IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

A Comprehensive Review of Security Measures and Implementation Challenges in Cloud Computing

Sanika Satish Lad, Sanika Rajan Shete, Disha Satyan Dahanukar, Anant Manish Singh
Department of Computer Engineering
Thakur College of Engineering and Technology, Mumbai, India
ladsanika01@gmail.com, sanika.shetee@gmail.com, dishadahanukar@gmail.com, anantsingh1302@gmail.com

Abstract: *Cloud computing has emerged as a cornerstone technology in the IT industry, transforming industries by providing flexible, scalable computing resources but the widespread adoption of cloud services has raised serious data security and privacy concerns. Cybercriminals always pose a threat by targeting sensitive information stored on cloud servers. To mitigate these risks, cloud encryption has emerged as an important safeguard, aiming to protect users data from unauthorized service providers against them and against unauthorized malicious hackers This paper examines the ongoing data security issues associated with cloud computing and analyzes the features and structures of cloud encryption. By examining complex approaches to cloud cryptography including encryption, key management and access control, this paper aims to provide insights into how these technologies can shape the security level of cloud-based systems confidentiality, integrity and availability are maintained, ensuring trust and confidence in cloud computing ecosystems.*

Keywords: Cloud computing, Data security, Privacy, Cybercriminals, Cloud cryptography, Encryption, Key management, Access control

I. INTRODUCTION

Cloud computing represents a paradigm shift in the way IT resources are provisioned, accessed and managed. At its core, cloud computing offers a model for delivering on-demand access to a shared pool of configurable computing resources (such as networks, servers, storage, applications and services) over the internet. This transformative technology enables organizations and individuals to access computing power and storage capacity without the need for extensive infrastructure investments or physical hardware maintenance. It only takes few minutes to automate the resources which is very time preventing. It is a set of hardware, interfaces, software, services, networks and storages which can be shared any time according to the need. It provides on demand, self service and pay per use models which are much more convenient than the deployment.

The rise of cloud computing has undoubtedly brought many benefits, changing the way we store, access and manage it. However, underlying these benefits are security and privacy risks that must be effectively managed. These risks include things like consolidation, multitenancy and sharing which can be exploited by cybercriminals and hackers for malicious purposes. For researchers and industry professionals, ensuring the security and privacy of client data is of utmost importance. Cloud users entrust their sensitive information to service providers and often don't specify at all how that data is handled, stored, or accessed. This lack of transparency raises concerns about the integrity and confidentiality of user data, especially in terms of shared resources and the number of rented spaces User privacy and security is not only a legal and ethical requirement but a key factor in establishing and maintaining customer trust. Users must be confident that their data is handled responsibly and protected from unauthorized access or use by third parties. Achieving this balance between privacy, data access and surveillance is a complex task that requires careful consideration of various factors. Implementing robust security measures, such as encryption, access controls and monitoring mechanisms is essential to safeguarding user data while still enabling legitimate access and usage.

DOI: 10.48175/IJARSCT-17250

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

For cloud computing, the most talked about way to achieve security and privacy is cryptography. A user can protect the data by encrypting it before uploading it or storing it with an untrusted cloud service provider. The encrypted data remains unreadable even when viewed by a third party.

II. IMPORTANCE OF DATA SECURITY

One of the most important concerns in the modern communication environment is data security. Data security is becoming more important than ever due to the extensive use of information technology and the growing volume of resources that are traded online. Protecting an organization's precious assets is the main goal of security measures and there are a lot of resources on the internet that are intrinsically very valuable.

Consider the resource known as money which serves as the foundation for all economic transactions. These days, we see innumerable examples of people moving money between bank accounts. It becomes imperative to make sure that only the intended recipient has access to the funds in order to protect the secrecy of such sensitive transactions. We can ensure that the money transfer stays private and the financial resources are protected by putting strong security measures in place. Web pages, one of the essential elements of the online environment, are in a similar situation. A web page's worth is mostly determined by the time, effort and imagination that went into making it. Because it lessens the value of the labor put into its creation, any unlawful modification or change of a web page compromises its integrity and may be seen as theft. To preserve the legitimacy of online material and defend the rights of producers, web page integrity must be carefully maintained.

