(IJIASE) 2024, Vol. No. 10, Special Issue No 1 **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

Identity and Access Management in the Cloud

Subash Banala
Capgemini
Senior Manager
Financial Services & Cloud Technologies
USA

[1]*Received: 06 June 2024; Accepted: 20 August 2024; Published: 23 August 2024*

ABSTRACT

Cloud security includes controls and process enhancements to deter potential attackers and identify problems as soon as they appear. Data backup measures should be considered in cloud security in an emergency or security incident. A multitude of cloud security options employ various methodologies to cater to private, public, and hybrid clouds. Customers are in charge of protecting their own assets, including data, apps, and virtual machines; cloud providers handle hardware and software security. Public cloud systems use this shared responsibility notion.

Even though the cloud offers many benefits and services, there are specific issues with safe data access and storage. Cloud security raises numerous problems, such as seller lock-in, multi-tenancy, carrier disruption, data loss, and loss of control. This study examines the primary issues with clouds and potential solutions. It also discusses several ways to protect data in the cloud through encryption techniques, authentication, and other measures and has identified data loss as a major risk.

INTRODUCTION

Cloud computing is a shared pool of reconfigurable computing assets (such as networks, servers, storage apps, and services) that can be quickly supplied and deployed with little administrative labour. It is a model for offering on-demand services to these resources. It's a paradigm offering storage and processing power; sometimes, it's just a way to get software and data from the cloud. Cloud computing is widely used in business and education since it offers its clients cutting-edge features like data availability, scalability, and flexibility. Cloud computing also reduces costs by enabling the sharing of records throughout the organisation. Businesses can use cloud storage to keep their data accessible to their shareholders. Google Apps is a demonstration of cloud computing. Despite its many features and advantages, The cloud has several problems with safe data access and storage. Cloud security is fraught with issues, including carrier disruption, data loss, loss of control, multi-tenancy, dealer lock-in, etc. In this paper, the security concerns related to the cloud computing concept have explicitly been studied. The main objective is to learn about different kinds of attacks and how to strengthen the cloud model's resilience. Because data storage is used to forecast insights for future business choices, security in cloud applications is essential.

[1] *How to cite the article:* Banala S.; Identity and Access Management in the Cloud; *International Journal of Innovations in Applied Sciences and Engineering;* Special Issue 1 (2024), Vol 10, No. 1, 60-69

(IJIASE) 2024, Vol. No. 10, Special Issue No 1 **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

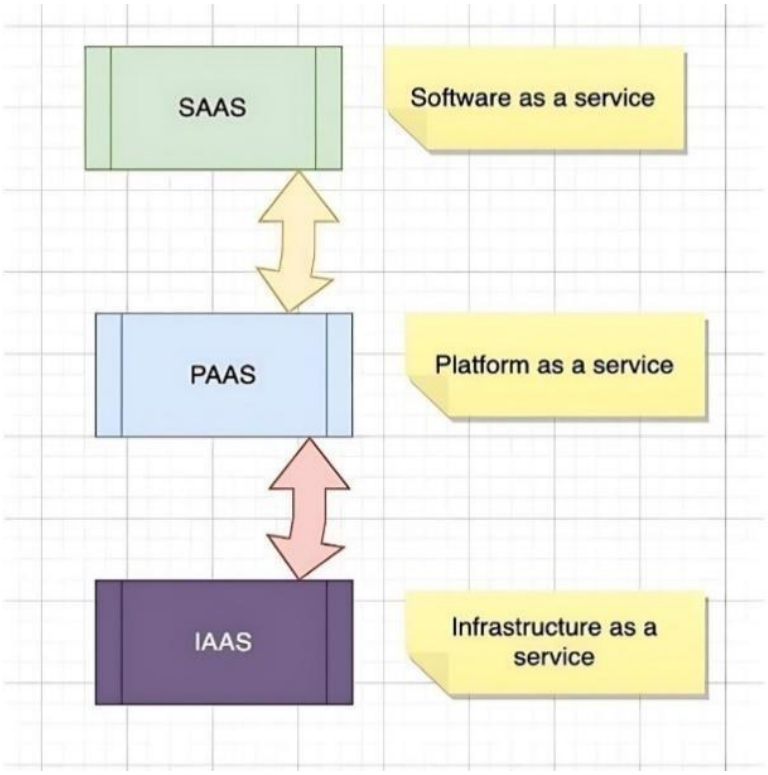


Figure 1: Cloud Service Models

Three types of cloud service models are available to meet company needs. Cloud security benefits vary throughout SaaS, PaaS, and IaaS, depending on the degree of abstraction and control over the underlying cloud architecture.

