Securing Data in the Cloud: An Analysis of Privacy and Security Concern

[1]Mohummed Washeem, [1]Dr Tarun Maini, [1]Sushant Jhingran, [1]Gourishankar Mishra, [1]Pradeep Kumar Mishra.

[1]Department of Computer Science Sharda University Knowledge Park III, Greater Noida, Uttar Pradesh 201310, India

E-mail:
[1]Shaikhwasheem@gmail.com, [1]Taruniitbhu@gmail.com, [1]Sushantjhingran@gmail.com, [1]Gourisankar.mishra@sharda.ac.in, [1]Pradeepkumar.mishra@sharda.ac.in

Abstract.

Storing and processing sensitive information on the cloud has raised serious privacy and security concerns. Cloud computing poses various challenges such as data breaches, loss, insider threats, lack of transparency, shared infrastructure, compliance issues, identity and access management difficulties, data location and sovereignty concerns, and reliance on cloud service providers. To protect sensitive data and comply with data privacy regulations, it is crucial to implement a comprehensive privacy and security strategy in cloud computing. Ensuring the security of cloud computing is vital for both individuals and businesses and different cloud deployment models come with various security risks. A multi-faceted approach involving both providers and tenants is required to tackle these challenges. This article provides an overview of the primary privacy and security concerns in cloud computing and explores various solutions. It also analyzes the challenges of implementing privacy and security controls in the cloud and offers suggestions to improve privacy and security in cloud computing, including encryption, access control, authentication, and advanced persistent threat(APT) prevention. The objective of this paper is to provide recommendations for addressing these concerns and increase awareness of the importance of privacy and security in cloud computing.

Keywords: Cloud computing, Security, Privacy

DOI Number: 10.48047/NQ.2022.20.20.NQ109301 NeuroQuantology2022;20(20):3039-3049

1 Introduction

A fast-developing technology, cloud computing has completely changed how both businesses and consumers access and use computing resources. The hardware and operating system software in the datacenters that offer the apps as services through the Internet are referred to as "cloud computing" in this context. The provision of on-demand computer services, such as servers, storage, databases, software, and networking, through the internet is known as cloud computing. A number of advantages come with cloud computing, such as lower infrastructure costs, more scalability and flexibility, and enhanced accessibility and teamwork. Cloud computing allows for simple, on-demand network access to a common set of reconfigurable computer resources. Computing applications, network resources, platforms, software

services, virtual servers, and computer infrastructure are all examples of resources [3]. The use of various technologies, such as Web services, virtualization, and multi-tenancy, in the cloud computing allows for the provision of distributed resources to the users [15]. There are four prevalent models of cloud computing that businesses adopt. (i) Private cloud: Services under this sort of cloud computing are only made available to certain businesses and are either managed by those businesses directly or by a third party. Other places may offer these services. (ii) Public cloud: It is owned by a business that offers public access to its cloud services and sells them, like the Amazon cloud service. (iii) Community cloud: where a lot of companies use their cloud resources to help one community with a variety of related problems (e.g., purpose, security needs, policy, and compliance issues). (iv) Hybrid cloud, This integrates many cloud infrastructures (public, private, or communal). An example of a hybrid cloud is data kept in a private cloud for a travel firm that is changed by software running on a public cloud. The cloud concept has two key components: multi-tenancy and elasticity. With the former, several tenants may share the same service instance. The latter, however, enables resource allocation to be scaled up or down depending on the needs of the service at hand [4].

1.1 Service Model

Infrastructure-as-a-Service (IaaS): Infrastructure-as-a-Service (IaaS) offers users access to virtualized computing resources, including servers, storage, and networking. Users can control and manage their operating systems, applications, and middleware, but are required to maintain the underlying infrastructure. The customer has the ability to configure servers to meet their specific needs, which typically results in higher maintenance requirements compared to the Platform-as-a-Service (PaaS) model [29].

Platform-as-a-Service (PaaS): The Platform-as-a-Service (PaaS) model offers a development platform to create, operate, and manage applications without needing to be concerned about the underlying infrastructure. The cloud provider takes care of the infrastructure, operating system, and middleware, while the user is accountable for managing the application. The security standards for PaaS are nearly identical to those for IaaS, as both service models share similarities in their virtualized environment features[4].

