CURRENT DATA SECURITY AND PRIVACY CHALLENGES IN CLOUD COMPUTING: A REVIEW

Olakunle Isaac IFAWOYE[1], Olalere MORUFU[2], Esther Tolubori OMONAYIN[3]
[1]Information and Communication Technology, Bingham University Karu, Nigeria
[2]Department of Cyber Security, National Open University of Nigeria, Head Quarter, Abuja, Nigeria
[3]Department of Computer Science, Baze University Abuja, Nigeria
kunle.i@binghamuni.edu.ng, molerejide@noun.edu,ng, esther.omonayin@bazeuniversity.edu.ng

Keywords: Cloud Computing, data security, data theft, security threats

Abstract: *Cloud computing has developed to be an integral aspect of current as well as future information technologies. Technology has been identified as an efficient tool for all the provided services but it is also associated with different threats. Despite many advantages of cloud computing, security remains a main challenge. To successfully migrate through the cloud, one must consider some critical factors, including understanding the main security concerns and putting effective mitigation strategies in place. Since the data that a business or a user stores in the cloud is frequently private and sensitive, numerous fire attacks and data theft have been reported as crucial factors over the years of its development. Cloud-based system contends with a few security risks such as DDoS attacks, man-in-the-middle attacks, phishing scams, and data breaches. Due to the multitenancy architecture, trust is a major challenge and fault tolerance continues to be a problem for the implementation of cloud computing. Data breaches in cloud computing environments may have serious repercussions, including monetary losses, reputational harm, and legal repercussions. Misconfigurations, insider threats, external attacks, malware injections, and phishing scams can all lead to breaches. The way government organizations and intelligence agencies manage data and information has been revolutionized by cloud computing. Organizations are discovering that cloud computing is a smart substitute for traditional hardware and infrastructure because it allows for the replacement of these resources with effective and affordable cloud solutions. Building trust and promoting wider adoption of cloud computing technologies will be greatly aided by emphasizing proactive security measures and ongoing monitoring. This paper presents a review of the security issues with cloud computing and some possible solutions were suggested*.

1. INTRODUCTION

Cloud computing‖ can be defined to be the application of the internet to produce technology-enabled facilities for organizations and people [1]. The technology allows clients or users to get entrance to resources virtually through the internet, from any place at any time without upsetting technical/physical management and maintenance of the original resources [2]. Cloud computing is interesting to business owners because that enables the elimination of the need for customers to plan for provisioning and permits establishments to commence small and scale up only when service demand upturns [3]. The use of cloud computing in business innovation is pertinent or applicable due to its adaptability and agility of cloud technology which enables new methods of working, operating, and running a business[4].

The service allows people to access files and software kept in the cloud from any place, eliminating the users' requirement to be always physically close to actual hardware [5]. Cloud computing makes connections available from anywhere because they are kept on a network of host computers that transfer data over the internet. Resources of cloud computing are dynamic, independent, scalable and different from grid and utility computing [6]. Cloud computing has now been considered one of the best computing paradigms in the field of information technology in recent years [7]. That happened due to advances in existing computing paradigms which include parallel computing, grid computing, distributed computing, and other

computing paradigms. Cloud computing has fundamentally altered the IT landscape by making a wide range of services and resources available to businesses and individuals online [8]. Data storage, processing, and sharing have undoubtedly undergone a revolution [9].

The major existing challenges in cloud environments are security/privacy, interoperability/portability, reliability/availability, bandwidth cost/performance and cloud computing threats can include unauthorized access to user data, theft of data, and malware attacks [10]. To protect data from these threats, organisations must ensure that only authorized users can access confidential data. Recent problems in cloud platforms have gone beyond data breaches, general cloud threats and privacy issues, the current challenges now include insufficient identity and access management controls, cloud misconfiguration, insider threats, unsecured or vulnerable APIs, compliance with regulatory mandates, open source and lack of information technology experts [11].