Main areas on which cloud security should be concentrated:

1. Management of Identity and Access

2. Protecting Information in the Cloud

3. Section using the OS

4. Guarding Network Layer Security

5. Overseeing Incident Response, Audit Trail, Alerting, and Security Monitoring

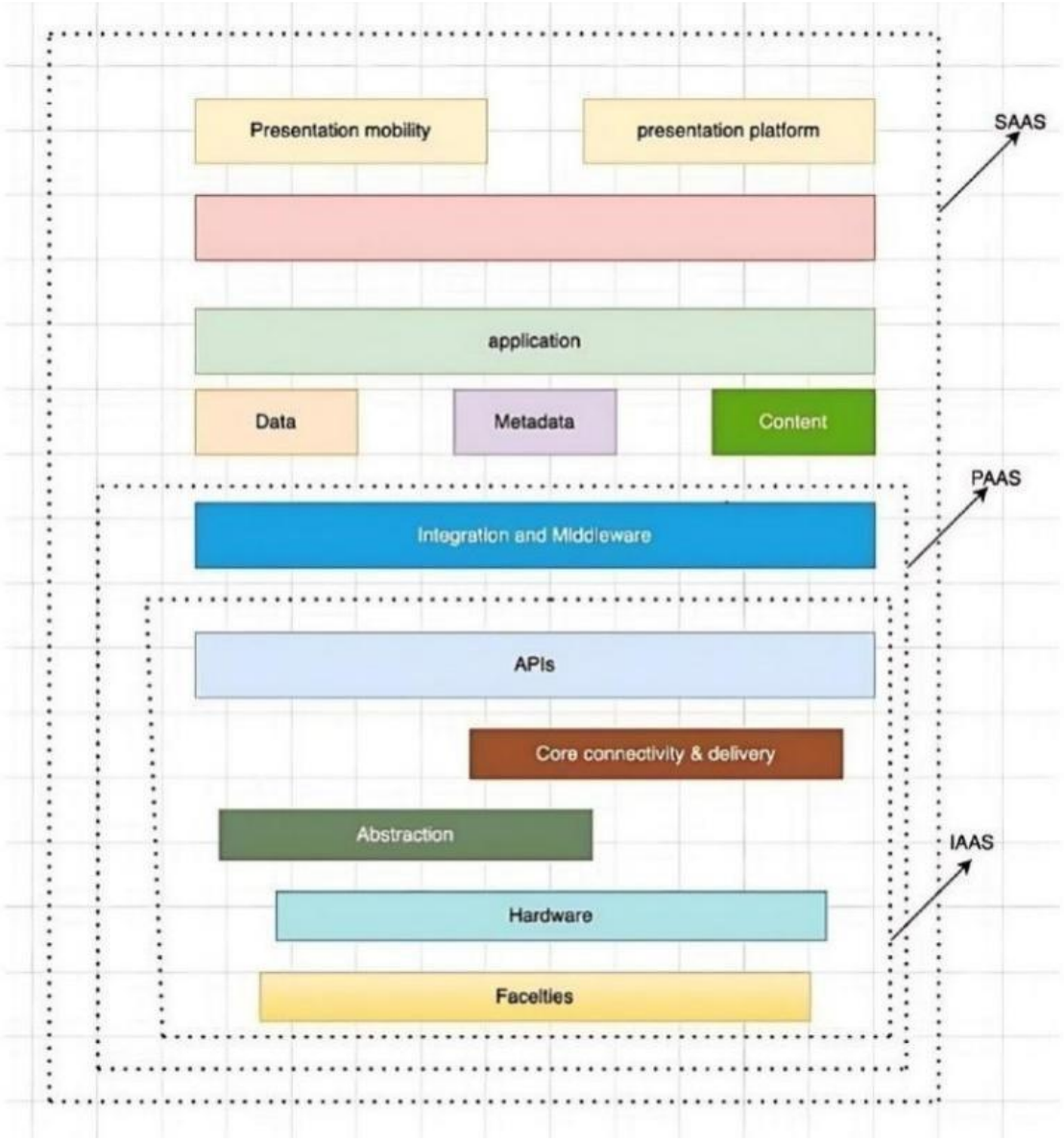


Figure 2: Cloud Security Architecture

This architecture explains cloud infrastructure, security layer types, and their relationships.

LITERATURE REVIEW

Since the most common concern regarding cloud computing is data security, we were able to obtain solid knowledge by consulting numerous study articles. The majority of them offer solutions that increase efficiency and shield cloud data from hackers.