Software-as-a-Service (SaaS): Software-as-a-Service (SaaS) delivers a comprehensive software package that is hosted and handled by the cloud provider. Users can conveniently access the software application via the internet, without needing to handle any of the underlying infrastructure. SaaS is a term used to describe any application that is hosted remotely and delivered over the internet [29].

The protection of data and applications against illegal usage, accessibility, disclosure, alteration, or destruction is referred to as security and privacy in cloud computing. Cloud computing poses unique privacy and security threats, including illegal access to data, data breaches, loss of data, and lack of transparency in data management. Use of cloud services paradigms violates privacy in a number of ways, including data propagation, probable secondary illegal use, cross-border data flow, dynamic provisioning, theft of private information, uncontrolled usage of cloud services, and [6]. Privacy-preservability is in some ways a more stringent kind of secrecy because both aim to prevent information leaks. Hence, privacy-preservability will likewise be compromised if cloud confidentiality is ever compromised. [7]. Here, we've brought up a crucial subject that might be considered one of the drawbacks of cloud computing, including concerns about security, privacy, and other factors..

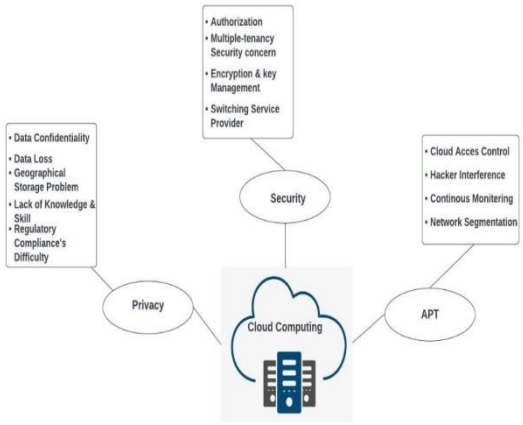

Fig. 1. Ecosystem of Privacy and Security of Cloud Computing

2 Privacy

Several cloud computing approaches are employed to boost an organization's profitability. Businesses may conduct their operations more conveniently and with more benefits thanks to the cloud. Yet, it has several problems with privacy. In the context of business and consumers, privacy refers to safeguarding and appropriately using customers' confidential information as well as satisfying their standards regarding its use [10]. Data from users are kept and stored off of users' premises. Many problems, such as data theft, are brought on by poor data protection and have an impact on each firm. Users of the cloud may be happy if their data is adequately guarded from illegal access. Despite the many benefits that cloud computing offers, there are still a number of worries and problems that need to be resolved before this computing paradigm is widely used [1]. The supplier offers restricted but limitless access to the network and storage, or on occasion they give a free trial, further undermining the idea of cloud computing. Although it is very impossible to guarantee that data backups or duplicates are not stored or used by a particular authority, all of these copies of the data are erased if such a request is made. This is true even if many companies dealing with data proliferation are managed or under no authority of the data owner [2]. The success of cloud computing and its effects on information sharing for social networking and teamwork on a particular project depend on preserving privacy [13].

2.1 Data confidentiality

The process of preventing unwanted access, a server that is outsourced, and gain unauthorized access to and sharing of information is known as data confidentiality. Data confidentiality, which is frequently confused with privacy, refers to guarding against unauthorized access that could reveal private information [20]. Data is encrypted to make it impossible for users to decipher it. Insensitive data is not encrypted, only sensitive data is, Various encryption keys can be used to encrypt various data components, Only information pertinent to this query is encrypted/decrypted during query execution. Storage that is encrypted is an additional option to improve secrecy [11]. Users should avoid directly storing their private information on the cloud since customers do not rely on cloud providers. and internal threats are nearly difficult to eradicate for cloud storage service providers [3].

Any cloud implementation must have strong authentication. User authentication is the primary tenet of access control as everyone may access the cloud along with its entire data over the Internet, access control and authentication are more important than ever in the context of the cloud. [1]. Data is scattered globally on the cloud. The user is not aware of where the data are located and has no control over the steps required to acquire physical access to it. The definition of privacy varies greatly across many various countries, cultures, and legal systems. While an inquiry is ongoing, the issue of whose jurisdiction the data belongs to must be resolved. There are several databases and applications in a distributed system [8].