Several organisations such as small, medium and enterprises have transferred to this technology for several reasons like as resources of computing, decreased total ownership cost, on-demand services, increased revenue and so on [12]. Cloud computing gives many advantages of cloud migration that encourage business enterprises to accept this change [13]. There are some challenges for companies implementing cloud computing like interoperability, portability, and organizational aspects the most important challenge is the security and privacy of the information [14] [15]. Although cloud computing has many benefits, it also raises many security concerns that must be addressed if sensitive data is to be kept private, undamaged, and accessible [16].

Many studies have been apprehensive about overcoming problems and challenges that depend upon the lure of cloud computing. Security has been always seen as one of the great serious matters of cloud computing and resolving such matters would lead to a persistent increase in the popularity and use of the cloud [17]. Requirements of Security denote a main issue that must be met to reduce some effects of these problems. The same threats that affect computer networks and data in transit, such as man-in-the-middle attacks, phishing scams, eavesdropping, sniffing, and other similar threats, also apply to cloud-based services. The DDoS (Distributed Denial of Service) attack is a frequent but important attack on the cloud computing infrastructure [18]. As more data is exposed, the harm to users and society will worsen [19]. This paper investigates some security threats and issues of cloud computing along with possible approaches to resolving them. Also, the future research directions that will involve the development of current techniques for reducing these threats were mentioned.

2. LITERATURE REVIEW

2.1 Cloud Computing

Cloud computing is a model for enabling universal and convenient distributed access to a shared pool of powerful computing resources [20]. It is a networked system of computer resources such as servers, applications, storage and services that are available on demand with minimal managerial effort on the part of the consumer [21]. The National Institute of Standards and Technology (NIST) perhaps gives the most widely used definition of cloud computing as a model that enables convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly allocated and scaled as released with minimal management effort or service provider intervention [22].

Cloud services are categorized into three main models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [23]. IaaS provides virtualized computing resources[24], PaaS offers a platform for application development and SaaS delivers software applications over the Internet [25]. Cloud computing can be deployed in various ways: Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud [26]. Each deployment model has distinct characteristics, addressing different organizational needs and concerns. Organisational adoption of cloud computing is influenced by factors such as cost savings, flexibility, and business agility [27]. However, challenges like data migration, interoperability, and vendor lock-in can hinder seamless adoption.

2.2 Related Work

A provision of a better knowledge of cloud computing as well as suggestions on relevant research paths in this growing field was conducted by [28]. The future benefits or advantages and the imminent possible challenges in cloud computing such as performance,

architecture, scale-up, and big data were discussed.

[29]discussed privacy-associated issues, problems and solutions. It was stated that cloud computing is growing fast, conspicuously based on processing capacity and time of response. Whether through public service or privately for the enterprise, the public can now have significantly more knowledge and opportunity to employ cloud computing than they could some years ago. The study concluded that educating the public about data privacy should be a priority for the development of cloud computing, as doing so can increase people's responsibility for how they handle their personal information, help them understand the value of internet security and assist them in identifying the undesirable results of unintentionally exposing sensitive information.

[30] examined major security issues and challenges associated with the platform of cloud computing. The cloud-specific vulnerabilities were properly described with their causes which add to the provision of assistance for analysis and identification of security risk. It was mentioned that in future work the assessment and analysis of risk can be done by applying vulnerabilities to protect the cloud from impostors.

A review of the advancement of privacy security issues from the perspective of several privacy security protection technologies in cloud computing [14]. The study presented some cloud computing privacy security risks and built a framework for comprehensive privacy security protection. Also, it was revealed and discussed the development of many technologies, such as access control; cipher text policy attribute-based encryption (CP-ABE); key policy attribute-based encryption (KP-ABE); the fine-grain, multi-authority, revocation mechanism; the trace mechanism; proxy re-encryption (PRE); hierarchical encryption; searchable encryption (SE); and multi-tenant, trust, and a combination of various technologies, and the comparison and analysis of the features and application scope of typical schemes was performed. In conclusion, the discussion on current challenges and likely future work directions were mentioned. A survey on threats in the scope of Data, Applications, Infrastructure and services in general in the cloud computing platform was conducted by [31]. The threat types or attacks in the context of the cloud have been well-defined using surveys of relevant papers. The methodology used is surveying some of the results of earlier studies relating to threats or obstacles in cloud computing carried out in five steps, namely: writing the formulation, conducting a search, conducting selection and evaluation, analysis, and summarizing the results. The survey results claimed there were many types of threats in the cloud computing environment, which are divided into four categories, namely: Threats to applications, Threats to data, Threats to infrastructure, and threats to cloud services in general. The output of this study is to provide a more detailed understanding of the types of threats for each service in the cloud.