Threat-specific risk assessment in the cloud is the title of the article. In 2021, this article will be published. The context concerns the computation of a threat-specific risk factor or parameter based on threats supplied by the customer that can secure that data using the necessary security measures at a reasonable cost. According to the author, the majority of the security risk evaluation techniques now in use are asset-based and concentrate on assessing the risk connected with the asset in its entirety rather than the risk related to various threats to the asset. In this study, he suggested that threat-specific risk assessment can assess and pinpoint more precise, effective responses that consider dangers as reported by the user.[1] Cloud Chain: A Cloud Blockchain Using Shared Memory Consensus and RDMA is the article's title.

In 2022, this article was released. The article's context is an inventive blockchain that is focused on the cloud called Cloud Chain. In order to empirically evaluate our concept, the Cloud Chain is built on a RoCEv2-based testbed. The

outcomes confirm the viability and effectiveness of the Cloud Chain. This paper's primary goal was to develop Cloud Chain, which combines blockchain technology with cloud shared memory and RDMA to deliver great performance while maintaining decentralisation and safeguarding against Byzantine opponents. The author discovered that clients will favour permissioned blockchains with strong cloud chains that have shared memory and RDMA. --[11]. The primary issue of theft is highlighted in the article A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats.

It will provide infrastructure, platform, and software for some data breaches with on-demand services. The cloud provider faced many challenges in maintaining cloud security. The solution put out by the author increases the protection of the data. The approach divides the data into sections and stores it in the cloud while maintaining encryption so that anyone can unread the encrypted data. --[9] The article, published on May 28, 2020, is titled Privacy-Preserving Linear Regression on Distributed Data via Homomorphic Encryption and Data Masking. The primary purpose of data masking is data security; it uses techniques such as substituting bogus data for actual data. The format remains unchanged, but there are certain key ideas for replacing the real data with bogus data. When data is placed in any region, it should be replaced. utilised a method that involved data substitution and data scrambling as well. Ultimately, maintaining high availability and data security is the primary goals of data masking.[8]

