IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A Systematic Literature Review on Security and Privacy Challenges in Cloud Computing Networks

Eluwa Jumoke, Ogbeide Oluwafunmilayo
School of Science, Engineering and Environment, The University of Salford, United Kingdom.

Abstract *- The phrase "cloud computing" has garnered lots of attention because of the rising demand in recent years. Customers' need for computing resources such as servers, networks, services, storage, and applications are being met by cloud service providers as they provide the option to rent these resources rather than purchase them. To give their consumers access to the cloud, many well-known businesses, Amazon, Google, and Microsoft, among others, have begun to enhance their offerings by integrating cloud computing technology. It is true there are many advantages to employing a cloud-based system, however its special features worsen security and privacy problems. The current security and privacy solutions require a critical reevaluation in terms of their suitability for clouds, even though cloud security and privacy services can be customized and managed by expert groups who might be able to deliver effective security management and threat assessment. It is urgently necessary to implement more modern and cutting-edge technologies to realize the full benefits of cloud computing. As a result, additional research is needed to understand these problems and solutions to reduce the dangers. Hence, this article focuses on security and privacy concerns that cloud users, cloud service providers, and data owners confront in cloud computing networks and the solutions for creating a safe cloud computing environment.*

Keywords — Cloud Computing, Security, Data Protection, Privacy.

1.0. INTRODUCTION

In traditional computer infrastructure, large areas and enormous amounts of power are required in the processing of transactions. However, in recent years, smaller more powerful computers have replaced huge computers and the demand for data as well as the number of online users have both surpassed all predictions. Additionally, it is hard for traditional computing to access data at any time or place thereby necessitating the use of off-site storage devices for data storage. Furthermore, the growth in the number of Internet users worldwide has constantly expanded, volume of users on networking websites, social networks, and multimedia broadcasts has outgrown the level for conventional data processing. As a result, a novel concept known as cloud computing has been developed [1].

The National Institute of Standards and Technology (NIST) has defined cloud computing as "a model that enables convenient, ubiquitous, on-demand access to resources that can be easily provisioned through various types of interaction with service providers" [2]. Cloud computing provides Infrastructure-as-a-Service (IaaS), Software-as-a- Service (SaaS) and Platform-as-a-Service (PaaS) as three distinct service delivery models. IaaS enables customers to develop and run applications on a variety of virtualized infrastructure components offered by the cloud provider, such as storage and virtual machines (VMs). The program will finally run on the virtual machine and operating system. Trusting the VM image, securing the hosts, and safeguarding communications between the hosts are a few of the critical IaaS challenges. For SaaS, application software is enabled and made available as on-demand services by cloud service providers. It is challenging to securely compile and guarantee that the information processed by these compiled services is successfully protected because clients purchase and use software components from numerous sources. PaaS enables development environments to access and use more resources when creating applications. These programming settings influence the application's architecture, for instance by limiting the services an application can request from the operating system [1].

Despite the popularity of cloud computing in both academia and commerce, the paradigm is still in development. It aims to integrate the economic value model with the development of numerous modern techniques and computing technologies, such as applications, distributed services, and information infrastructures like storage, networks, and computer resource pools [2]. Cloud computing is a fundamental paradigm that can considerably lower costs by streamlining procedures and boosting operational and financial efficiency. Additionally, it may greatly enhance cooperation, scalability, and flexibility, as well as aiding a fully global computing paradigm across the Internet infrastructure. However, if suitable security and privacy solutions are not developed, this potentially revolutionary computing paradigm will possibly fail catastrophically. In addition to financial losses, businesses may face legal repercussions and brand harm because of a security breach. For example, the Equifax data breach of 2017 resulted in $700 million in compensation and irreparable harm to the company's reputation [4]. Security and privacy concerns are the key factors holding back cloud adoption, according to various surveys of potential users [3]. Therefore, a service provider in the cloud has a big obligation to handle any threats and attacks that it or its clients might experience. Hence, a thorough understanding of security and privacy concerns and the creation of feasible solutions are crucial for the success of cloud computing implementation and adoption.