A framework on what cloud computing is, main security risks and issues that are presently current in the field of cloud computing, research challenges, importance in key industries and also the personal hypothesis on future advances in the field of cloud security. [32] discussed issues on security, requirements and problems that cloud service providers (CSP) encounter during cloud engineering. The study further recommended protection standards and management models to address these issues for the technical and business community.

3. CHALLENGES AND MITIGATION STRATEGIES IN CLOUD COMPUTING SECURITY

Cloud computing users are getting higher every day, also the problems of security and risks of data in the cloud are increasing [33]. Security technology is a single component, security is about people, processes and technology all three of which have to be in unison or agreement because if any one of these areas is affected, then the security platform breaks down. Without any hesitation, cloud computing is a valuable tool for almost every business that is using it. There are several security challenges contending with cloud computing that open a wide area to research for researchers. Every technology has two aspects, one aspect leads to prosperity and the other rises to challenges or problems. Likewise, with cloud computing, there are different security problems facing cloud computing [34]. The Multi-Agency Cloud Computing Group made serious determinations to produce effective controls in the cloud platform to provide cyber security, it is revealed

that the major security problems with the cloud are trust, confidentiality and encryption [35].

(i) Trust Problem

A cloud service is trusted by users concerning its performance, security, and privacy based on the provider's identity [36]. If the user hopes that the provider offers dependable cloud services, then the cloud service is trusted[37]. The trust that exists between the serving end and the receiving end is the key issue in cloud computing. The individual at the receiving end is never sure whether the serving end is providing trustful data so the servicing ends are bound by the Service Level Agreement (SLA) document. SLA framework is used as a trust management model for security in a cloud environment [38]. SLA document includes the duties of the service provider and their plan activities.

(ii) Confidentiality Problem

Confidentiality can compromised due to unreliable cloud service providers [39]. The user's data security depends on the cloud provider's responsibility [40]. The confidentiality of data can be achieved by circumventing the illegitimate user access. Confidentiality can be ensured through better encryption techniques. Basically, there are two different approaches to achieving confidentiality: physical isolation and cryptography. Design a secure storage service as a public cloud infrastructure and apply cryptographic analysis.

(iii) Authenticity Problem

Authentication involves the method of determining the client's identity. The authentication information varies subject to how cloud storage is being accessed, but also, falls into two common types: A server-centric flow enables an application to directly hold the credentials of a service account to complete authentication [41]. Cloud needs to be completely secured from unauthorised users. The authentication challenge must be solved by generally applying a digital signature approach. An access control mechanism is a robust and distributed control mechanism where the cloud confirms the individuality of the cloud user without knowing the user's information and stores the information of the user. The stored information can be decrypted by the authentic users.

(iv) Encryption Problem

Many widely used data-securing technique in cloud computing is encryption [42]. But the main drawback of encryption is, that it needs high computational power. It also produces overall database performance because every time a query is run, decryption is required for the encryption. The use of cryptographic algorithms in combination instead of only one algorithm can efficiently accelerate the throughput. The cloud tables are maintained in such a way that data are encrypted using these methods. Here requested query is executed against the stored data, and the result is decoded by the user.

This increases overall performance. Another method called end-to-end mechanism-based encryption works differently for the cryptographic processes [43]. Another approach is called fully Holomorphic encryption which can calculate the results of encrypted data processing instead of the raw data, which might increase potential data confidentiality [30].

(v) Key Management

Key management involves the process of putting specific standards in place to allow the security of cryptographic keys in an organization. The technology deals with the creation, exchange, storage, deletion, and refreshing of keys. Key management forms the basis of all data security. Data is encrypted and decrypted via the use of encryption keys, which means the loss or compromise of any encryption key would invalidate the data security measures put into place. Keys also ensure the safe transmission of data across an Internet connection. Managing the efficient use of keys is a big security problem in the cloud which includes the proper management of encryption/decryption and keys [44]. Cloud stores the encrypted key which is a very complex technique. A small database should be maintained to accommodate keys protectively. To accomplish this, additional hardware and software resources are required and cost increases to implement. A two-level encryption solution is given to this problem.