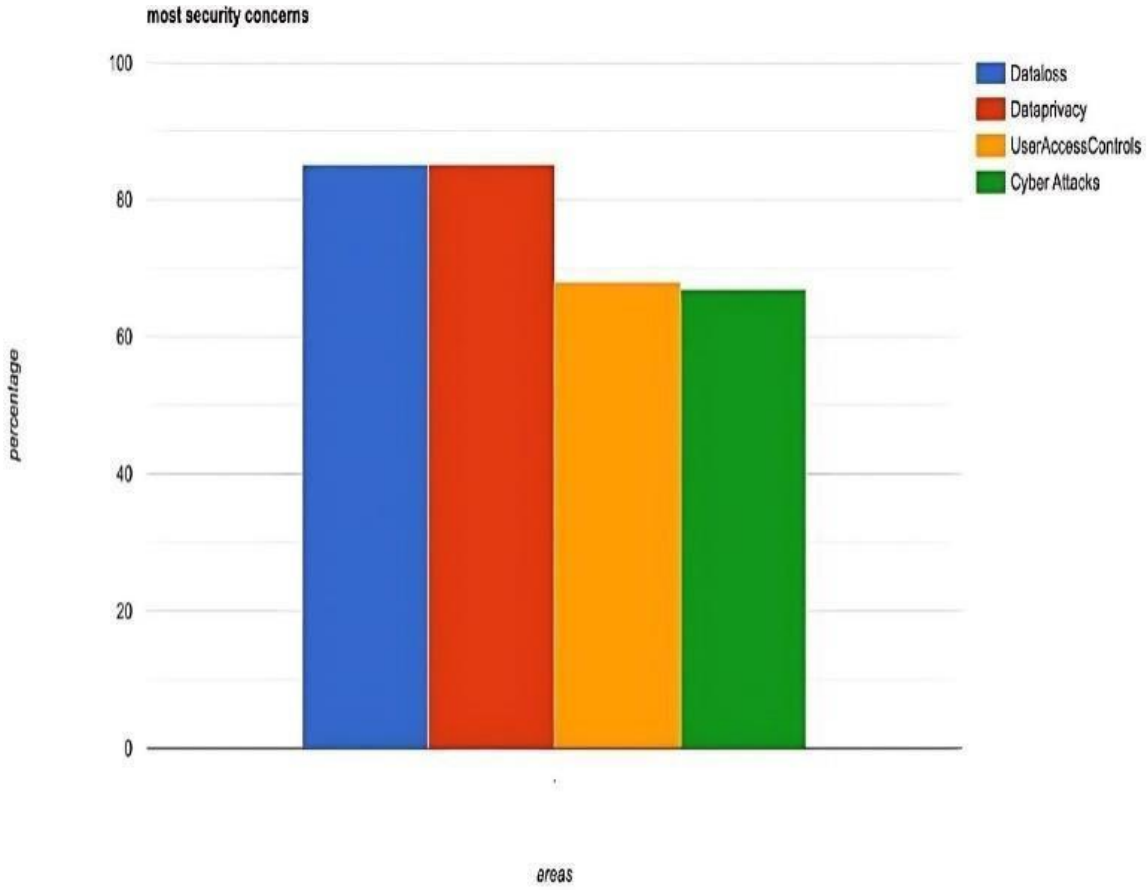


Figure 3 Security Concern in cloud

The above graphic illustrates the regions where the majority of clouds are experiencing problems and the locations where we need to focus our efforts in order to find a solution or lower the risks. Thus, it follows that we should focus more on data loss and security.

SECURITY ISSUES IN CLOUD

(a) IP spoofing: By using IP spoofing, the attacker will substitute a phoney ID for the original IP address. This phoney IP address that has been injected is used to steal and misuse data. Man in the middle refers to IP spoofing, in which a hacker eavesdrops on a conversation between two computers and takes advantage of the IP packets.

b) Theft of accounts: Attackers use stolen credentials to get access to the cloud and steal crucial data. Attackers gain access to cloud storage by using phishing emails, passwords, and complete credentials.

c) Multi-tenancy: Tenant data will also be affected if a cloud host becomes the target of a cyberattack. There is a strong correlation between data security and cloud service provider. Multitenant cloud services are susceptible due to insufficient bandwidth and traffic isolation, which allows hostile tenants to attack other tenants housed in the same cloud service centre.[2]

d) Data Breaches: When personal information is accessed or taken without consent, it is called a data breach. There may be attacks whose main objective is data theft. Potential reasons of data breaches include human error, inadequate security protocols, and security vulnerabilities in commonly used programs [4].

e) Problems with Cloud Identity and Access Management: While supply chain vulnerabilities are typically addressed in relation to APIs (see above), they might also arise from other cloud components. Code that is reused from open-source libraries is a common feature of software, regardless of whether it is intended for cloud computing or not. You now have a vulnerability in your program if it exists in the open-source software you are utilising.

f) Abuse and Reprehensible Use of the Cloud: Hackers and other third parties will launch various, vague attacks on the cloud. others Hackers can launch a variety of assaults, such as password or key cracking, by taking advantage of favourable premises, such as straightforward procedures and relatively undefined access to cloud services.

g) Manipulation of hidden fields: These are essentially fields that are hidden on websites that hold information about page details. If an attacker manages to obtain these fields, they may easily alter them to make page details phoney, which will create a significant loss for the user since they are unable to write pages.

h) Attack on fundamental infrastructure: With a thorough understanding of the cloud's architecture, they can also target an important aspect of cloud computing. The most crucial element of any organisation is its infrastructure, so any information stored on the cloud should be safeguarded to prevent hackers from accessing it and using it to compromise the organization's essential infrastructure.

i) Denial-of-Service attack (DDoS): DDoS attacks target cloud servers or the network that surrounds them in an attempt to disrupt or stop services. These might come after botnet and phishing attacks, in which hackers break into a system and use an already-built remote computer "army" to conduct an attack. Any cloud-based data could be impacted by the attack, which also makes it possible for other hackers and outside parties to access it.

j) Misconfigured data: The cloud may have different settings when we use it, and when services are expanded, the cloud settings may also alter. Therefore, every business uses many cloud providers, and the business needs to be aware of how to configure data in the cloud.

