opportunities in cloud computing security cited in (Chen and Zhao 2012), (Sun et al. 2014a), (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

6.2 Cloud Security Threats Issues

There are numerous security concerns with cloud computing, which is now widely employed. According to “The Famous Nine: Cloud Computing Top Threat” by the Cloud Security Alliance (CSA) Kandias et al, referenced in (An, Y. Z. Zaaba, Z. F. Samsudin 2016), there are top nine threats that constitute a serious threat to cloud computing in 2013. The following are the top six threats mentioned in the white paper:

a. Breaches of Data: Users' data stored in the cloud could be significant and sensitive. Unauthorized users may steal data stored in the cloud, posing a risk to the users who are being attacked. It is the most serious threat to cloud computing since hackers or attackers can simply access the data stored in the cloud by users. Many users' sensitive information was kept in the cloud. Customers of cloud services need additionally verify the cloud service providers' quality, dependability, and performance through Service Level Agreements (SLAs) agreed between providers and users.

Khoshkholghi et al cited in (An, Y. Z. Zaaba, Z. F. Samsudin 2016). As a result, data breaches are the most serious issue that clouds computing services confront (Sun et al. 2014a), (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Bhadra 2020).

b. **Inadequate Due Diligence**: Many people don't do enough research on their cloud service providers (CSPs). They didn't even think of doing basic due diligence, including evaluating the CSP's financial health or ascertaining how long the CSP has been in business, according to McDowell, cited in (An, Y. Z. Zaaba, Z. F. Samsudin 2016). Due diligence should not be overlooked because the cloud service provider may not be sufficiently secure and may not be held liable for data taken from the cloud by some hackers (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

c. **Hijacking of User Account**: The user's account has been stolen or hijacked, and hackers may use it to execute malicious and unlawful activities that may harm the user, according to Kiblin (An, Y. Z. Zaaba, Z. F. Samsudin 2016). Hackers could, for example, modify data, present fake information, and eavesdrop on transactions made with the stolen account. Furthermore, no native APIs are utilised for login, and anyone can register as a cloud service user, putting the account at risk of being hacked Kill cited in (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

d. **Denial of Service**: Hackers use this form of attack to flood the cloud service provider's machine or network resources, disrupting users and preventing them from connecting to the network (An, Y. Z. Zaaba, Z. F. Samsudin 2016). Cites Kandias et al. and Kuyoro et al. Furthermore, the user may be harmed as a result of the security vulnerabilities since cloud services may become unavailable to users, and they may not receive what they require promptly (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

e. **Disgruntled or Malicious Employees**: A firm employee could potentially pose a significant threat. They could be the attacker or a hacker's accomplice, with a larger possibility of stealing or manipulating the cloud model's data on purpose. These behaviours expose users' sensitive or confidential data to outsiders, potentially harming the targeted users. Studies by Li et al, cited in (An, Y. Z. Zaaba, Z. F. Samsudin 2016) indicates that hostile insiders of cloud service providers can readily access passwords and other personal data. Malimi's studies (An, Y. Z. Zaaba, Z. F. Samsudin 2016) address the issues of harmful insiders, claiming that they should be researched in two contexts: insider threat in cloud providers (i.e. insider is a malevolent employee working for a cloud provider) and insider threat in cloud outsourcers (i.e. employee of an organisation which sourced its infrastructure to the cloud) (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

f. **Abuse of Cloud Service**: The majority of cloud computing solutions feature a sluggish registration method. Anyone with a valid payment card, for example, can register and use the cloud service right away. As a result, attackers frequently carry out destructive operations by taking advantage of the relative anonymity of cloud computing service registration. Password and key cracking, DDOS attacks, launching dynamic assault points, and hosting malicious material are all future areas of concern (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

g. Threats to cloud-based information assets can differ depending on the cloud delivery models utilised by cloud user organisations. Cloud computing is exposed to several different forms of security vulnerabilities. The Above summarises the dangers to cloud customers as classified by the confidentiality, integrity, and availability (CIA) security model, as well as its applicability to each cloud service delivery architecture. (Sinjilawi et al. 2014), (Suleiman, Muhammad Muhammad Anas, Abubakar Abdurrahman Jafaru 2020).