(vi) Multitenancy Issue

Multitenancy is a form of software design where a single software instance can provide many different user groups [45]. It means that several customers of cloud vendors are using the same computing resources. They share the same computing resources, but the data of each cloud customer is stored separately and protected [46]. It is a very important concept of cloud computing. Confidentiality issues might arise due to scattered resources in different geographical areas of a cloud environment.

Isolation of applications and systems should be done for proper confidentiality, if not done may lead to insecurity issues. If data are stored virtually, then a virtual machine hosting a malicious program may affect the data.

(vii) Data Splitting

Data splitting is a process of splitting data to more than one host at a time when they cannot communicate individually [47]. So when users want their data back, the user must access all of the service allocators to recollect the original data. It is generally employed in machine learning to divide data into a train, test or validation set. This method enables the finding of the model hyper-parameter and also the estimation of the generalization performance [48].

Data splitting is an alternative to the encryption process and works faster than encryption. It also has some security problems. If multiple clouds are being used, then ensuring integrity should be checked after the splitting process can be done using the Multi-Cloud Database Model. As data are stored in different clouds and replication should be done, security also is in higher priority. Because the attacker will get less chance to access multiple clouds at a time.

3.2 Data Breaches in Cloud Computing

Cloud computing is a completely online-based technology where the information of customers is set aside and stored in the server farm of a cloud supplier like Amazon, Salesforce.com Google Microsoft and so on [49]. Cloud computing has grown in popularity due to its level of scalability, flexibility and affordability. The constrained control over the information may obtain diverse security issues and threats that incorporate data accessibility, data breaches, unreliable connectivity, sharing of resources and inside attacks [50]. A breach can be considered as an event in which an individual's name, medical record, financial record or debit card is potentially put at risk either in paper format or electronic [51].

A breach of security may lead to accidental or unlawful destruction, loss alteration, or unauthorized disclosure of access to personal data transmission. Serious repercussions for the security of cloud computing environments can result from data breaches. Data is processed and stored on remote servers that can be accessed through the internet in cloud computing. Data loss typically happens when a cloud system's hardware or software malfunctions, which is typically brought on by human error and also during data transfer [52]. Data breaches in cloud computing can happen for many reasons, such as incorrect configurations of cloud services that expose sensitive data to unauthorized access [53].

Human error or a lack of knowledge of best practices for cloud security could be to blame for this. If there aren't enough backups in place, a data breach could lead to data loss or deletion, which can be very problematic [54]. Significant business disruptions and information loss may result from this. Cloud service providers and their clients must put strong security measures in place, including encryption, access controls, multi-factor authentication, routine security audits, and continuous monitoring of the cloud infrastructure, to reduce the risk of data breaches in cloud computing environments. Additionally, spreading awareness of cybersecurity best practices among employees and users can aid in preventing breaches brought on by human error or social engineering attacks.

4. SUMMARY AND DISCUSSION

The users of cloud computing are increasing daily so the security concerns and risks of data in the cloud are also increasing. There is a need to look at cloud security a bit differently, it must be looked at from a holistic point of view in terms of what endpoints are interacting with it and what is the user community doing with it. The infrastructure constructed, like what type of security grips are available and in what different methods the infrastructure can be segmented. What is allowed to communicate with what why and how these applications are supposed to behave so that the right policies can be employed? But more important is to extend the right security capabilities to where the customer data, user, and endpoints are all going.

Hosting of the cloud has become the standard due to many factors such as flexibility, and scalability. efficiency and accessibility, it also optimizes Information Technology expenses and encourages collaboration to happen. However, with the upswing of present digitalization arrives a surge of cloud security risks. With such threats, organisations must be attentive to the cloud security of their businesses. Several measures have been implemented to significantly enhance cloud security but impossible to eliminate all security risks. To help deal with these new

challenges, a creative and more intelligent detection strategy is required as well as the use of new information sources.