TECHNIQUES

The on-demand, pay-per-use provision of computer services via the internet, encompassing applications, computing resources, storage, databases, networking resources, etc., is known as cloud computing. The current growth in demand for cloud computing skills is correlated with an increase in the requirement for cloud computing services. Its three main service model types are Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). Businesses of all sizes can select from a range of cloud models, including public, private, hybrid, and community clouds, depending on their needs, as a result of the widespread use of cloud services.

a) Install antivirus software: All of the security measures stated above can be utilised to safeguard your data, but sometimes the problem isn't with cloud security—rather, it's with the system you are using. Accessing your account will be effortless for hackers if your system is not adequately secured. You expose yourself to viruses that provide entrance opportunities in these situations.

b) Encrypting cloud data: In order to prevent others from accessing or changing your data, any data uploaded to the cloud should be completely changed by providing some external, important configuration. This includes encrypting data by adding a password and using an OTP method.

c) Algorithms for data backup: Attacks against clouds are frequent and will never end. Data needs to be properly safeguarded somewhere with a backup. Numerous algorithms exist, such as hybrid backup, object level backups, cloud to cloud, deduplication, etc. These are the most popular ones that a reputable cloud service company ought to employ.

d) Cypher Cloud: All other products and services, including as Office 365, Amazon online services, and Google apps, are protected by an application known as Cypher Cloud. It ensures that encryption, ongoing traffic monitoring, and virus scanning will safeguard the data.

e) Multi-factor authentication: In an MFA system, each user's identity is verified by two or even three authentication factors, such as a smart card, smartphone, USB key, fingerprints, etc., in addition to the first authentication factor, which is often a password. The attacker has at least one extra obstacle to overcome before reaching the target if any factor is compromised. The need to set up MFA systems for cloud services is currently very high.[3]

f) Data Masking: Data masking is primarily used to secure sensitive data by producing a different version of the data that is difficult to identify or reverse. It is crucial that the data remains consistent and maintains its usability across several databases. A few cloud-related concepts are explained in this essay along with some of their advantages, which include scalability, platform independence, adaptability, and reliability. While there are many security risks associated with cloud computing, we have discussed a few of them in this paper along with preventative measures that can be taken to ensure the security of communications and eliminate security risks.

The main purpose of this survey is to look at all of the problems, including attacks, data loss, and illegal access to data, as well as potential solutions. Because cloud computing is dynamic and complex, the standard security solutions provided by the cloud environment do not transfer well to its virtualised contexts. The Cloud Security Alliance (CSA) and NIST are two groups that are engaged in this.

g) SASE (Secure Access Service Edge): This solution combines network security services with wide area networks (WANs).

Cloud advantages:

- Boots performance
- inexpensive
- a decrease in complexity
- Adaptability
- Security of data

Regardless of where cloud users are located, security is increased since the standards are maintained consistently. in order to prevent new security threats from being encountered by the cloud service provider without the need for extra infrastructure. Among the security features that can be implemented in SASE are encryption, multi-factor authentication, threat prevention, DNS, Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), and Zero Trust Network Access (ZTNA).