2.0. BACKGROUND

All techniques intended to safeguard, correct, and make sure that data in computer systems are secured against a variety of risks are categorized as security [8]. Security services such as integrity, availability, confidentiality, non-repudiation, and authentication aid in the protection of computer networks and information systems. Information is kept private so that it cannot be shared with or utilized by groups, people, or other procedures that are not allowed to. Throughout transmission, data should be sent and received without being viewed by unauthorized parties. Encryption is a dependable method to achieve confidentiality. Integrity ensures that the information a legitimate person receives is accurate and identical to what was supplied, it guarantees that the data has not been altered by a third party, whether purposefully or unintentionally. The connection is severed, and the transmission of the incorrect information is halted in the event of an incursion. Accessibility guarantees that data is accessible and useful upon request from an authorized organization and guarantees that services are offered to authorized users. A system, for instance, can no longer carry data if it is the target of a distributed denial of service (DDoS) assault. Authentication verifies the sender and recipient of information's identities. Integrity and confidentiality of information are crucial when the sender's and receiver's identities have been correctly established. The principle of non-repudiation guarantees that neither the sender nor the recipient may retract their actions. Repudiation can have two different forms: by the source and by the destination [8]. Both the sender and the recipient cannot contest the message's delivery in the first scenario, and neither can they do so in the second. Therefore, to achieve security and privacy in cloud computing networks, these security services must be taken into cognizance.

2.1. Prior research

In surveys published over the last ten years, the difficulties with cloud computing security have received a lot of attention. A taxonomy of assaults on virtualized systems has been presented in the work of [9] in terms of the source, the targets, and the targets at various levels of the attackers. At several levels, including hardware, operating system, and application, it demonstrates the rise in dangers in virtualized systems. [10] provides a study on security issues with cloud computing that covered issues with data placement, storage, security, availability, and integrity. However, the writers did not outline potential solutions; they merely discussed security issues. In addition to highlighting several data security issues in cloud computing, [11] also put forth a solution to security issues in multi-tenant environments. The report only addresses issues with data security and offers privacy and data protection solutions. [12] presents review research on the privacy and security concerns with cloud computing. The report lists many types of cloud vulnerabilities and categorizes numerous known security concerns and assaults. This evaluation process also discusses potential future security issues and examined the weaknesses of the existing remedies. [13] highlights the security risks related to cloud computing. By examining alternative security models and technologies, this article also discussed the primary security concerns of both suppliers and end users regarding cloud computing. The shielding data technique, which aims to protect data from cloud infrastructure providers, is one of the significant research subjects that [14] highlights in his work. Additionally, the paper provides a method for converting browser keys that enables software- as-a-service applications to provide secrecy services. Based on prior research, this study observed that most authors discussed the security and privacy challenges in cloud computing without considering the cloud computing applications focused on security that can be employed by Cloud Service Providers (CSPs) and cloud clients to secure information and information assets.

2.2. Research goals

Since many of the cloud-related technologies have developed recently, security risks have increased, and new challenges have surfaced. Therefore, rigorous research is necessary, along with the recognition of potential issues and the creation of novel solutions. To achieve this goal, this study aims to answer the following research questions (RQs). RQ1: What are the security challenges related to CSPs in cloud computing networks?
RQ2: What are the security challenges related to cloud clients in cloud computing networks?
RQ3: What are the existing solutions related to security challenges in cloud computing networks?
RQ4: What are the latest cloud computing applications focused on security?
RQ5: How is cloud computing used to improve cyber security?
RQ6: What access control methods are available in cloud computing?

2.3. Contributions and layout

Through a thorough analysis of the literature, this article adds to the body of knowledge by outlining the security and privacy concerns that cloud users, cloud service providers, and data owners face as well as offering solutions for creating a dependable cloud computing environment. This study examines the challenges with security and privacy networks for cloud computing thus: Security issues with cloud clients were covered in Section I, Section II explores Security Challenges Associated with CSPs, Section III addresses Privacy Concerns Associated with Cloud Computing, Section IV addresses the cloud computing applications focused on security, Section V is centered on how cloud computing can be used to improve cybersecurity, Section VI discusses the access control methods available in cloud computing and Section VII is centered on existing solutions.

3.0. RESEARCH METHODOLOGY

This study has employed a systematic and in-depth analysis of significant peer-reviewed literature to evaluate the many aspects of cloud computing security and privacy challenges. Various keyword combinations were sent to database search engines. Among the keywords that were filtered were "cloud computing network problems," "cloud computing network security," "cloud computing privacy," "cloud computing issues," and "cloud computing issues solutions". Because of how successfully they described concepts, this approach was adopted. In the first stage, the search word in Google Scholar alerts was clarified. To select which papers to analyze, a set of inclusion and exclusion criteria had to be used. The second step involves expanding the search to include new research databases. To guarantee consistency in the results, the same keywords were used across all databases, and a 13-year window, from 2010 through 2023, was chosen (Table 1).