Adoption of a multi-cloud technique, by organisations and businesses can decide to apply more than one cloud service provider. This gives opportunities and flexibility based on every provider's distinctive competencies. A multi-cloud technique can act as a safety net for organizations to reduce the effect of downtime and disruptions. DevOps methodology can be employed, these are practices that combine Information and Technology operations software development and IT operations to optimize the life cycle of software development. DevSecOps, on the other hand, integrates security at each stage of that development life cycle, from initial design to final delivery. The implementation of DevSecOps requires organizations to perform different tasks, including security audits on previous infrastructures, security tests automation and integration of security tools with DevOps tools, implementation of an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) as part of cloud infrastructure is also effective approach of minimizing cloud security threats. Both systems scrutinize whether certain traffic resembles a threat. IDS can act as a watchful watchdog for cloud systems. It uses sophisticated methods and predefined signatures to identify general malicious attack patterns and any form of suspicious activity.

Data management technology must be able to effectively manage large datasets because cloud computing requires processing and analyzing of distributed and mass data. A well-known approach that is dependable for data security is cryptography. Processing the data in an encrypted form, however, will raise the cost of computation and is technically challenging. Information hosted on cloud servers may be encrypted and only accessible at the client level with a key to ensure data privacy. Since it might require a lot of processing power, this is only trustworthy if the data can be quickly decrypted at the client level. This will be possible and more information will be integrated with credit to the multi-core processors that are developing**.**

To address these threats and enhance cybersecurity in cloud computing, organizations should adopt a comprehensive security strategy, which may include: security audits and risk assessments, robust access controls and authentication mechanisms, encryption of data at rest and in transit, implementing security measures provided by the cloud provider, continuous monitoring, incident response capabilities, employee training and awareness programs, regularly updating and patching systems and applications.

By considering a proactive and multi-layered approach to security, businesses can better protect their cloud assets and mitigate the risks associated with cloud computing. To maintain security as an ongoing process, security measures must be continually adapted to emerging threats and changes towards cloud infrastructure. Collaboration with experienced security professionals and staying up-to-date with the latest security trends are also vital for ensuring the safety of the cloud environment**.**

5. CONCLUSION

Cybersecurity and threats in cloud computing are critical aspects that need to be addressed to ensure the safety and integrity of data and applications hosted in the cloud. While cloud computing offers numerous benefits, it also introduces new security challenges. While cloud computing offers unprecedented flexibility and scalability, its security issues cannot be ignored. Organizations must be proactive in implementing robust security measures to safeguard their data and applications. Cloud service providers also play a crucial role in maintaining a secure infrastructure and must continuously update their security protocols to counter emerging threats. By understanding these security challenges and adopting appropriate mitigation strategies, businesses can harness the full potential of cloud computing without compromising sensitive information.

REFERENCES

[1] Baharuddin, D. Ampera, H. Fibriasari, M. A. R. Sembiring, and A. Hamid, "Implementation of the cloud computing system in learning system development in engineering education study program," *Int. J. Educ. Math. Sci. Technol.*, vol. 9, no. 4, pp. 697–740, 2021, doi: 10.46328/ijemst.2114.

[2] C. Lin, L. Li, and Y. Chen, "Dynamic system allocation and application of cloud computing virtual resources based on system architecture," *Open Comput. Sci.*, vol. 13, no. 1, pp. 1–11, 2023, doi: 10.1515/comp-2022-0259.

[3] R. Ibrahim and A. A. Muslim, "Determinants of Cloud Computing Adoption and Usage in Nigerian

Universities," *Niger. J. Eng. Sci. Res.*, vol. 6, no. 2, pp. 12–23, 2023, [Online]. Available: https://www.iuokada.edu.ng/journals/nijesr/

[4] S. Liu, F. T. S. Chan, J. Yang, and B. Niu, "Understanding the effect of cloud computing on organizational agility: An empirical examination," *Int. J. Inf. Manage.*, vol. 43, pp. 98–111, 2018, doi: 10.1016/j.ijinfomgt.2018.07.010.