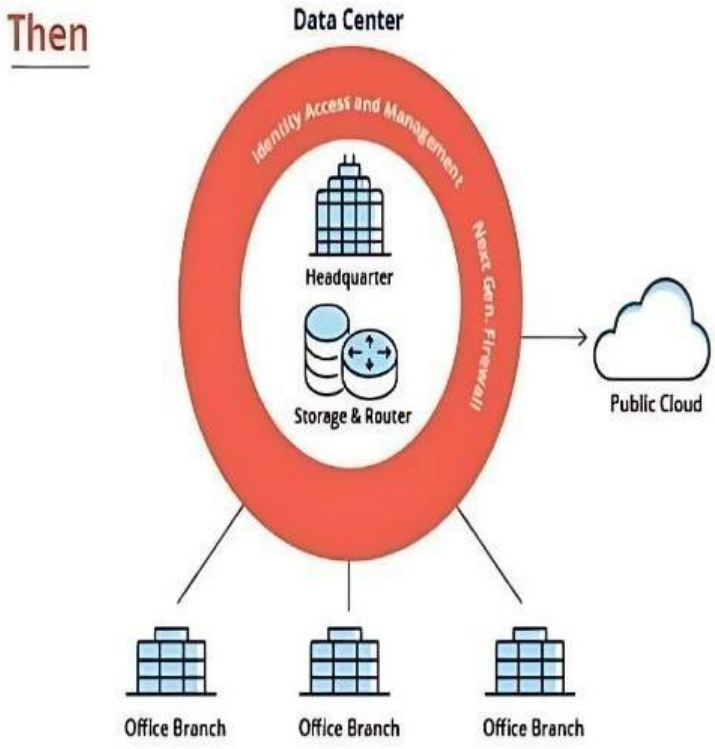


Figure 4: Outdated Sase approach

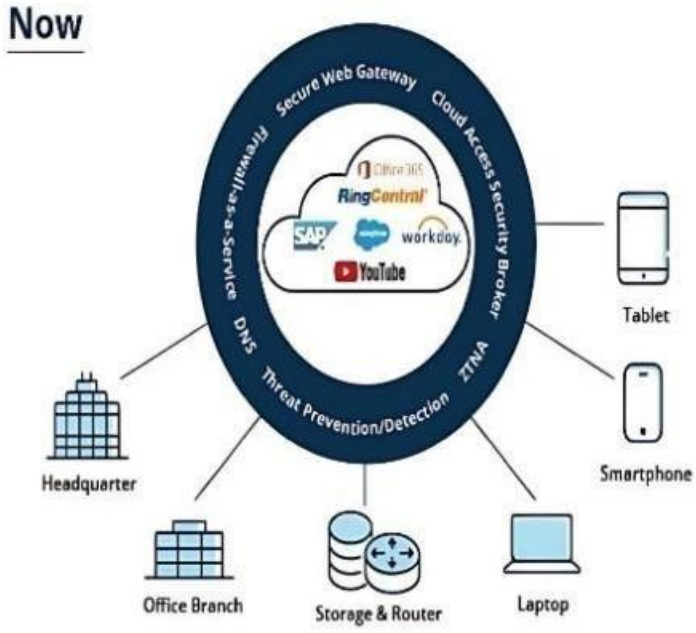


Figure 5: Trending Sase approach

Up to 40% of businesses will use SASE tactics by 2024, which is a significant increase from the 1% that did so in 2018.

h) Managed Cloud Security Posture (CSPM): CSPM improves cloud security. It guarantees compliance in the cloud and automates security. The following is how CSPM works well for businesses:

1. Misconfigured cloud environments are simple to identify and fix.
2. A novel idea for various cloud configuration uses.
3. Constantly monitor the state of the configuration.
4. Working well with PaaS and SaaS systems even in a multi-cloud setup.
5. Maintains accurate records of permissions, encryptions, and storage bucked.

TOOLS FOR CLOUD SECURITY

a) Zero spam: A well-known cloud security solution for email defence is Zero spam. Its primary product is a high-performing cloud-based email security solution that can be integrated with Office 365 and other email providers. Partners are able to provide their clients with total protection against sophisticated attacks by integrating Office 365 with Zero spam.

b) Web Application Firewall by Cloudflare:

Our sophisticated application security offering is built around the Cloudflare web application firewall (WAF). It detects irregularities and malicious payloads, thwarts DDoS attacks, protects against bot attacks, and keeps an eye out for risks to the browser supply chain.

c) TOPIA:

By actively identifying risks and removing threats with unique xTags TM and Patchless Protection TM, which go beyond conventional vulnerability management, this cloud-structured system provides a solution. You are always aware of the cyber security of your organisation since TOPIA does real-time risk assessments and keeps an eye on all repair stages. With TOPIA's risk-prioritization criteria, automatic security patch, and helpful reports on team growth and productivity, you can accomplish more work faster.

d) Zscalar:

Regardless of device, location, or network, this SaaS security platform offers users quick and secure connections to their apps. Utilising any network, it serves as an intelligent switchboard to protect communications between users and

apps as well as between machines. Additionally, it is a cloud firewall that permits quick and safe network connections. It is a fantastic tool for networked private access as well as Internet access.

e) Orca Security: This cloud security technology finds, ranks, and fixes security threats and legal violations throughout the cloud infrastructure. When a customer connects to the Orca console, it gathers metadata from their cloud accounts and workloads. Orca cloud vision provides complete stack visibility into the cloud architecture by leveraging Side Scanning technology. Additionally, it enhanced risk detection, strategically corrected, increased efficiency, and prioritised crown jewels.