3.1. Selection of primary studies

There were three processes in the selection of primary research: identification, screening, and inclusion and exclusion. The identification and gathering of bibliometric data comprised stage 1. The entire result was then screened to decide which documents may be taken into consideration based on the study topics deemed vital and relevant. The selection of the articles for analysis was aided by inclusion.

3.2. Inclusion and exclusion criteria

ACM Digital Library, Springer, MDPI, Google Scholar, IEEE Xplore Digital Library, Springer, Elsevier / Science Direct, and other platforms, or databases were used for the search. The search engines produced a total of 96 articles. After eliminating duplicates based on titles and authors, we did an article search based on relevancy of the abstract and keywords.

3.3 Selection results

Following quality screening, 52 papers representing 54.17% of the total papers that were the most relevant to this research were selected, while 41 papers representing 45.83% of the total papers were eliminated.

3.4 Quality assessment

Table 1: Keywords and period

Keywords	Period
Cloud Computing Privacy Cloud Computing Network Challenges Issues in Cloud computing networks	2010 - 2023

The search returned in total 96 potentially useful documents. The result extracted Elsevier (40) are numerically superior to the other databases namely Springer (23), Taylor & Francis (19), MDPI (10), Copernicus (11), John Wiley & Sons (11), (Table 2).

3.5. Data extraction

Table 2: Total results of articles on electronic database

Documents Review Carried out in 2023

Source of Articles	Results
Elsevier	40
Springer	23
Taylor & Francis	19
MDPI	10
Copernicus	11
John Wiley & Sons	11

3.6. Data analysis

The result underlines that most of the documents are articles (63.54%) and subsequently conference papers (36.46%). All the document types are filled in Table 3.

Table 3. Distribution of document types

Documents Review Carried out in 2023

Document Types	Records	Contribute %
Article	61	63.54
Conference Paper	12	12.50
Review	7	7.91
Proceedings Paper	7	7.29
Book Chapter	5	5.20
Editorial	2	2.08
Book	2	2.08

I. SECURITY CHALLENGES RELATED TO CLOUD CLIENTS

- Data security and privacy: Customer data is exposed to hazards of data integrity, confidentiality, and availability [15] when a single-tenant system is converted to a multi-tenant one.
- Customers' rights and access control: Customers are accountable for maintaining the security of login and other sensitive information they use while the CSP alone has the responsibility of limiting access to the network service [16]. The CSP must choose the means to handle credentials, assign responsibility of upholding data security, and how to reveal information about people handling customers' information.
- Data Loss: Because sensitive information and data may be stored and retrieved by several users, data loss is a serious risk in cloud computing networks [17]. Data loss occurs often in cloud computing due to cyberattacks, human mistakes, and natural disasters [18]. The effects of data loss must be minimized using effective data backup and recovery procedures.
- Policies and Service Level Agreements (SLAs): Before implementing cloud computing, service providers and clients should have a comprehensive understanding of SLA and rules. Robust cloud computing security policies should address crucial

cloud computing security issues such as access control, confidentiality, authentication, integrity, communication security, identification, data protection and accountability [18].

- Long-term viability: Consumers of CSPs ought to take into consideration the prospect of their CSP being a party to a merger or acquisition, since this has the potential to influence the data consumers store in the cloud. Customers can consider incorporating clauses in their SLA with the CSP that specify the customer's requirements and expectations regarding data security to reduce the risk that is posed by this situation.
- Insecure interfaces and APIs: To mitigate the risks associated with insecure interfaces and APIs, it is essential to adhere to secure coding practices, use secure communication protocols (such as HTTPS), and implement the appropriate authentication and authorization controls. Regular vulnerability assessments and penetration testing can also aid in identifying and fixing system vulnerabilities.
- Insider Threat: These are security hazards that originate from within an organization. It occurs when someone with authorized access to a company's sensitive data or systems exposes or misuses them, jeopardizing the integrity confidentiality, and availability of vital data. The threat posed by insiders to cloud computing networks is a significant concern. According to a study by IBM [19], 60% of all cyber incidents are caused by internal threats, making them the leading cause of data breaches. These incidents can be intentional, such as when employees pilfer sensitive information for their own gain, or unintentional, such as when employees inadvertently disclose private information due to ignorance or a lack of training [20]. Because of the highly dynamic and complex nature of the cloud environment, it can be especially difficult to detect and eliminate insider threats in cloud-computing networks. To reduce the risk of insider attacks, organization's need robust security measures, such as monitoring, access controls, instituting security policies and procedures and educating employees through awareness programmes to foster security-conscious culture [21].
- Distributed Denial of Service (DDoS) Attack: This attack uses multiple compromised systems to overwhelm a network or server with traffic, making it unreachable to authorized users [22]. The perpetrator overwhelms the cloud server with fraudulent requests, consuming additional memory, disc space, and network bandwidth. These attacks strain the system and impede the delivery of services to actual consumers. DDoS attacks can cause collateral harm and affect many customers sharing the same infrastructure [24]. Organizations utilizing cloud services must implement security measures such as load balancers, intrusion detection/prevention systems, and firewalls to defend themselves from DDoS attacks [25].