[5] R. Nazir, Z. Ahmed, Z. Ahmad, N. Shaikh, A. Laghari, and K. Kumar, "Cloud Computing Applications: A Review," in *EAI Endorsed Transactions on Cloud Systems*, 2020, pp. 1–11. doi: 10.4108/eai.22-5-2020.164667.

[6] R. Hooda, A.K & Ahuja, "Cloud Computing Vs. Grid Computing," *Int. J. Res. Publ. Rev.*, vol. 04, no. 01, pp. 1806–1812, 2023, doi: 10.55248/gengpi.2023.4149.

[7] T. Alam, "Cloud Computing and Its Role in the Information Technology Cloud Computing and its role in the Information Technology," in *IAIC Transactions on Sustainable Digital Innovation (ITSDI) Vol.*, 2021, pp. 108–115. doi: 10.2139/ssrn.3639063.

[8] G. Kiryakova, N. Angelova, and L. Yordanova, "Application of cloud computing services in business," *Trakia J. Sci.*, vol. 13, no. Suppl.1, pp. 392–396, 2015, doi: 10.15547/tjs.2015.s.01.067.

[9] A. Ait *et al.*, "New mechanism for Cloud Computing Storage Security," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, pp. 526–539, 2016.

[10] R. Palaniappan, S and Awang, "Web-Based Heart Disease Decision Support System using Data Mining Classification Modeling Techniques," *Proc. ii AS2007*, pp. 157–167, 2007.

[11] S. Khan, I. Kabanov, Y. Hua, and S. Madnick, "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned," *ACM Trans. Priv. Secur.*, vol. 26, no. 1, pp. 1–29, 2022, doi: 10.1145/3546068.

[12] A. Ahmad Dar, "Cloud Computing-Positive Impacts and Challenges in Business Perspective," *J. Comput. Sci. Syst. Biol.*, vol. 12, no. 01, pp. 15–18, 2018, doi: 10.4172/jcsb.1000294.

[13] N. Soveizi, F. Turkmen, and D. Karastoyanova, "Security and privacy concerns in cloud-based scientific and business workflows: A systematic review," *Futur. Gener. Comput. Syst.*, vol. 148, pp. 184–200, 2023, doi: 10.1016/j.future.2023.05.015.

[14] P. J. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *J. Netw. Comput. Appl.*, vol. 160, no. March, p. 102642, 2020, doi: 10.1016/j.jnca.2020.102642.

[15] Y. S. & Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: Technical review," *Futur. Internet*, vol. 14, no. 1, pp. 1–27, 2022, doi: 10.3390/fi14010011.

[16] M. K. Sasubilli and R. Venkateswarlu, "Cloud Computing Security Challenges, Threats and Vulnerabilities," in *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, 2021, pp. 476–480. doi: 10.1109/ICICT50816.2021.9358709.

[17] T. Alam, "Cloud Computing and its Role in the Information Technology," in *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 2022, pp. 9–15. doi: 10.34306/itsdi.v1i2.103.

[18] D. Tang and X. Kuang, "Distributed Denial of Service Attacks and Defense Mechanisms," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 612, no. 5, pp. 1–5, 2019, doi: 10.1088/1757-899X/612/5/052046.

[19] V. K. Bollinadi, M & Damera, "Cloud Computing: Security Issues and Research Challenges," *J. Netw. Commun. Emerg. Technol.*, vol. 7, no. 11, pp. 64–73, 2017, doi: 10.14445/22312803/ijctt-v30p128.

[20] P. . Asifor and M. O. Emezaivwakpor, "Use of Cloud Computing by Professional Librarians in Curtailing the Spread of Covid-19 Pandemic: The Nigerian Scenario," *Inf. Impact J. Inf. Knowl. Manag.*, vol. 13, no. 2, pp. 64–74, 2023, doi: 10.4314/iijikm.v13i2.5.

[21] A. Rashid and A. Chaturvedi, "Virtualization and its Role in Cloud Computing Environment," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 4, pp. 1131–1136, 2019, doi: 10.26438/ijcse/v7i4.11311136.