2.2 Data loss

Data loss is a possibility in the cloud, much like it is with hardware-based storage solutions. There are security solutions for both scenarios, including backups, security software, redundancy, and others. Storage resources are intricate systems that use both hardware and software. Data may be exposed if a minor security compromise occurs on the public cloud. For really sensitive data, it is typically advisable to establish a private cloud, if practical, to minimize such risks [4]. In order to avoid the publication of private information, confidentiality and integrity are obviously important. Integrity ensures that data and computation are not altered in any manner [7]. The greatest options for securing data when it is at rest unquestionably include cryptographic encryption technology [1]. Data is transmitted from one location to another in a cloud system. The majority of data is not encrypted while processing, thus It is necessary to first decrypt the data before processing it for any purpose. Encryption techniques are employed to protect data during transmission. An attacker may locate a gap in a communication channel. The communication can be altered by the attacker [8].

2.3 Geographical data storage issue

Due to the fact that the cloud infrastructure is dispersed throughout several distinct geographic regions worldwide, It is frequently conceivable that the user's data is kept somewhere that is not within the boundaries of the law, It makes the user concerned about laws governing data stored outside of their region and the authorized accessibility of local law enforcement. Change management is becoming the responsibility of the cloud provider across all cloud delivery types., therefore there is a risk that changes might have unfavorable outcomes. This might result from updates to cloud services' underlying hardware or software [1]. With the use of the cloud, databases and application software are moved to massive data centers with questionable data and service administration [12].

On the cloud, data is dispersed globally. The user has no control over the procedures for obtaining physical access to the data and has no awareness of its location. Many nations, cultures, and legal systems have wildly different conceptions about what privacy is. The question of whose jurisdiction the data belongs to must be addressed while an investigation is underway. A distributed system has several databases and applications [8]. Cloud environments have been effectively transported using modern data centers. It assembles hundreds of machines using data center network technologies to provide incredible processing and storage capabilities [7]. These service providers have to have knowledge of protecting large data center buildings and have taken resilience into account along with other availability measures. There is a risk that the physical security of cloud user infrastructure might be compromised more readily, either whenever less secure office environments or remote working are indeed the standard, whether within or outside [1]. The protection of applications is the user's responsibility in the cloud but physical security is the responsibility of the cloud provider, as is probably implementing exterior firewall rules [9].

2.4 Lack of knowledge and skills

Because of a lack of cloud experience that stops them from utilizing the advantages of the cloud and developing technologies, businesses are losing market share and income as a result of the technical skills gap among IT workers, notably in the area of cloud computing. For businesses hoping to maximize the benefits of their multiload strategy and increase their usage of the cloud, this is terrible news. With pay growing and cloud workers expecting greater autonomy, flexible working arrangements, and other advantages, they are now in a talent competition with

companies like Amazon, Google, and Microsoft. Existing datacenter security models are inadequate for the cloud, and administrators must adopt new approaches and expertise specifically designed for cloud computing. While the cloud has the potential to enhance organizational efficiency, it can also make companies vulnerable if they lack the necessary knowledge and expertise [27].

2.5 Regulatory compliance's difficulty

According to the users' Quality of Service (QoS) criteria, cloud computing seeks to provide a network of virtual services that can be accessed by subscribers from anywhere in the world at affordable prices [16]. Although financial services companies have accelerated their usage of the cloud recently, regulatory uncertainties and the complexity of legacy systems continue to impede growth. In contrast to a single cloud, the multi-cloud architecture offers flexibility and options, and an organization may find this to have compelling commercial benefits. The multi-cloud approach, however, makes administration more difficult in several ways, especially with regard to cloud regulatory compliance.

3 Security

Understanding the security standards for data protection has grown essential as firms move more operations to the cloud. It is really possible that third-party cloud computing service providers may take over management of this infrastructure, but there's no assurance that the responsibility and security of data assets will follow. A collection of practices and technology known as cloud security were created to handle the security threats to businesses from both internal and external sources. As they implement their digital transformation plan and integrate cloud-based services and applications into their infrastructure, organizations need cloud security. Cloud computing raises unanswered problems regarding the confidentiality and safety of information that is outsourced. Due to the dynamic abstraction and scalability of the cloud, applications and information that are outsourced have infinite security boundaries and infrastructure [5]. According to Wikipedia, network security, computer security, and information security as a whole all fall under the heading of cloud computing security. It also refers to a significant group of rules, methods, and controls used to protect the infrastructure, data, and applications of cloud computing. [8].