Cryptography shows up as a crucial and useful instrument in guaranteeing data security in each of these cases. Cryptographic methods offer a safe and dependable way to safeguard private data, stop illegal access and confirm the accuracy of data transferred over the internet. Digital signatures, encryption algorithms and other cryptographic protocols are tools that individuals and organizations may employ to protect their data and communication channels from possible dangers.

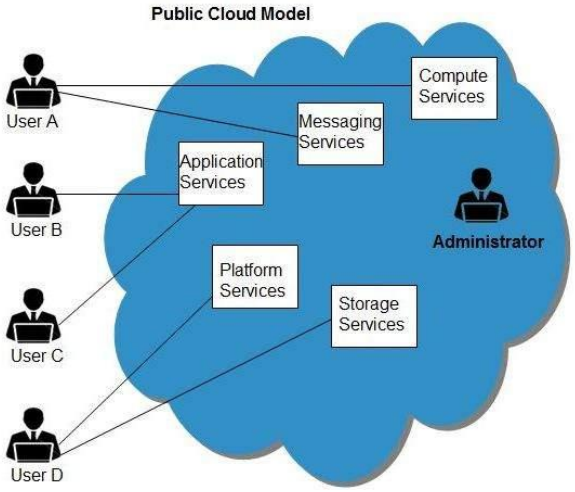
Given the present technical trend toward cloud computing it is sense to consider the advantages of outsourcing data storage and computation. This method has alluring benefits, such lowering client-side resource needs and opening up access to external data processing services. But these advantages also raise a number of data security issues. It is concerning to entrust data modification to a third party because of the possibility of tampering or illegal access. What measures are in place to stop violations? How do we guarantee data manipulation that is error-free? Furthermore, because of the greater volume of data from several customers, the third party has a greater load even when client-side resource requirements can decrease.

It makes sense that people are reluctant to employ cloud computing in applications where data integrity and security must be at an extreme degree.

III. CLOUD DEPLOYMENT MODELS

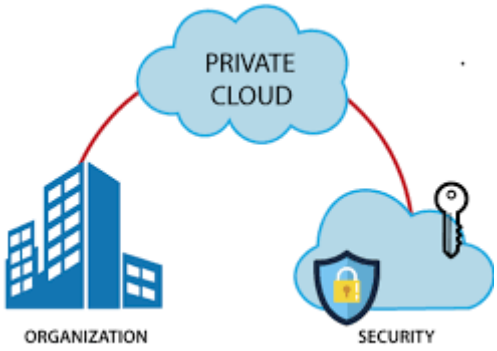
Public Cloud: Public clouds are ubiquitous in today's IT landscape, providing organizations with unparalleled power, scalability and access to computing resources and services. These clouds are owned and operated by third party cloud service providers economic scale computing resources such as servers, storage and applications to a large number of customers over the Internet. The main advantage of using a public cloud is that it is on demand, allowing organizations to deliver resources quickly and scale accordingly flexible work and business requirements are correct. Besides, public cloud provides cost efficiencies, as organizations pay only their customers for resources, without having to make up-front infrastructure investments or long-term commitments. However, public clouds also present challenges and considerations. Because resources are shared among multiple users, data privacy, security and compliance concerns arise. Organizations should carefully examine the security measures and data protection mechanisms employed by a cloud service provider to ensure the privacy, integrity and availability of their data Despite these challenges, public cloud remains the interested by organizations of all sizes, from startups to large enterprises, they are looking for scalable and flexible solutions

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024



Examples of public cloud providers include Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

Private Cloud: Private clouds offer organizations a dedicated and isolated computing environment that is exclusively owned and operated by a single organization, either on-premises or hosted by a third-party provider. Unlike public clouds, private clouds provide greater control, security and customization options as resources are not shared with other organizations. This makes private clouds ideal for organizations with specific security, compliance or performance requirements, such as government agencies, financial institutions and healthcare providers. Additionally, private clouds offer enhanced privacy and data protection, as organizations have full control over the physical and virtual infrastructure, network configuration and access controls.