[22] I. Ahmad, H. Bakht, and U. Mohan, "Cloud Computing – A Comprehensive Definition," *J. Comput. Manag. Stud.*, vol. 1, no. 1, pp. 30–2017, 2017.

[23] C. Mustafa Mohammed and S. R. M Zeebaree, "Sufficient Comparison Among Cloud Computing Services: IaaS, PaaS, and SaaS: A Review," *Int. J. Sci. Bus.*, vol. 5, no. 2, pp. 17–30, 2021, doi: 10.5281/zenodo.4450129.

[24] A. Lokesh, M. Saleem, B. K. Swar, S. Kumar, and R. Sharma, "Cloud Computing: The Emerging Technology," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 4, no. 10, pp. 1503–1510, 2022.

[25] M. S. Kavitha and P. Damodharan, "Software as a Service in Cloud Computing," *Int. J. Recent Adv. Eng. Technol.*, vol. 08, no. 04, pp. 1–4, 2020, doi: 10.46564/ijraet.2020.v08i04.001.

[26] P. Maniatis, "Comparison of Public, Private, Hybrid, and Community Cloud Computing in Terms of Purchasing and Supply Management: A Quantitative Approach," *Int. J. Multidiscip. Res. Anal.*, vol. 06, no. 06, pp. 2359–2369, 2023, doi: 10.47191/ijmra/v6-i6-04.

[27] A. Nyachiro, K. Ondimu, and G. Mafura, "Adoption Strategy for Cloud Computing in Research Institutions: A Structured Literature Review," *J. Comput. Commun.*, vol. 11, no. 04, pp. 63–78, 2023, doi: 10.4236/jcc.2023.114004.

[28] R. Islam *et al.*, "The Future of Cloud Computing: Benefits and Challenges," *Int. J. Commun. Netw. Syst. Sci.*, vol. 16, no. 04, pp. 53–65, 2023, doi: 10.4236/ijcns.2023.164004.

[29] F. K. Aljwari, "Challenges of Privacy in Cloud Computing," *J. Comput. Commun.*, vol. 10, no. 12, pp. 51–61, 2022, doi: 10.4236/jcc.2022.1012004.

[30] T. K. Kousar, S. Bashir, H., Raza, H., "A Survey of Data Security in Cloud Computing," *Int. J. Appl. Eng. Res.*, vol. 9, no. 11, pp. 652–657, 2021.

[31] E. Abdurachman, F. L. Gaol, and B. Soewito, "Survey on Threats and Risks in the Cloud Computing Environment Survey on Threats and Risks in the Cloud Computing Environment," *Procedia Comput. Sci.*, vol. 161, pp. 1325–1332, 2019, doi: 10.1016/j.procs.2019.11.248.

[32] P. Kresimir and H. Zeljko, "Cloud computing security issues and challenges Tetracom View project BusinessLogicIntegrationPlatform View project Kresimir Popovic Siemens 4 PUBLICATIONS 143 CITATIONS Cloud computing security issues and challenges," in *Ieeexplore.Ieee.Org*, 2016, pp. 1–7. [Online]. Available: https://www.researchgate.net/publication/224162841

[33] V. Som and D. R. Kumar, "Cloud Computing & Data Security Threats: Systematic review," *Int. Adv. Res. J. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 421–425, 2023, doi: 10.17148/iarjset.2023.10666.

[34] R. Tadapaneni, N, "Cloud Computing Security Challenges," *Adv. Sci. Technol. Secur. Appl.*, vol. 7, no. 6, pp. 1–6, 2021, doi: 10.1007/978-3-030-68534-8_29.

[35] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, "Cloud computing security issues challenges: A Review," in *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, 2020. doi: 10.1109/ICCCI48352.2020.9104155.

[36] A. Singh, A. Kaur, and D. Gupta, "Reviewing Trust Issues in Cloud Computing," *J. Phys. Conf. Ser.*, vol. 1969, no. 1, pp. 1–10, 2021, doi: 10.1088/1742-6596/1969/1/012043.

[37] V. L. Hallappanavar and M. N. Birje, "Trust Management in Cloud Computing," in *International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM-2019)*, 2019, pp. 1686–1711. doi: 10.4018/978-1-5225-8176-5.ch083.