CLOUD BLOCK CHAIN

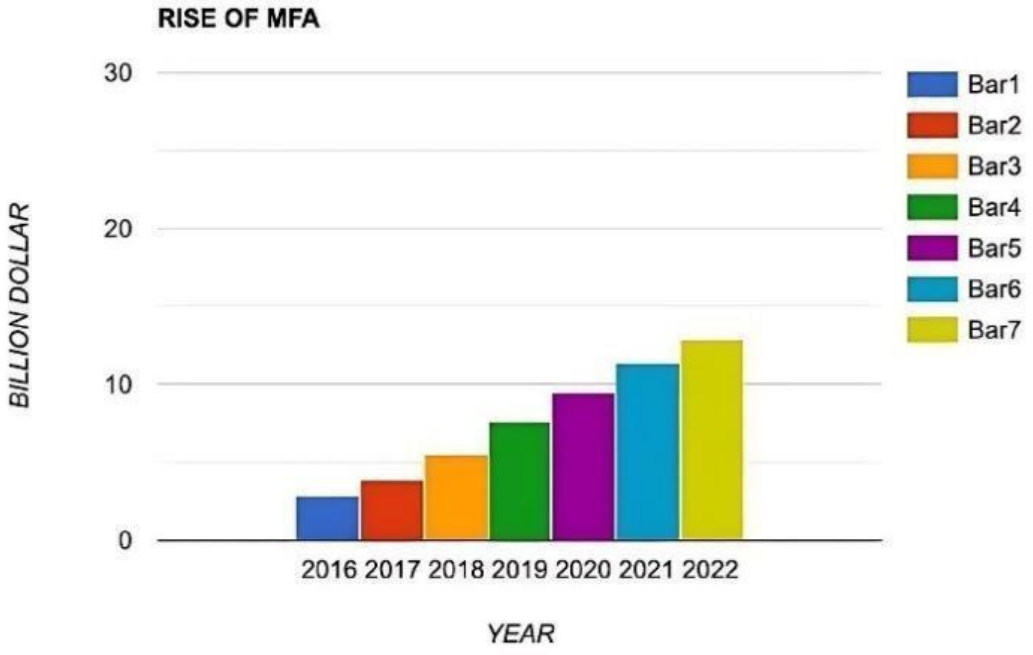
a) Decentralise: Using a server will increase the complexity of calculating the data required by the business. When data is lost or the server is unable to make modifications, it might make the data more vulnerable to hacking by others. The block chain method is an efficient way to tackle this problem. It allows for the creation of many copies and the maintenance of multiple servers, which can be helpful in the event that a single server fails.

b) Service tracking: It is crucial to maintain track of the vehicles and products associated with your company. Although a company's tracking system may not be very effective, block chain technology provides sufficient methods for system maintenance.

c) Improved Data Security: Most IOT-stored data relate to a homeowner's personal information, such as voice and video recordings, household items, assets, and daily schedules. Such data breaches put people's security at risk, increasing their susceptibility to crimes like robberies and the unlawful sale of personal data for financial gain.

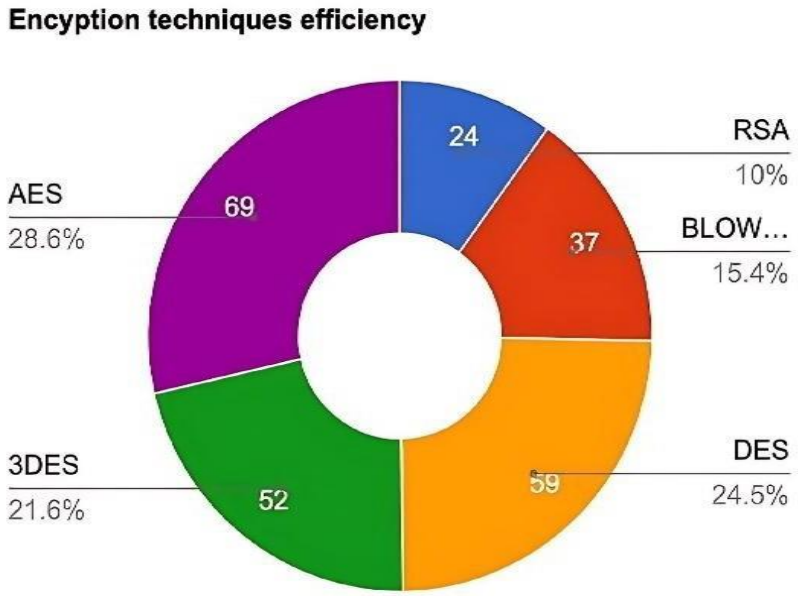
d) Geo-Independence: A lot of businesses now use cloud computing to store and manage their location-based data. The likelihood of data loss and server failure is reduced. Data replication and data transmission to appropriate destinations are made possible by the block chain algorithm.

RESULT



Plot1: The aforementioned figure illustrates the ways in which multifactor authentication has improved the business sector annually. This makes it clear that MFA is the preferred method in the current cloud security trend.

(IJIASE) 2024, Vol. No. 10, Special Issue No 1 e-ISSN: 2454-9258, p-ISSN: 2454-809X



Plot 2: The plot above illustrates the effectiveness of encryption techniques such as RSA, Blowfish, DES, and AES. AES is the most effective because of the key length option.

The cloud has grown in importance as a resource in recent years for all business sectors. Problems are frequent, but if they are ignored, their business may suffer. The most successful strategies were discovered simultaneously. By using security solutions, you may prevent hackers from accessing your data and safeguard it with secure techniques. Employing novel algorithms such as blockchain technology can facilitate the encryption of data using optimal methods and safeguard against data loss.