II. SECURITY CHALLENGES RELATED TO CLOUD SERVICE PROVIDERS

A provider of cloud services must manage both internal and external hazards. For each hazard, different security considerations must be considered. Several of these dangers are enumerated below.

- Man-in-the-middle (MITM) attack – This attack occurs when a hacker intercepts an exchange between two parties to gain entry to and manipulate the data being transmitted [26]. Given that data is continuously transported over the internet and may pass through multiple servers before getting to its destination, MITM attacks can be extremely disruptive in cloud computing networking [27]. During an MITM attack, a hacker can obtain private data or information, such as financial information or login credentials whichcan lead to identity theft and other forms of fraud. [28]. ARP spoofing, DNS spoofing, and HTTPS interception are frequently used by attackers to conduct MITM attacks [29]. Among the preventive measures against MITM attacks are strong encryption protocols such as TLS/SSL, network segmentation and frequent network activity monitoring for anomalous behaviour [31].
- Weak access controls: An insufficient access control system can provide hackers with access to a company's assets and lead to the disclosure of customer information. It is a significant concern that could result in serious security problems. To track who uses it, the service provider must implement a more robust access control system.
- Complexity of configuration: The requirements of the cloud computing architecture necessitate that virtual devices are used to construct layers. The added complication of these layers may result in improper configuration and unknown vulnerabilities. A weak environment can result in security breaches with severe consequences for businesses. The Cloud Security Alliance (CSA) survey found that misconfiguration is the leading cause of cloud data intrusions, accounting for 95% of events [30]. A common configuration error occurs when the system's default security parameters are not modified. In 2019, an inappropriately configured firewall led to data intrusion at Capital One that granted hacker access to confidential customer information [32]. Inadequately securing storage buckets is an additional configuration flaw that may end in data

breaches. In 2020, a data breach caused by an improperly configured Amazon Web Services (AWS) storage bucket exposed over 10 million records comprising personal information [33]. When configuring cloud infrastructure, it is essential to adhere to best practices and security guidelines to prevent severe security risks and data breaches. This includes instituting secure authentication and access controls, reviewing and updating configurations frequently, and utilizing tools and automation.

- Segregation of duties: Thanks to cloud computing, a cloud service provider could be built utilizing a few parts. Therefore, even though it is challenging to manage, the division of roles should be employed in the CSP system [17].
- Privilege escalation: This involves increasing privileges on a system with restricted access permissions, then leveraging the hypervisor to attack a virtual machine with more access rights. When configuring cloud infrastructure, it is essential to adhere to best practices and security guidelines to prevent severe security risks and data breaches.

III. PRIVACY IN CLOUD COMPUTING NETWORKS

Most concerns with cloud computing networks are privacy-related, such as the need to protect identifying data, policy elements during integration, and transaction histories. Many businesses are hesitant to store their software and data on servers located in datacenters other than their own [34]. When responsibilities are moved to a shared infrastructure, sensitive client data is more likely to be exposed and subject to unauthorized access. CSPs must provide their clients with a high level of operational transparency and privacy protection in order to inspire confidence. Therefore, all security systems must include privacy protection features.

IV. CLOUD COMPUTING APPLICATIONS FOCUSED ON SECURITY

To improve security, there have been several recent advances in cloud computing applications. Notable amongst them are Confidential Computing, Cloud Access Security Brokers (CASB) and Multi-Cloud Security. Data processing in an encrypted environment is made possible by confidential computing, hence enhancing security. Because it safeguards data even from cloud providers, confidential computing represents a significant advancement in cloud computing security. Azure Confidential Computing, a service offered by Microsoft that offers a private enclave for processing sensitive data, is one of the newest cloud computing applications [37a]. With the use of CASB enables organizations to monitor and regulate access to cloud applications. They give users visibility into and control over cloud services and data, safeguarding it from virus, unauthorized access, and data loss. Prisma Cloud, provided by Palo Alto Networks, is one of the newest cloud computing solutions in the CASB market [37b]. Due to the overabundance of cloud services, it is increasingly common for organizations to employ various cloud providers, which makes security management challenging. The security of many cloud environments is the main objective of the developing field of multi-cloud security in cloud computing. Google Cloud Armour, a security service that provides defense against DDoS assaults, is one of the newest cloud computing applications in this field [37c].