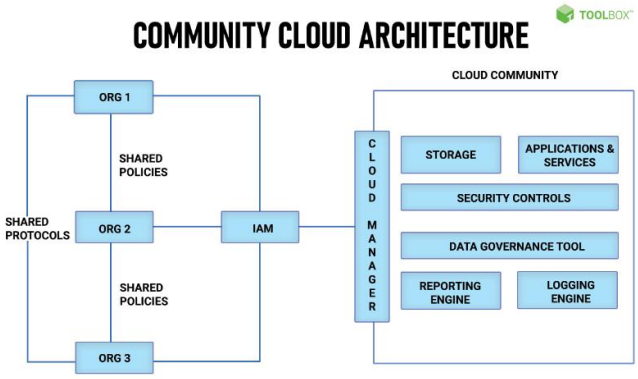
Although private clouds provide many advantages, there are potential drawbacks as well. Compared to public clouds, the deployment and management of a private cloud may entail more initial expenses and continuous upkeep. Building and running a private cloud infrastructure requires investments in people, software and hardware which can be prohibitive for smaller businesses with tighter budgets. Still, the advantages of a private cloud - better control, privacy and security - often exceed the related costs for businesses with strict security and compliance needs. Private Cloud provide robust security measures such as firewalls, detection and blocking systems, encryption and access controls to protect against unauthorized access, data breaches and cyberattacks will set up a private cloud system Comply with industry regulations, such as PCI-DSS (Payment Card Industry Data Security Standard) or SOX (Sarbanes-Oxley Act). More importantly, where private cloud environments are specifically designed to meet or exceed the stringent security and privacy requirements of this regulation.

Community Cloud: A community cloud is a shared computing environment used by multiple organizations with common interests, needs, or regulatory requirements. Unlike public clouds which serve a wide range of users, local clouds are designed for specific regions or industries, enabling collaboration, sharing of resources and cost efficiencies

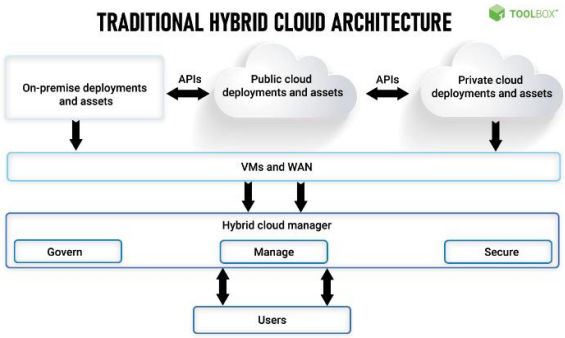
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

among member organizations. An example of a community cloud is the Health Information Exchange (HIE) platform used by hospitals, hospitals, physicians and other healthcare providers to securely share patient health records and medical information.

Community Cloud is designed to comply with stringent healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), while ensuring patient data privacy, security and integrity. They use strong encryption, access controls and audit mechanisms to protect against unauthorized access, data breaches and illegal activities.



Hybrid Cloud: The advantages of several cloud environments—public, private and on-premises data centers—are combined by hybrid cloud technology to produce a single, flexible computing platform. Through this combination, businesses may take advantage of each cloud model's advantages while minimizing its drawbacks. Fundamentally, hybrid cloud enables enterprises to attain data and application mobility by facilitating the smooth transfer of data and programs between various cloud environments. Workloads may be dynamically spread over different cloud platforms according to performance needs, cost concerns and resource availability, thanks to advanced load balancing methods.



Hybrid clouds also provide improved catastrophe recovery and resilience. Organizations may reduce the risk of data loss and guarantee business continuity in the case of infrastructure failures or natural catastrophes by duplicating data and apps across various cloud environments.

Hybrid cloud offers enterprises not just these technological advantages but also the adaptability to change as business demands and regulatory obligations do. It permits a phased adoption of cloud-based solutions, allowing enterprises to hold onto their current investments in on-premises infrastructure while easing into cloud computing.