In the realm of cloud computing, security is a critical aspect, particularly for service providers like IaaS, PaaS, and SaaS. The level of security varies depending on the provider's policies and service model. It is worth emphasizing that while service providers implement various security measures, users also play a crucial role in safeguarding their data and applications. This involves setting up robust passwords, frequently updating software and applications, and configuring security settings correctly.

3.1 Authorization

In cloud computing, the concept of authorization risk describes the potential for unauthorized access to resources or data stored there as a result of insufficient or faulty access restrictions. Several reasons, including improper access rights, weak passwords, and insufficient identity and access management (IAM) regulations, might contribute to this risk. Access rights that have been improperly established may allow certain individuals or groups to access cloud resources including storage, databases, and virtual machines. Unauthorized users may access sensitive data or resources if these permissions are not set up appropriately. By putting in place suitable access restrictions, keeping an eye on user activity, and informing users of appropriate security procedures, this risk may be reduced.

Organizations should create robust access controls, enforce strong password rules,

routinely review and update IAM policies, and routinely monitor user activity to identify any illegal access in order to reduce authorization risks in cloud computing.

3.2 Multiple-tenancy security concern

Another distinguishing characteristic of clouds, particularly public clouds, is multi-tenancy. This feature enables cloud providers to more effectively control resource utilization by dividing a virtualized, shared infrastructure among various clients [17]. Risks associated with integrity and confidentiality while sharing resources in cloud computing are connected to multi-tenancy security problems. When numerous users are accessing the same resources, a malevolent user may utilize various cunning methods to get access to all of the other users' resources. There are several new security issues and weaknesses with the multi-tenancy approach. New approaches and solutions are needed to address these emerging security issues and vulnerabilities. For instance, a tenant accessing another tenant's data and returning it to them, or a tenant impacting another tenant's resource sharing. Because of the fluid nature of the cloud, which makes it challenging to choose a specific server that will be used for transnational data transfer, the user is concerned that local regulations may be violated. A host may be used in a public cloud architecture to store data about numerous people. Security risks and dependability decline may result from this [23].

3.3 Encryption and Key Management

The process of converting data into a hidden code that hides the true meaning of the data or information is known as encryption [18]. Even if they have direct physical access to the computer or hard disk, data encryption makes it difficult for unauthorized users to access data [21].Today's IT uses a variety of solutions for data at rest encryption. While having access to all of this knowledge is beneficial for businesses, it gets much more complicated when encryption and key management techniques are used in the cloud. Infrastructure as a Service (IaaS) on the public cloud should be the main focus. The most difficulties and hazards are there in this instance. I'll attempt to list some considerations for a consumer of such a cloud. Of course, these principles may be applied to platform as a service and software as a service (SaaS) (PaaS) offerings, but when they do so within the constraints of these other types of services, the security aspects and solutions are somewhat more constrained by the technologies and what the cloud service provider can provide

3.4 Switching service providers

While most cloud service providers make it easy to migrate data and apps, doing it to a different cloud platform is much trickier and more expensive. Businesses adopting cloud solutions should carefully consider a backup strategy while evaluating cloud providers. Companies should be aware of how difficult it may be to terminate a contract for any reason, such as unhappiness, exorbitant expenses, a cloud provider ceasing operations or altering its business plan, subpar performance, and more. Certain cloud service providers might not have the power, cooling, access to communications, or storage essential to offer the services you will need as company requirements evolve. The majority of suppliers have several sites, each with unique features.

A great strategy to save expenses, improve quality, and acquire global coverage as you expand is to integrate and outsource a lot of your traditional IT requirements to your cloud services provider. Make sure you are familiar with the full variety of optional services and products before changing cloud service providers. Many cloud providers opt to rent servers from third-party service providers as it lowers expenses and increases operational flexibility. However, this increases the

likelihood and inclination for malicious users to steal the data stored on their servers [25]. Although cloud computing service providers bragged about the security and dependability of their offerings, it turns out that the real implementation of these services is not as secure and dependable as they claim [14].