V. IMPROVING CYBER SECURITY THROUGH CLOUD COMPUTING

According to ISACA (2017), cloud computing has a lot of benefits for enhancing cybersecurity in the cloud. These include but are not limited to scalable security measures, automated security, redundancy and backup services, and granular access control. Using this solution, cloud service providers have a substantial team of cybersecurity specialists to monitor, recognize, and react to any security threat. These experts can react fast to any attack because they are always monitoring the system. This means that companies using cloud computing can benefit from these security experts' experience without having to hire their own team. Antivirus software, firewalls, and intrusion detection and prevention systems are among the automatic security features offered by cloud computing. The time it takes to respond to a security breach is decreased by these automated security systems' swift detection and reaction to security threats. Moreover, granular access controls are provided by cloud computing providers, allowing organizations to manage who has access to their data and systems. This lowers the chance of information breaches and unauthorized access. In general, and with cloud computing, businesses have access to scalable security measures, automated security, redundancy and backup services, and granular access control using this solution [37d] for enhancing cybersecurity.

VI. CLOUD COMPUTING ACCESS CONTROL METHODS

Cloud computing companies may manage security in several ways, some of which are role-based access control (RBAC), Multi-factor authentication (MFA), Security monitoring and logging, Regular security audits and assessments and encryption [35]. However, the best strategy will rely on the organization's unique demands and the amount of protection required [36]. The security paradigm RBAC limits access to cloud resources based on the responsibilities of specific users inside an organization. Administrators can more easily control who has access to sensitive data by defining roles and permissions for different user groups. MFA on the other hand is a security measure that prevents users from accessing their accounts without providing two or more pieces of identification. It can be used in several ways, such as a password and one- time code, a smart card and a fingerprint, or a security token and a PIN. MFA has the potential to be a useful tool for limiting unauthorized access to cloud resources. Also, tools for security monitoring and logging can be used by cloud providers to find security issues and take appropriate action.

It enables administrators to take action to reduce security vulnerabilities by using these tools to identify unauthorized access attempts, malware infections, and other security threats. In the same vein, it is advisable for cloud providers to regularly undertake security audits and assessments as it helps to pinpoint weaknesses and guarantee adherence to security norms and guidelines and to prevent security lapses and guarantee that cloud resources are properly safeguarded. Lastly, to prevent unauthorized access, encryption can be used by cloud providers to safeguard data while it is in storage and transit by encrypting data into a secret code making it more difficult for hackers to access confidential data [42].

VII. EXISTING SOLUTIONS

For cloud computing solutions, a variety of techniques and plans are available to manage security. Among the most popular techniques are:

A. Encryption

In cloud computing networks, encryption is a common kind of data intrusion protection. It involves the transformation of plaintext into cypher text, making it inconceivable to anybody who does not possess the needed decryption keys. Thanks to the flexibility of encryption, businesses may safeguard their data on a variety of scales, from single files to large databases or storage volumes. However, encryption can be expensive because it may require specialized software or hardware and additional personnel to manage the overall security protocols and encryption keys [34].

B. Access Controls

Access control is a crucial component of cloud computing networking's defense against data breaches. It comprises regulating access to sensitive data to impose restrictions on user permissions. To do this, a variety of techniques like encryption, authentication, and authorization can be applied. Access control is a critical step in preventing security breaches in cloud computing networks, according to [35]. To prevent mistakes, access control policies should be set up appropriately and updated periodically [36].

C. Network Segmentation

Network segmentation is the division of a computer network into smaller subnetworks known as segments or zones with the goal of enhancing security by restricting access to different parts of the network [37]. Network segmentation is one of the most effective ways to avoid security breaches in cloud computing [38] because it lowers the attack surface [37] and allows administrators to give priority to some types of data while denying or limiting access to the rest. However, segmentation has the potential to hinder communication between various network components and increase complexity [37, 38], both of which could have a detrimental effect on the performance of the network.

D. Intrusion Detection and Prevention (IDP)

In cloud computing networks, IDP systems are widely employed to prevent data intrusions [39]. They help monitor network traffic for malevolent activity and also alert administrators or take action to block or quarantine traffic [40].