IV. CLOUD CHARACTERSTICS

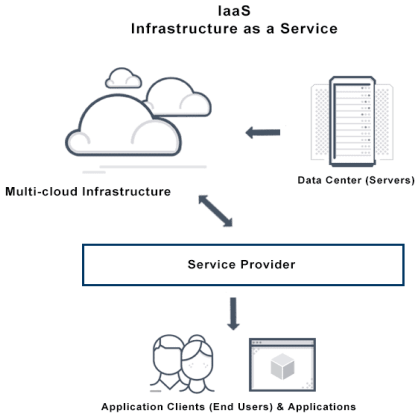
- On demand service: Every cloud is a huge pool of resources and services which you can access by paying some amount of money accordingly.
- Network Access: Cloud provides serviceeverywhere through standard devices likemobile, laptops etc. with a good internet connection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

- Easy Use: Majority of the cloud providers gives internet-based services and interface which are much simpler than the applications and softwares.
- Business Model: In the cloud computing business model, customers utilize the internet to access cloud service providers' computer resources, including storage, processing power and apps.
- Location Independent resource poling:The computing resources are pooled to serve multiple customers using multitenant modelwith different physical and virtual resources dynamically assigned and reassigned according to demand.
- On demand service: Every cloud is a huge pool of resources and services which you can access by paying some amount of money accordingly.
- Network Access: Cloud provides serviceeverywhere through standard devices likemobile, laptops etc. with a good internet connection
- Easy Use: Majority of the cloud providers gives internet-based services and interface which are much simpler than the applications and softwares.
- Business Model: Cloud is a business modelwhere the user has to pay for the services they need according to pay per use.
- Location Independent resource poling:The computing resources are pooled to serve multiple customers using multitenant modelwith different physical and virtual resources dynamically assigned and reassigned according to demand.

V. CLOUD SOLUTIONS

Infrastructure as a service (IaaS): A key element of cloud computing is Infrastructure as a Service (IaaS) which provides virtualized computer resources via the internet. Under the Infrastructure as a Service (IaaS) paradigm, customers may access and control virtualized resources, such as servers, storage, networking and other computer resources as a service in place of making investments in physical hardware, software and data center infrastructure. This enables businesses to keep control and flexibility over their computer environments while offloading the complexity of infrastructure administration and maintenance to cloud service providers.

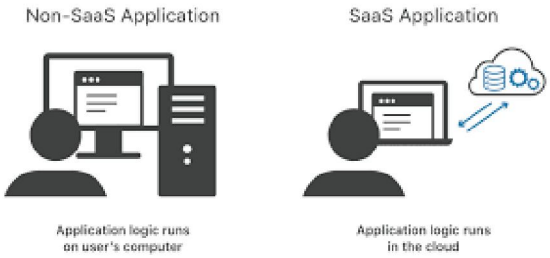


Self-service interfaces, including web-based portals or APIs, provide users the freedom to independently provision and configure computer resources. With the help of this self-service architecture, enterprises may quickly install and manage infrastructure resources without the need for IT personnel to manually intervene.

Software as a Service (SaaS): A cloud computing approach known as Software as a Service (SaaS) allows customers to access software programs via the internet, hosted by a third-party provider. SaaS offers fully working software programs that can be accessed and utilized via a web browser, usually without the requirement for installation or maintenance on the part of the user, in contrast to IaaS, where users control infrastructure resources. SaaS vendors often utilize a subscription-based pricing structure, in which customers pay a set amount each month to access the program.

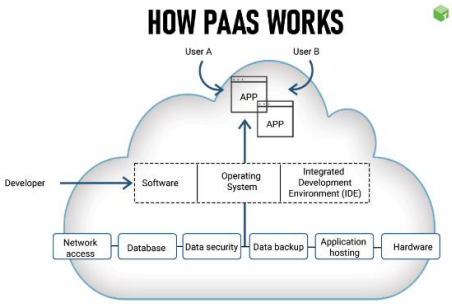
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

This pricing structure frequently covers upkeep, upgrades and support services, enabling customers to take advantage of the newest features and advancements without incurring extra expenses.