6.3 Other Cloud Security and Privacy Challenges

a. **Data Replication**: Every company faces this problem. Every day, snapshots and data backups are taken. They were saved to the cloud automatically. Are you aware of where they have been kept and who has access to them? Can you detect and prevent unlawful data copying (Sinjilawi et al. 2014)?

b. **Data Loss:** Loss of data may be disastrous for any company. As virtual data flows between VMs or on the cloud, it is easy to lose or expose it. Are you confident that authorised individuals are accessing your data by established policies? Do you have the authority to ban any user who violates the data usage policies (An, Y. Z. Zaaba, Z. F. Samsudin 2016), [13], (Hassler 2001)?

c. **New Class of Users**: Security, storage, application, and security administrators must work together in cloud computing. They are all in charge of your sensitive business information. As the number of users grows, so does the risk. If one administrator makes a mistake, the entire system's data is in danger (Sun et al. 2014b).

d. **Insecure APIs**: Application Programming Interfaces (API) users should be able to tailor their cloud computing methods. Because of their nature, APIs might pose a threat to cloud security. APIs provide developers with the tools they need to create solutions for integrating their apps with other software. The communication that takes place between applications determines an API's vulnerability. While this may be beneficial to developers and businesses, it raises severe security risks (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

e. **Internal Threat:** This is something you should never forget. You might believe that data is protected on the inside. However, this is one of the most significant challenges that businesses face. Employees can misuse or gain access to financial, customer, and other information by using their access to an organization's cloud-based services (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

7. Mitigations and Best Practices for Cloud Security Issues

Because more people are realising the benefits of cloud computing, it is becoming more popular. It allows the user to easily reduce the size of the operation and save money. However, as the cloud service's adoption rate rises, so do the security concerns and risks, as Mell and Grance cited in (An, Y. Z. Zaaba, Z. F. Samsudin 2016). A few technologies and practices can assist make cloud computing a better option for increasing user storage capacity and securing personal information from unauthorised access. (Hassler 2001).

a. **Vulnerability shielding**
The cloud service provider should improve Patch administration. They should check the vulnerability of their cloud service regularly and always update and maintain it to minimise the number of possible access points and reduce the chance of a hacker attack on the cloud. To ensure that the cloud service supplied is secure and safe, the cloud service provider may deploy an Intrusion Detection System (IDS) (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

b. **Data encryption**
Data encryption is one of the most effective techniques to protect your data while using cloud storage. Because decryption is required before accessing the data, this is the best type of security. This will safeguard data from both service providers and users. You can also enable cloud encryption during the uploading and downloading phases to make it more secure. However, this will impede down data sharing and synchronisation in the cloud platform (Bhadra 2020), (Hassler 2001).

c. **Read your user agreement and Privacy Policy**
If you are new to cloud computing and are not sure which cloud storage to use or how it works, read the user agreement for the service you are considering signing up for. It will be tough to understand at first, and it will tax your patience at times, but you must persevere. User agreements always include important information that can help you understand things more thoroughly (Bhadra 2020), (Suleiman, Muhammad Muhammad Anas, Abubakar Abdurrahman Jafaru 2020), (Hassler 2001).

d. **Access Control**
Allow only those users who have a genuine need for access. Internal users and third-party vendors should only have access to files that are necessary for their work. If necessary, use encryption keys. Make sure to evaluate users and vendors regularly, and add/remove people as needed (An, Y. Z. Zaaba, Z. F. Samsudin 2016), (Shirazi and Iqbal 2017), (Bhadra 2020), (Hassler 2001).

e. **Keep software up to date**
Install any fixes that the seller publishes for the software that runs your device as soon as feasible. Installing these will prevent attackers from exploiting the situation (Suleiman, Muhammad Muhammad Anas, Abubakar Abdurrahman Jafaru 2020).