E. Regular Auditing and Monitoring

Regular auditing and monitoring are necessary for minimizing data intrusions in cloud computing networks. IBM found that the average cost of a data breach in 2020 was $3.86 million, highlighting the importance of instituting security measures such as regular auditing and monitoring to prevent and detect breaches [41]. Regular auditing and supervision could reduce the likelihood of fines and other unfavourable outcomes by ensuring that the company adheres to the sector's standards and regulations. Before they are exploited by an attacker, vulnerabilities can be rapidly patched [40].

4.0. FUTURE RESEARCH DIRECTION

With terabytes of externally stored data, it is crucial to safeguard data from a variety of threats [43]. Several techniques, such as the creation of a new, independent security layer, have been implemented to protect against many of these vulnerabilities and other cloud technology hazards. Future trends in cloud security and available research areas are outlined.

- Overcome virtualization and multi-tenancy problems: One of the foundational elements of any cloud system is virtualization [44]. Consequently, cloud providers should address the security concerns related to their virtualized architecture.
- Offer solutions to safeguard the company's cloud from Bring-Your-Own-Device (BYOD) [45]: In today's companies, BYOD policies are increasingly the norm rather than the exception. More and more workers are accustomed to bringing their own cellular devices to work. New technologies such as PDAs, smartphones and tablets rely heavily on cloud-based solutions to be effectively integrated into a company. Therefore, businesses should establish policies and standards for cloud usage.
- Set more security policies on cloud [46]: Margaret Dawson, Vice President of Product Management at Symform, a cloud storage provider claims a survey reveals that non-IT departments are using cloud apps and services at an exceedingly rapid rate [47]. As a result, IT must exert more control over policy and governance while allowing the business to make use of the benefits of the cloud.
- Develop new cryptographic methods for cloud environment [48]. The secure transmission of data through the cloud requires the use of encryption. To achieve a level of security for user data on clouds, numerous encryption approaches, either public or private key cryptosystems, are deployed. However, current methods do not address all cloud data

security challenges, hence, we urgently need new methods and technology.

- Improve more trusted computing for cloud [49]: Customers who use the cloud cannot entirely rely on service providers. Therefore, researchers are working to develop non-traditional access control methods that are typically founded on cryptographic approaches, for data object access control [50].
- Improve information centric security (ICS) [51]: ICS places greater emphasis on the security of the information itself than on the security of the applications, infrastructure, and networks. According to cloud security expert Ed Reynolds, chief technologist at HP Enterprise Services [52], an information-centric approach makes more sense in shared and open computing environments than the traditional emphasis on infrastructure protection.

6.0 CONCLUSION

Cloud computing has expanded quickly in recent years, making secure data protection solutions necessary to make it more dependable and trustworthy. For businesses using cloud services, the term "cloud computing security" refers to a wide range of security issues. The client data that CSPs keep for customers and organizations must be protected from security breaches. As security and privacy concerns in cloud computing networks continues to rise, both CSPs and cloud clients can cooperate to ensure the security of the cloud by considering a number of solutions, such as access control, data at rest and in transit, encryption, and regular auditing etc. This essay thoroughly examines each of these areas of cloud security and offers suggestions for CSPs best practices. Both the consumer and the cloud provider share responsibilities for cloud computing security and understanding this shared responsibility model and adhering to recommended practices can help businesses use the cloud as a secure location to store and process their data.

Organizations and individuals must, however, consider the dangers and advantages to their business before deploying their system in the cloud. The future appears less gloomy as more businesses adopt cloud computing and make investments in research and development to address its drawbacks. To adapt to cloud architecture, new security protocols and management standards must be developed, and already existing ones must be entirely revised. Future technology advancements like Confidential Computing, Cloud Access Security Brokers (CASB) and Multi-Cloud Security will probably improve cloud security by providing more sophisticated threat detection and response capabilities.

REFERENCES

[1] Tabrizchi, H. & Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*. 76. 9493–9532. https://doi.org/10.1007/s11227-020-03213-1.

[2] Mell, P. & Grance, T. (2018). SP 800-145, The NIST Defnition of cloud computing | CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/fnal.

[3] Takabi, H., James B., & Gail-Joon, A. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE COMPUTER AND RELIABILITY SOCIETIES. 1540-7993.

[4] Fruhlinger, J. (2020). Equifax data breach FAQ: What happened, who was affected, what was the impact? Available at: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[5] Bruening, P. & Treacy, B. (2009). Cloud Computing: Privacy, Security Challenges. Bureau of Nat'l Affairs, 2009; www.hunton.com/files/tbl_s47Details/FileUpload 265/2488/CloudComputing_Bruening-Treacy.pdf.