[38] E. Bajrami and F. Halili, "Service level agreement for cloud computing and usability in service level agreement for cloud computing and usability in," no. October, 2022.

[39] M. Yusuf Haider and S. Selvan, "Confidentiality Issues in Cloud Computing and Countermeasures : A Survey," in *Conference: National Conference On Emerging Computer Paradigms 2016, At NMAMIT, Nitte*, 2016, pp. 1–5.

[40] N. Alrehaili and A. Mutaha, "Cloud Computing Security Challenges," *Iarjset*, vol. 7, no. 8, pp. 120–123, 2020, doi: 10.17148/iarjset.2020.7817.

[41] A. Sharma, B. Keshwani, and P. Dadheech, "Authentication Issues and Techniques in Cloud Computing Security: A Review," in *International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM-2019)*, 2019, pp. 2305–2307. doi: 10.2139/ssrn.3362164.

[42] B. A. Alenizi, M. Humayun, and N. Z. Jhanjhi, "Security and Privacy Issues in Cloud Computing," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1979/1/012038.

[43] S. Mondal, A., Goswami, R. T., & Nath, "Cloud Computing Security Issues & Challenges : A Review," in *2020 International Computer Communication and Informatics*, 2022, pp. 1–6. doi: 10.1109/ICCCI48352.2020.9104155.

[44] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. C. Liu, "Adoption of cloud computing as innovation in the organization," *Int. J. Eng. Bus. Manag.*, vol. 14, pp. 1–17, 2022, doi: 10.1177/18479790221093992.

[45] S. Mangesh Latekar and R. Ravindran, "Resolving Multi-Tenancy Issues Using Cloud Automation," *Int. J. Sci. Res. Eng. Trends*, vol. 6, no. 3, pp. 2395–566, 2020.

[46] E. A. Adeniyi, R. O. Ogundokun, S. Misra, J. B. Awotunde, and K. M. Abiodun, "Enhanced Security and Privacy Issue in Multi-Tenant Environment of Green Computing Using Blockchain Technology," *EAI/Springer Innov. Commun. Comput.*, no. January, pp. 65–83, 2022, doi: 10.1007/978-3-030-89546-4_4.

[47] V. R. Joseph and A. Vakayil, "SPlit: An Optimal Method for Data Splitting," *Technometrics*, vol. 64, no. 2, pp. 166–176, 2022, doi: 10.1080/00401706.2021.1921037.

[48] N. Mücke, E. Reiss, J. Rungenhagen, and M. Klein, "Data splitting improves statistical performance in overparameterized regimes," in *Proceedings of Machine Learning Research*, 2022, pp. 10322–10350.

[49] T. Alam, "Cloud Computing and its Role in the Information Technology," in *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 2020, pp. 108–115. doi: 10.34306/itsdi.v1i2.103.

[50] S. Shreyas, "Security Model for Cloud Computing: Case Report of Organizational Vulnerability," *J. Inf. Secur.*, vol. 14, no. 04, pp. 250–263, 2023, doi: 10.4236/jis.2023.144015.

[51] R. Barona and E. A. M. Anita, "A Survey on Data Breach Challenges in Cloud Computing Security: Issues and threats," in *Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2017*, 2017, pp. 1–8. doi: 10.1109/ICCPCT.2017.8074287.

[52] J. U. Maheswari, S. Vijayalakshmi, N. R. Gandhi, L. H. Alzubaidi, K. Anvar, and R. Elangovan, "Data Privacy and Security in Cloud Computing Environments," in *E3S Web of Conferences*, 2023, pp. 1–9. doi: 10.1051/e3sconf/202339904040.

[53] Agarwal P and Goyal A, "Data Security and Privacy Issues in Cloud Computing: A Review," *J. Netw. Comput. Appl.*, vol. 98, pp. 1–25, 2018.

[54] L. M. Bruma, "Data Security Methods in Cloud Computing," *Inform. Econ.*, vol. 24, no. 1/2020, pp. 48–60, 2020, doi: 10.24818/issn14531305/24.1.2020.05.