CRM software, email and communication tools, project management platforms and enterprise resource planning (ERP) systems are a few examples of Software as a Service (SaaS) applications.

Platform as a Service (PaaS): A cloud computing architecture known as Platform as a Service (PaaS) offers a full development and deployment environment as an online service. Developers may create, test, deploy and manage apps in a PaaS environment without having to worry about the intricacies of overseeing the underlying infrastructure.



Desktop as a Service (DaaS): Users may access a whole desktop environment hosted in the cloud using Desktop as a Service (DaaS). Rather of executing programs and saving information locally, users access their desktops remotely over the internet. A variety of client devices, including as desktop PCs, laptops, tablets and thin clients, can access the desktop environment.

VI. CLOUD SECURITY ISSUES

Cloud Security has always been a big challengefor the users and the cloud service providers and the organizations. Most of the industries are migrating to cloud services now, especiallypublic cloud services, where infrastructure service is provided by a cloud service provider.

To cope up these issues it is really important totake management initiatives within. The ownership and responsibility roles shouldclearly be distributed to both cloud service provider and the organization or user.

There are a lot of factors on which these management initiatives should be taken. There are security managers who determine the detective and preventive controls exist to define security posture of an organization. Asset, threat and vulnerability risk assessment matrices are the factors on which the proper security control must be implemented. The security risk assessment report is always from vendor's point of view because they are the onewho manages the cloud service.

Regulatory Compliance: Cloud Computing providers who refuse to external audits and security certifications.

Privileged user access: sensitive dataprocessed outside the organization brings with in an inherent level of risk.

Data Location: When you use cloud, you probably won't know exactly where your data hosted.

Data Segregation: Data in the cloud is shared environment alongside data from other customers.

Recovery: Even if you don't know where your data is, a cloud provider should tell you what will happen to yourdata in case of a disaster.

Investigative Support: Investigatinginappropriate or illegal activity may be impossible in cloud computing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

Long Term availability: You have to make sure your data will remain available even after such event.

VII. PROPOSED SOLUTIONS

Data storage concerns always arise in cloud computing as it requires to transfer large amount of data throughout the cloud. Users know nothing about what happens to their data after the upload it on a cloud service. Nor the exact location, neither the sources of data collectivity. To preserve the security of a cloud based virtual infrastructure it is necessary to maintain confidentiality, authenticity, integrity and availability. These steps should be taken for better security.

Encryption can be used at the host OS software through which the data transfer from virtual machine would be in encrypted form.

Physical Security is where the cloud management hosts and virtual systems are safe in the environment with carded doors.

Authentication capability of a virtual system should be same as of the physical machine authentication system. Digital signatures, biometricsand one-time passwords are some goodexamples of authentication.

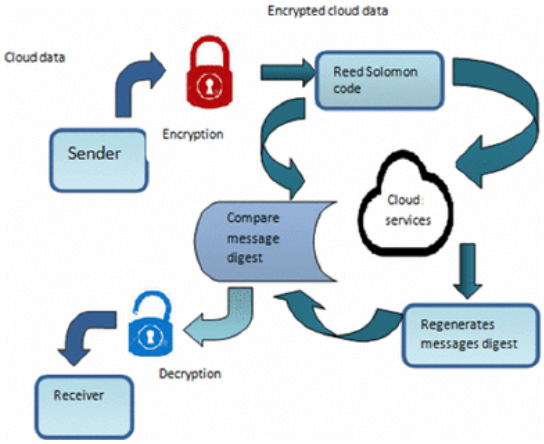
Separation of duties is important because as the system gets more complex, there is a very high chance of misconfiguration due to less experience with poor communication. Enforcing least privileges with access controls and accountability should also be done.