3.5 Cyber Security

Organizations using cloud computing services should prioritize cybersecurity as data and applications stored in the cloud are accessed and managed via the internet, making them susceptible to cyber threats. The reach of cyberspace transcends physical borders, and those who pose a threat through cyber-attacks can come from a range of sources, from individual hackers to highly organized groups backed by governments [28].

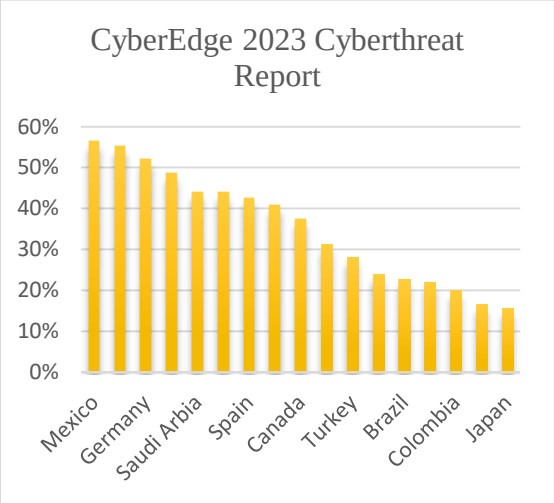

Fig.2 Attacks on organizations in the past year, by country.

The chart provided by CyberEge shows the percentage of organizations that have been successfully attacked six or more times in the last 12 months, broken down by country. On a daily basis, the user is informed of problems related to flawed verification, breached login details, hacked accounts, data violations, and similar concerns [30]. Data can be vulnerable to a range of cybersecurity attacks that can be used for multiple purposes, including (i) unauthorized access to private information, (ii) surveillance of user behavior, and (iii) disrupting system availability for users [31].

4 Advanced Persistent Threat (APT)

A cyber assault known as an APT occurs when an unauthorized user logs onto a network and goes undiscovered for a long time, generally with the intention of stealing information or inflicting harm. APT attacks may be especially damaging when it comes to cloud computing since they can affect several systems and businesses. Strong security safeguards, routine monitoring, and the capacity to react swiftly to possible threats are all essential components of a proactive strategy for combating APT assaults in cloud computing. Cryptography could enhance the adoption of cloud computing technology among security-conscious companies who are suspicious and seek higher levels of security [26].

4.1 Cloud Access Controls

Access Control is a mechanism used in cloud security that allows businesses to formulate various rules that are best suited to their needs in order to control and monitor permissions or access to their corporate data. Cloud apps might not be able to offer the macro-level insight into data and user behavior that access management in cloud security offers due to their on-demand services and mobility. User privacy issues depend on both what important to a system's user and whether malicious intruders are present may use the system with the same ease [6]. To guarantee that only authorized users may access sensitive data and systems, access control measures such as identity and access management (IAM) should be implemented. Poor access control process implementation presents several danger chances, such as when displeased ex-workers of cloud provider firms continue to have remote access to manage client cloud services and can intentionally harm their data sources [1].

4.2 Hackers' interference

The security risk of hackers meddling with cloud computing systems is serious and can have a variety of unfavorable effects on people, companies, and organizations. Access management is one of the most pervasive security risks in cloud computing. The point of access is the secret to everything. Hackers routinely target it as a result. The simplest form of cloud hacking is the brute-force method, which includes testing several login and password combinations. Attackers may wreak havoc and steal data from the cloud after they have gained access to the system, just like they would during any other attack. Phishing is only a stand-in for brute-force attacks, which get user credentials by impersonating a trustworthy third party. Spear phishing is a more sophisticated technique that uses a personalized message to target a specific individual. Threats can range from back doors, trojans, and viruses to blatant hacking assaults [22].