[6] Hubbard, W. & Michael D. (2012). Top Threats to Cloud Computing. Cloud Security Alliance, 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[7] Basu, S., Bardhan, A., Gupta, K., Saha, P., Mahasweta, P., Manjima, B., Kaushik, B., Saunak, C., & Sarkar, P. (2018). Cloud Computing Security Challenges & Solutions-A Survey. IEEE. 978-1-5386-4649-6/18/$31.00.

[8] Roman R, Lopez, J., & Mambo, M. (2018). Mobile edge computing: a survey and analysis of security threats and challenges. *Future Generation Computer System*. 78. 680–698

[9] Sgandurra, D. & Lupu, E. (2016). Evolution of attacks, threat models, and solutions for virtualized systems. *ACM Computer Survey*. 48(3):1–38

[10] Kaur, M. & Singh, H. (2015). A review of cloud computing security issues. *International Journal Advanced Engineering Technol*. 8(3):397–403 17.

[11] Kumar, P., Raj, P., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Proc Computer Science. 125. 691–697.

[12] Khalil, I., Khreishah, A., Azeem, M. (2014). Cloud computing security: a survey. Computers 3(1):1–35 19.

[12a] Bashir, S., Haider, S. (2011). Security threats in cloud computing. In: Proceedings of the International Conference for Internet Technology and Secured Transactions. 20.214–219.

[13] Ryan, M. (2013). Cloud computing security: the scientific challenge, and a survey of solutions. *J Syst Software*. 86(9). 2263–2268.

[14] Hubbard, W. & Michael, Z. (2010). Top Threats to Cloud Computing. Cloud Security Alliance, 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. [Accessed: 20-Jun-2012].

[15] Younis, A., Kashif, K. & Madjid, M. (2014). Cloud Computing Security & Privacy Challenges. https://doi.org/10.13140/2.1.1779.6809.

[16] Kurtz, R. & Vines, R. (2010). Cloud security: A comprehensive guide to secure cloud computing. *John Wiley & Sons*, 384.

[17] Li, Y. (2020). Cloud Computing and Its Security Issues. *In Proceedings of the 2nd International Conference on Energy Conservation and Energy Storage Technology*. 13-18.

[18] Maity, S., & Jana, P. K. (2020). Cloud computing security and data loss prevention. *In Emerging Trends in Data Science Springer*. 385-393.

[19] Bhardwaj, S., Singh, S., Singh, S. K., & Kumar, V. (2021). Data backup and recovery in cloud computing: A systematic review. *Journal of Cloud Computing*. 10(1). 1-29.

[20] IBM. (2020). Cost of a Data Breach Report 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

[21] CERT Insider Threat Center. (2019). Common Sense Guide to Mitigating Insider Threats, 6th Edition. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540331.pdf

[22] Cloud Security Alliance. (2020). Top Threats to Cloud Computing: Egregious Eleven. https://downloads.cloudsecurityalliance.org/assets/research/top-threats/TOP_THREATS_2020.pdf

[23] Man-in-the-Middle (MitM) Attacks and How to Prevent Them." Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-man-in-the-middle-attack-mitm.

[24] What is a DDoS Attack?, Digital Guardian, accessed February 26, 2023, https://digitalguardian.com/blog/what-ddos- attack.

[25] Distributed Denial of Service (DDoS) Attacks," Cybersecurity and Infrastructure Security Agency, accessed February 26, 2023, https://www.cisa.gov/distributed-denial-service-ddos.

[26] Sriram, M. (2023). Protecting Cloud Infrastructure against DDoS Attacks. Cloud Security Alliance, https://cloudsecurityalliance.org/research/protecting-cloud-infrastructure-against-ddos-attacks/.

[27] "Man-in-the-Middle Attack." TechTarget, https://searchsecurity.techtarget.com/definition/man-in-the-middle-attack.

[28] Margaret, R. (2021). Man-in-the-Middle Attack (MITM). Search Cloud Security. https://searchcloudsecurity.techtarget.com/definition/man-in-the-middle-attack-MITM.

[29] Man-in-the-Middle Attacks: What Are They and How Do You Prevent Them?" Norton Life Lock, https://us.norton.com/internetsecurity-online-privacy-man-in-the-middle-attacks-what-are-they-and-how-do-you- prevent-them.html.

[30] Mitigating Man-in-the-Middle Attacks.Cloud Security Alliance, https://cloudsecurityalliance.org/artifacts/mitigating- man-middle-attacks/.

[31] "Man-in-the-Middle (MitM) Attacks and How to Prevent Them." Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-man-in-the-middle-attack-mitm.