f. **Facilities for recovery**
According to Sekhar et al cited in (An, Y. Z. Zaaba, Z. F. Samsudin 2016), the cloud service provider should take responsibility for recovering the data of users if there is any data loss owing to specific circumstances. Cloud service providers should ensure that they have enough backups and can retrieve and recover users' data, which could be costly. To ensure data recovery, cloud service providers might additionally employ the following methods (Sen 2016):

- In the event of a disaster, the quickest disc technology will be used to replicate data that is in jeopardy. ii. Changing the threshold for unclean pages (Sen 2016).
- Prediction and replacement of potentially dangerous devices (Sen 2016).
-

g. **Enterprise infrastructure**
The data that the user wants to keep in the cloud infrastructure must be safeguarded. Users should be able to install and configure hardware components such as firewalls, routers, servers, and proxy servers using the cloud service provider's infrastructure (Sen 2016), (An, Y. Z. Zaaba, Z. F. Samsudin 2016).

8. Conclusion

Cloud computing is a model for improving data management speed and flexibility while lowering costs. It is true that cloud computing has provided us with numerous benefits and is becoming increasingly popular in recent years. Many multinational corporations have begun to use cloud services in their operations. While cloud computing is becoming increasingly popular, security has become a major worry for anyone who uses cloud services. There is a lot of security that arises regularly, and the security model of the cloud service provided is improving. Despite the increasing use of the cloud service, the user should use the cloud service provided wisely in a way that always ensures good security practices so that this technology has the potential to bring the information technology to the next level.

Acknowledgment
First of all, We share our heartfelt debt of appreciation to the Almighty Allah, who always helps us in our endeavours. We would like to thank our teachers for their support and encouragement. We acknowledge the effort of JASIC, KIU for making our work published for the benefits of all.

References

Al-jaberi, Mariam, Nader Mohamed, and Al Ain. 2015. "E-Commerce Cloud : Opportunities and Challenges."

Almarabeh, Tamara, and Yousef Kh Majdalawi. 2019. "Cloud Computing of E-Commerce." *Modern Applied Science* 13(1).

An, Y. Z. Zaaba, Z. F. Samsudin, N. F. 2016. "Reviews on Security Issues and Challenges in Cloud Computing." *International Engineering Research and Innovation Symposium (IRIS)* 160.

Bhadra, Sompurna. 2020. "CLOUD COMPUTING THREATS AND RISKS: UNCERTAINTY AND UNCONROLLABILITY IN THE RISK SOCETY." *Journal of Emerging Technologies and Innovative Research (JETIR)* 7(2):1047–70.

Chandna, Anurag, Yashveer Singh, and Sagar Choudhary. 2020. "Legacy and Privacy Issues in Cloud Computing." *International Research Journal of Engineering and Technology (IRJET)* 07(01):2064–68.

Chen, Deyan, and Hong Zhao. 2012. "Data Security and Privacy Protection Issues in Cloud Computing." Pp. 647–51 in *2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*. Vol. 1.

Hassler, Vesna. 2001. *Security Fundamentals for E-Commerce*. edited by P. Moore.

https://www.narga.net/security-privacy-issues-cloud-computing/ Retrieved 12/05/2021

https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/ Retrieved 11/95/2020

https://autome.me/top-most-cloud-computing-privacy-and-security-issues/ Retrieved 02/01/2021

https://www.apogaeis.com/blog/data-privacy-security-in-cloud-computing/ Retrieved 07/02/2021

https://privacyrights.org/resources/privacy-implications-cloud-computing Retrieved 21/12/2020

Janseip, A. Wayne. 2015. "Cloud Hooks: Security and Privacy Issues in Cloud Computing." *NIST* 6–10.

Masud, Anwar Hossain, Jianming Yong, and Xiaodi Huang. 2012. "Cloud Computing for Higher Education: A Roadmap." Pp. 552–57 in *2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2012*.