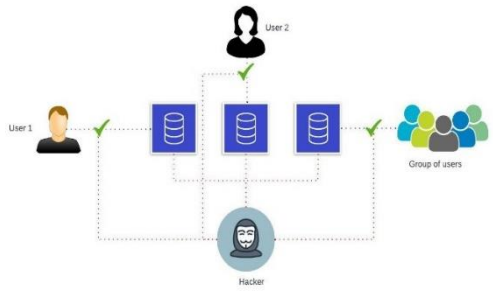

Fig. 2. Hacker's interference

Attackers and cybercriminals continually enhance their connecting and hacking skills, and they quickly learn about the primary targets [19].

4.3 Continuous Monitoring

It's crucial to regularly monitor cloud systems to identify possible APT assaults before they can do any harm. It is become more crucial to make sure continuous monitoring objectives are met in this environment since everything has gone to the cloud and will continue to do so. Particularly, standard approaches for continuous monitoring that are effective for on-premise systems don't necessarily apply to the cloud since cloud assets might be very dynamic and lacking in durability. To assess the possible security threats in a cloud computing setting, it is essential to comprehend the security hazards associated with the three primary cloud deployment models - SaaS, PaaS, and IaaS.

4.4 Network segmentation

If an APT assault happens, segmenting the cloud network into smaller, more secure pieces can help stop its spread. Teams at enterprise-level firms can enhance network performance and security capabilities by using cloud-based network segmentation. A tried-and-true network security strategy called network segmentation divides a network into more manageable, smaller sub-networks that may be divided up by network security teams. When the network has been divided into smaller, more manageable portions, the security staff may provide each segment the best security tools and services.

5 RESULT

The article discusses how cloud computing has transformed the way businesses access computing resources, offering various benefits such as cost savings, scalability, and collaboration. However, it also highlights several security concerns associated with cloud computing, including data confidentiality, data loss, and jurisdictional issues. To address these risks, organizations must prioritize data privacy and security by implementing security measures such as encryption, backups, and redundancy. Additionally, the article identifies several challenges associated with cloud computing, such as lack of technical skills and regulatory compliance issues, which must be addressed to ensure the full potential of cloud computing is realized. The article also emphasizes the importance of strong access controls and password policies to

prevent unauthorized access to sensitive data and systems.

Moreover, the article discusses the risks of cyber threats to cloud computing systems, such as Advanced Persistent Threats (APTs), which can cause significant damage to businesses. To protect against these threats, organizations must adopt proactive strategies such as continuous monitoring and network segmentation to prevent lateral movement of attackers.

Overall, the article provides valuable insights into the benefits and challenges of cloud computing and emphasizes the need for organizations to prioritize data privacy and security to ensure the success and widespread adoption of cloud computing.

6 CONCLUSION

In the IT industry, cloud computing is currently defined and discussed in a variety of contexts and with different meanings. The primary concept is that utilizing the cloud is equivalent to utilizing a server provider that could host services for users that are networked to it. As a result of the advancement of computing, communication, and networking technologies, technology has advanced in this direction. The ability to connect quickly and consistently is essential for cloud computing. In conclusion, it is critical to address privacy and security problems in cloud computing in order to guarantee the security and protection of sensitive data. While cloud computing has many advantages, including scalability, flexibility, and cost-effectiveness, it also comes with a number of concerns, including the possibility of data breaches, cyberattacks, and illegal access. Data breaches, denial of service assaults, virus attacks, and insider threats are a few of the major security and privacy problems in cloud computing. Data loss, financial loss, reputational damage, and legal responsibility are all possible outcomes of these assaults. Cloud computing will need ongoing research to address privacy and security concerns. Future work may involve techniques such as homomorphic encryption, confidential computing, federated learning, zero-trust security, and blockchain-based security. These approaches have the potential to protect sensitive data in the cloud, but there are still technical and regulatory challenges to overcome.

In the end, it is critical that users and cloud service providers collaborate to make sure that cloud computing is a safe and dependable platform for storing, handling, and gaining access to sensitive data. Organizations may profit from cloud computing while reducing the dangers involved by adopting a proactive approach to security and privacy.

References

[1] Sen, Jaydip. (2013). Security and Privacy Issues in Cloud Computing. 10.4018/978-1-4666-4514-1.ch001.

[2] Aljwari, F. K. (2022). Challenges of Privacy in Cloud Computing. Journal of Computer and Communications, 10(12), 51–61.