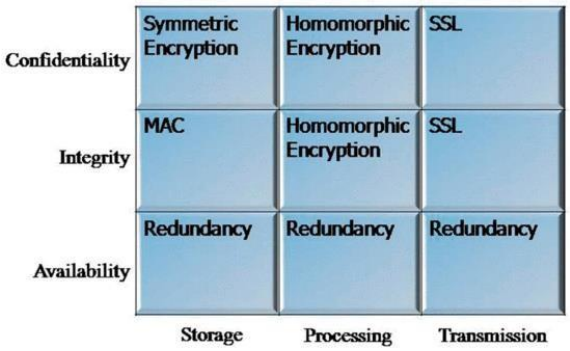
Configuration, change control and patch management are overlooked in small organizations sometimes but they are really important for data security and should be managed in virtual aswell as physical world.

Intrusion detection and prevention isused to know that what data is transferring through the network. This can keep a check on virtual network traffic with a hypervisor-based solution.

VIII. ENCRYPTION IN CLOUD

Encryption s away of scrambling data so that only authorized parties can understand the information. In technical terms it is a process of converting plaintext into cyphertext. In simple terms, encryption takes readable data and alters it so that it appears random.Encryption requires the use of encryption key which is a set of mathematical values that boththe sender and the recipient of an encrypted message know.





IX. SECURITY COMPONENTS

Confidentiality, Integrity and Availability,also known as the CIA triad, is a model designed to guide the policies for information security in some organization and are the three most important components of data security. It is also referred as AIC to avoid the clash with Central Intelligence Agency.

Confidentiality limits the access to the information, Integrity is the assurance for the information to be trustworthy and accurate andAvailability guarantees the access ofinformation to the authorized entities in thecloud network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

CONFIDENTIALITY

Confidentiality is very close to privacy. The steps are taken to stop the sensitive information from reaching in the wrong hands and making sure that the right people could access it like biometric verification, data encryption and security tokens etc. The data is categorized according to the amount it can do to a particular user or organization if it falls in the wrong hands. According to that, the measures are taken and implemented because of their priorities and severeness.

INTEGRITY

Integrity maintains the trustworthiness, accuracy and consistency of data through its life. If a data has to be transferred from one user to another or if someone wants to upload it on the cloud, data could not be changed or should maintain its consistency and accuracy throughout. The measures taken include file permissions and user access control. Checksums are often used for the verification of integrity.

AVAILABILITY

Availability keeps an eye on the resources requirement for the user such as maintaining all the hardware, performing hardware repairs when needed and maintaining a correctly functioning operating system and also all the necessary system updates which are required. These measures make the system fast and adaptive for the worst-case scenarios.

ENCRYPTION PROTOCOLS

Homomorphic Encryption: Homomorphic encryption is a method of encryption that allows any data to remain encrypted while it's being processed and manipulated. It enables you or a third party (such as a cloud provider) to apply functions on encrypted data without needing to reveal the values of the data.

In practice, most homomorphic encryption schemes work best with data represented as integers and while using addition and multiplication as the operational functions. This means that the encrypted data can be manipulated and analysed as though it's in plaintext format without actually being decrypted.

Symmetric Key Encryption: Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages. By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. Symmetric encryption is frequently used in cloud storage systems to encrypt data prior to its storage on cloud servers. This lessens the possibility of unwanted access to private data kept on cloud storage. Cloud service providers can use symmetric encryption methods to encrypt data while it is at rest in a number of ways, including disk encryption and file-level encryption. Depending on the deployment strategy, either the user or the cloud provider normally manages the encryption keys securely.

Symmetric encryption is used (together with asymmetric encryption for key exchange) in cloud computing protocols like HTTPS (Hypertext Transfer Protocol Secure) to create secure communication channels between clients and cloud services. Symmetric encryption makes sure that information sent back and forth between the client and the cloud server is private and unreadable by others.

SSL (Secure Socket Layer) Encryption: Secure Socket Layer is a standard security technology for establishing an encrypted link between a server and a client, typically a web server (website) and a browser, or a mail server and a mail client (e.g. Outlook).

More specifically, SSL is a security protocol. Protocols describe how algorithms should be used. In this case, SSL protocol determines variables of the encryption for both the link and the data being transmitted.

MAC (Message authentication Code): A message authentication code (MAC) is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.

A MAC requires two inputs: a message and a secret key known only to the originator of the message and its intended recipient(s). This allows the recipient of the message to verify the integrity of the message and authenticate that the message's sender has the shared secret key. If a sender doesn't know the secret key, the hash value would then be different which would tell the recipient that the message was not from the original sender.