Muthulakshmi, B., and M. V. Venkatesulu. 2019. "Privacy and Security Aware Cloud Storage Using Double Cryptography Method." *International Journal of Recent Technology and Engineering (IJRTE)* 8(4):577–82.

Sen, Jaydip. 2016. "Security and Privacy Issues in Cloud Computing." *Architectures and Protocols for Secure Information Technology Infrastructures* (May):1–45.

Sharma, Divya, Preeti Vaidya, and Oves Khan. 2013. "Survey on Security Issues in Cloud Computing." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 3(1):83–87.

Shirazi, Farid, and Amna Iqbal. 2017. "Cloud Computing Security and Privacy: An Empirical Study." *Springer International Publishing AG* (December):534–549.

Sinjilawi, Yousef K., Mohammad Q. AL-Nabhan, and Emad A. Abu-Shanab. 2014. "Addressing Security and Privacy Issues in Cloud Computing." *Journal of Emerging Technologies in Web Intelligence* 6(2):192–99.

Suleiman, Muhammad Muhammad Anas, Abubakar Abdurrahman Jafaru, Aminu. 2020. "The Concept and Scope of Cybercrimes." *International Journal of Research* 7(6):118–29.

Suleiman, Muhammad Muhammad, Zakari Idris Matinja, Zainab Musa Aliyu, and Zainab Abdulkadir. 2020. "Cloud Computing Is An Integral Tool For E-Government: Challenges And Prospects." *Mukt Shabd Journal* IX(VI):2824–36.

Sun, Yunchuan, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. 2014a. "Data Security and Privacy in Cloud Computing." *International Journal of Distributed Sensor Networks* 2014.

Sun, Yunchuan, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. 2014b. "Data Security and Privacy in Cloud Computing." *International Journal OfDistributed Sensor Networks* 2014.

Takabi, Daniel, and James B. D. Joshi. 2010. "Security and Privacy Challenges in Cloud Computing Environments." *EEE Xplore Security and Privacy Magazine, IEEE COMPUTER AND RELIABILITY SOCIETIES.*

Virat, Molugu Surya Bindu, S . M Aishwarya, B.

Dhanush, B. N. Kounte, R. Manjunnth. 2018. “Security and Privacy Challenges in Internet of Things.” in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018) IEEE Conference Record: # 42666; IEEE Xplore*.

Younis, Younis A., Kashif Kifayat, and Madjid Merabti. 2014. “Cloud Computing Security & Privacy Challenges.” in *The 15th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and BroadcastingAt: Liverpool*.

About The Corresponding Author

The author obtained a Nigerian Certificate in Education (N.C.E) Business Education (Secretarial Education) in 2004 from Federal College of Education (Technical), Bichi, International Diploma (Information Communication Technology) and International Advanced Diploma (Computer and Networks Security) in 2012 and 2013 from Informatics Academy, Singapore. He has also undergone Bachelor of Education (Business Education) from Ahmadu Bello University, Zaria and Bachelor of Information Technology from International University of East Africa, Kampala, Uganda in 2012 and 2014 respectively; the author also obtained a Master of Science in Information Technology from Lovely Professional University, Phagwara, India in 2020.

He is a professional member of several professional organizations including the Teachers' Registration Council of Nigeria (TRCN), Association of Business Educators of Nigeria (ABEN), Business Educators Association in Vocational Education (BEAVE) Indian Science Congress Association, Kolkata (ISCA). Among the hobbies of the author are ICT, Education, Data Mining, Information Security, Grid Computing and Cloud Computing.

The author published more than 22 articles in many reputable journals and presented papers in more than 18 conferences and workshops both locally and globally. The author has adequate skill in many citations, referencing and data analysis tools including Mendeley, SPSS, Spreadsheet, Latex, Rapidminer, Weka and plagiarism minimizing/fixing tools like Turnitin, Grammarly, and Spoilbot etc. He is currently a Lecturer I in the Department of Home and Rural Economics, School of Rural Technology and Entrepreneurship Development, Rano, Kano State Polytechnic, Kano State - Nigeria.