TABLE 1. Techniques and their purpose

Techniques	purpose
Multi-factor authentication (MFA)	which includes a two or more forms of authentication to enhance security and avoid theft
Data masking	helps prevent unauthorized access to sensitive data by obscuring it, even if an attacker gains access to the system
Encyrption algorithms	which convert data into a format that is unreadable format which has a security key to decrypt it.
SASE(Secure Access service edge)	a combination of all multi security services which increases the data protection in cloud.
CP SM (cloud security poster management)	cpsm provides protection with many services like compliance monitoring, threat detection and access controls
Cipher cloud	take cares of data protection in cloud through encryption, tokenization.
Data backup algorithms	saves the redundant data copies prior to data loss or any damage in cloud.

FINAL ANALYSIS

Data in cloud computing settings is protected by a variety of security techniques, including Cypher Cloud, SASE (Secure Access Service Edge), CPSM (Cloud Security Posture Management), data masking, encryption, and multi-

factor authentication. Comparing their accuracy is inaccurate though, as they have different uses and are applied in various situations. A summary of the entire analysis is completed in Table 1.

CONCLUSION

IT security in the cloud is a top priority for any company that want to protect its data and apps from hackers. It is already commonly known that cloud computing can benefit organisations by helping them maintain a strong security posture. Along with these advantages, cloud security also offers the potential to scale, improve DDoS defence, raise stability and availability, and reduce initial and continuing operating and administrative costs. These days, the most widely used on-demand solution while making business decisions is cloud computing. Thus, it is essential to safeguard the stack holders' data.

There are issues, but they can also be resolved. As a result, the developer must exercise caution when developing algorithms and ensure that they satisfy the requirements of the software. In this study, data loss or damage has been prioritised.

REFERENCES

[1] Armstrong Nhlabatsi, Threat -Specific Security Risk Evaluation in the Cloud, iee transactions on cloud computing, VOL. 9, NO. 2, april-june-2021

[2] A. Jyothsna, A survey on efficient security algorithm in cloud computing, December 2016 International Journal of Pharmacy and Technology.

[3] Rajani Sajjan, Vijay dhonge, Multi-factor Authentication as a Service for Cloud Data Security, June 2016 Conference: International Journal of Computer Sciences and Engineering Volume: 4.

[4] Naresh vurukonda1, B.Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing,2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016)

[5] Dr.K.Rama Krishna Reddy, Data Masking Techniques in Cloud Computing, International Journal of Scientific Research and Review,2018.

[6] Wayne J. Brown, Vince Anderson, QingTan, Multitenancy-Security Risks and Countermeasure,15th International Conference on Network-Based Information Systems.

[7] Ahmed Albugmi, Madini O. Alasaffi, Data Security in Cloud Computing, fifth international conference on future generation communication technologies.

[8] Rohit bhadauria, sugata Sanyal, A Survey on Security issues in Cloud computing, International Journal of Computer Applications • April 2012

[9] R.Barona, E.A. Mary Anita, A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats,2017 International Conference on circuits Power and Computing Technologies

[10] GUOWEI QIU, YINGLIANG ZHAO Article Linear Regression on Distributed Data by Homomorphic Encrypt ion and Data Masking.

[11] Minghui Xu, Shuo Liu, Dongxiao Yu, Xiuzhen Cheng Cloud Chain :A Cloud Blockchain Using Shared memory consenses with rdma. ieee transactions on computers, VOL. 71, NO. 12, DECEMBER 2022.

[12] Mrs. Anjali Sharma, Dr. Garima Sinha, An Efficient Approach on Data Security with Cloud Computing Environment: A Comprehensive Research, Vol.12 No.14 (2021), 1372 – 1382

[13] Praveen Challagidad, Local and Remote Recovery of Cloud Services Using Backward Atomic Backup Recovery Technique for High Availability in Strongly Consistent Cloud Service: Recovery of Cloud Service for High Availability, International Journal of Advanced Pervasive and Ubiquitous Computing, Volume 11,Issue 4 ,October-December 2019

[14] Zina Balani, Cloud Computing Security Challenges and Threats 2020 8th International Symposium on Digital Forensics and Security (ISDFS)

[15] Jyoti Bolannavar, CSPM, CSPM- Cloud Security Posture Management (Comprehensive Security for Cloud Environment),International Journal of Scientific Research in Computer Science, Engineering and Information Technology.