[3] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. In International Journal of Distributed Sensor Networks (Vol. 2014). Hindawi Limited.

[4] Sangeetha, R., & Silambarasi, M. (2019). DATA SECURITY IN CLOUD COMPUTING (Vol. 6). JETIR.

[5] Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: A review. Procedia Computer Science, 112, 1516–1522.

[6] Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. In Future Internet (Vol. 14, Issue 1). MDPI.

[7] Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. IEEE Communications Surveys and Tutorials, 15(2), 843–859.

[8] Rahul, S., & Rai, J. (n.d.). Security & Privacy Issues In Cloud Computing. www.ijert.org

[9] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.

[10] Pearson, S., 2013. Privacy, security and trust in cloud computing (pp. 3-42). Springer London.

[11] Zhou, M., Zhang, R., Xie, W., Qian, W. and Zhou, A., 2010, November. Security and privacy in cloud computing: A survey. In 2010 Sixth International Conference on Semantics, Knowledge and Grids (pp. 105-112). IEEE.

[12] Subashini, S. and Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), pp.1-11.

[13] Chang, V. and Ramachandran, M., 2015. Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on services computing, 9(1), pp.138-151.

[14] Chen, D. and Zhao, H., 2012, March. Data security and privacy protection issues in cloud computing. In 2012 international conference on computer science and electronics engineering (Vol. 1, pp. 647-651). IEEE.

[15] Ali, M., Khan, S.U. and Vasilakos, A.V., 2015. Security in cloud computing: Opportunities and challenges. Information sciences, 305, pp.357-383.

[16] Garg, S.K., Versteeg, S. and Buyya, R., 2013. A framework for ranking of cloud computing services. Future Generation Computer Systems, 29(4), pp.1012-1023.

[17] Takabi, H., Joshi, J.B. and Ahn, G.J., 2010. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), pp.24-31.

[18] Kumar, A.V., Monica, K. and Mandadi, K., 2023, January. Data Privacy Over Cloud Computing using Multi Party Computation. In 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 262-267). IEEE.

[19] Ahmed, A., Kumar, S., Shah, A.A. and Bhutto, A., 2023. CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES. Tropical Scientific Journal, 2(1), pp.1-8.

[20] Thushari, P.D., 2022, November. Current security and privacy issues, and concerns of Internet of Things (IoT) and Cloud Computing: A review. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 13-17). IEEE.

[21] Achar, S., 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), pp.379-384.

[22] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), pp.9493-9532.

[23] Jangjou, M. and Sohrabi, M.K., 2022. A comprehensive survey on security challenges in different network layers in cloud computing. *Archives of Computational Methods in Engineering*, *29*(6), pp.3587-3608.

[24] To assess the possible security threats in a cloud computing setting, it is essential to comprehend the security hazards associated with the three primary cloud deployment models - SaaS, PaaS, and IaaS - that have been previously outlined.

[25] Bala, S., 2019. Cloud computing and database security. *Int. J. Adv. Stud. Ecol., Develop. Sustainability*, *6*(1), pp.47-55.

[26] Mathur, P., Gupta, A.K. and Vashishtha, P., 2019. Comparative study of cryptography for cloud computing for data security. *Recent Adv Comput Sci Commun*, *12*, pp.1-00.

[27] Mallisetty, S.B., Tripuramallu, G.A., Kamada, K., Devineni, P., Kavitha, S. and Krishna, A.V.P., 2023, January. A Review on Cloud Security and Its Challenges.

In *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 798-804). IEEE.

[28] Haque, A.K.M., 2019. Need for critical cyber defence, security strategy and privacy policy in Bangladesh-hype or reality?. *arXiv preprint arXiv:1906.01285*.

[29] Haque, A.B., Mahmood, S., Ahmed, M., Ali, M.H. and Piyal, N.M., 2020. Challenges and opportunities in mobile cloud computing.

[30] Salek, M.S., Khan, S.M., Rahman, M., Deng, H.W., Islam, M., Khan, Z., Chowdhury, M. and Shue, M., 2022. A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. *IEEE Internet of Things Journal*, *9*(11), pp.8250-8268.

[31] Haque, A.B., Bhushan, B. and Dhiman, G., 2022. Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems*, *39*(5), p.e12753.