[32] Chen, B. (2021). Cloud Misconfigurations Continue to Plague Organizations, Exposing Them to Cyber Attacks. Security Boulevard. https://securityboulevard.com/2021/06/cloud-misconfigurations-continue-to-plague-organizations-exposing- them-to-cyber-attacks/

[33] Zorz, Z. (2019). Capital One Data Breach Due to Misconfigured Firewall. Help Net Security. https://www.helpnetsecurity.com/2019/07/30/capital-one-data-breach-firewall/.

[34] Orcutt, M. (2020). AWS Misconfiguration Exposes 10 Million Records in Data Breach. Threatpost. https://threatpost.com/aws-misconfiguration-exposes-10-million-records-in-data-breach/153528/.

[34a] Rashid, F. (2020). The rise of confidential computing: Big tech companies are adopting a new security model to protect data while it's in use. *IEEE Spectrum*. 57(6). 8-9. https://doi:10.1109/MSPEC.2020.9099920.

[34b] Ahmad, S., Mehfuz, S., & Beg, J. (2021). Enhancing Security of Cloud Platform with Cloud Access Security Broker. In: Kaiser, M.S., Xie, J., Rathore, V.S. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems. 190. Springer, Singapore. https://doi.org/10.1007/978-981-16-0882- 7_27.

[34c] Sandesh, A. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering 16(9). 379-384.

[34d] https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/cloud-computing-and-cybersecurity-benefits-risks- and-controls

[35] Liu, Q., Zhang, J., Yang, Y., & Hu, X. (2017). Study on access control technology in cloud computing. Journal of Ambient Intelligence and Humanized Computing. 8(6). 881-889.

[36] National Institute of Standards and Technology. (2021). Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[37] Liu, Q., Zhang, J., Yang, Y., & Hu, X. (2017). Study on access control technology in cloud computing. Journal of Ambient Intelligence and Humanized Computing, 8(6), 881-889.

[38] Rong, C. (2020). Network Segmentation and Security Measures in Cloud Computing. In J. Yu, X. Sun, & G. Li (Eds.), Advances in Computer Science and Engineering. 381-390. Springer. https://doi/10.1007/978-3-030-36240-7_38.

[39] Buyya, R., Yeo, C. & Venugopal, S. (2008). "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," in Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications. 5–13.

[40] Garg, S., Tunc, E. & Buyya, R. (2016). Distributed and scalable intrusion detection and prevention for collaborative cloud networks. Journal of Network and Computer Applications. 74. 25–36.

[41] IBM Security. (2021). Cost of a Data Breach Report 2020. Retrieved from https://www.ibm.com/security/data-breach

[42] Kavya, S. (2018). A Comparative Study on Homomorphic Encryption Schemes in Cloud Computing. *3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*.

[43] Radwan, T., Marianne, A. & Nashwa, A. (2017). Cloud computing security: challenges and future trends. International Journal of Computer Applications in Technology. 55. 158. 10.1504/IJCAT.2017.082865.

[44] Ren, K., Wang, C. and Wang, Q. (2012). Security challenges for the public cloud. Internet Computing, IEEE. 16(1), 69– 73.

[45] Westervelt, R. (2012) Mobile-impacting-cloud-security-issues-sayspanel. Available online at: http://searchcloudsecurity.techtarget. com/news/2240170513/Mobile-impacting-cloud-security-issuessays-panel.

[46] Sengupta, S., Kaulgud, V. & Sharma, V. (2011). Cloud computing security – trends and research directions. Services IEEE World Congress. 524–531.

[47] Symform (2012). Cloud security research. Available online at: http://www.symform.com/about-us/news-reviews/press- releases/ cloud-security-research/

[48] Dijk,V., Juels, V. (2010). On the impossibility of cryptography alone for privacy-preserving cloud computing. Proceedings of the 5th USENIX Conference onHot Topics in Security, USENIX Association. 1–8.

[49] Lui, S. (2013). Case study: Ballarat grammar uses sdn to fight malware. Available online at: http://www.zdnet.com/au/casestudy-ballarat-grammar-uses-sdn-to-fight-malware7000015942/

[50] Yu, S., Wang, C., Ren, K. & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. INFOCOM. Proceedings IEEE. 1–9.

[51] Kimmel, G., Domangue, E. & Adamouski, F. (2010). Information-centric security.

[52] HP (n.d.) Secure the data – not the cloud. Available online at: http://h30458.www3.hp.com/us/us/ezine/secure-the-data-notthe-cloud.html/title/secure-the-data not-the-cloud.