In the past, the most common approach to creating a MAC was to use block ciphers like Data Encryption Standard (DES), but hash-based MACs (HMACs) which use a secret key in conjunction with a cryptographic hash

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

function to produce a hash, have become more widely used. Ensuring secure communication between clients and cloud services is crucial in cloud computing to prevent unwanted access and data manipulation. MAC is used by protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to enable message integrity verification and authentication.

X. CONCLUSION

Finally, investigating cloud cryptography protocols and data security challenges highlights how crucial strong encryption techniques are to protecting sensitive data in cloud computing systems. With more and more businesses depending on cloud services for data processing, storage and transmission it is critical to guarantee the privacy, availability and integrity of this data. Cloud data security problems are caused by a variety of dangers, including as malicious attacks, insider threats, illegal access and data breaches. Comprehensive security solutions, including as encryption, access restrictions, authentication procedures and security monitoring, are needed to address these issues.

REFERENCES

[1] J. Thomas, "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks." International Journal of Business Management, 12(3), 1-23, 2018 [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727

[2] W. Sun, N. Zhang, W. Lou, & Y. T. Hou, "When gene meets cloud: Enabling scalable and efficient range query on encrypted genomic data." In IEEE INFOCOM 2017-IEEE Conference on Computer Communications (pp. 1-9). IEEE, May, 2017 [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8056952/?casa_token= mIVlrm-3JekAAAAA:jm9RmVwuAaa74WggVF3A4BVQNWDrT4TiPpzo-86MfR7SpxAbl7PrGWoPqm024di6CsKuggE45-7oT0

[3] A. Albugmi, M. O. Alassafi, R. Walters, & G. Wills, "Data security in cloud computing." In 2016 Fifth international conference on future generation communication technologies (FGCT) (pp. 55-59). IEEE, August, 2016 [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7605062/?casa_token= gYCfDKXeuQoAAAAA:M7ZVVdmCZIDah8vHkHPf4_WJKT6_q w_A0NYJHFbg-LZt1CbmMvMOJoxEV2Sm_ZDEChddIY6yuObfr8

[4] D. Wang, Y. Jiang, H. Song, F. He, M. Gu, & J. Sun, "Verification of implementations of cryptographic hash functions." IEEE Access, 5, 7816-7825, 2017 [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7924403/

[5] P. Semwal, & M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing." In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-7). IEEE, September, 2017 [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8344738/

[6] M. Ansar, I. A. Shokat, M. Fatima, & K. Nazir, "Security of Information in Cloud Computing: A Systematic Review." American Scientific Research Journal for Engineering, Technology and Sciences (ASRJETS), 48(1), 90-103, 2018 [Online]. Available: http://www.asrjetsjournal.org/index.php/American_Scientific_Journ al/article/view/4451

[7] J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[8] D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.

[9] E. Mohamed, "Enhanced data security model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.

[10] C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[11] V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.

[12] F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

[13] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.
[14] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software platforms," Comput. Secur., vol. 31, no. 1, pp. 96–108, 2012.
[15] A. U. Khan, M. Oriol, M. Kiran, M. Jiang and K. Djemame, "Security risks and their management in cloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.
[16] T. Mather, S. Kumaraswamy and S. Latif, "Cloud Security and Privacy," p. 299, 2009.
[17] F. Yahya, V. Chang, J. Walters and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.
[18] Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM
[19] Lipinski, T. A. (2013, September). Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements. In International Symposium on Information Management in a Changing World (pp. 92-111). Springer Berlin Heidelberg.
[20] Ransome, J. F., Rittinghouse, J. W., & Books24x7, I. 2009).
[21] Catteddu, D., & Hogben, G. (2009). Cloud computing risk assessment. European Network and Information Security Agency (ENISA), 583-592.
[22] H. Qian, J. He, Y. Zhou and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," Math. Probl. Eng., vol. 2010, pp. 7– 9, 2010.
[23] P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348, 2015.