Cyber Security Model to Secure Data Transmission using Cloud Cryptography

HARSHIT DUBEY[1], SUDHAKAR KUMAR [2], ANUREET CHHABRA[3]
[1] UG Scholar, Chandigarh College of Engineering and Technology, Chandigarh
[2]Department of Computer science, Chandigarh College of Engineering and Technology, Chandigarh
[3]UG Scholar, Chandigarh College of Engineering and Technology, Chandigarh

ABSTRACT

Cloud cryptography is cryptography that is done on a cloud-based system. This enables encryption services to be provided as software, in an accessible and cost-effective manner. Cloud crypto services are commonly offered as a managed service by hosting providers but can also be offered by dedicated parties who take on all the costs and liabilities of providing such resources. It is encryption that protects data stored in the cloud. The problem of data leakage in distributed systems is widespread since data is transferred and spread across multiple systems at the same time. Aside from the security measures deployed by the cloud infrastructure, intrusion detection systems (IDS) and firewalls are also in place. By doing so, cloud computing ensures data security. Several mechanisms are being used in cloud cryptography to add a high layer of security to secure data to prevent it from being infiltrated, hacked, or impacted by malware.

KEYWORDS Cloud cryptography; Cyber Security; Security; Threats; Vulnerabilities

I. INTRODUCTION

Cloud crypto services are often compared to traditional cryptography and security options that are still used today. They differ mainly in the capability they offer in terms of decentralization and availability [1], [6], [21]. Cloud crypto services have greater access to resources, which makes them easily available to the public [3]. This enables higher levels of encryption and security over individual machines that do not have to bear all the cost and responsibility for doing so [8] [11], [22].

The cloud is more adaptable and nimbler than traditional computer systems, but it also introduces new security risks that cause users to be concerned about reliability and security. This computer paradigm's security is impacted by deployment patterns, service models, and end service characteristics. The security and privacy of the cloud platform are more important compared to conventional information security-data systems [15], [23].

Cloud computing data analytics may be pushing your company's use of cloud services such as data management systems, automatic software upgrades, instant data access to key information, and user-based growth services. Amazing benefits have been enjoyed by our clientele as a result. Just a few of the industries affected by cloud computing include e-learning, healthcare, and e-commerce. provides an economical and speedy internet connection. The next industrial and technological revolution may be this one. More and more e-commerce companies are using cloud computing to improve convenience [19], [24].

FIGURE 1: Cloud Cryptography

The growing dispersion of sensitive data over several devices and storage systems, including servers and various wearable devices such as wireless sensor networks, medical devices, gaming consoles, tablets, and smartphones, complicates data security. The security and privacy of the cloud platform are more important compared to conventional information security-data systems [20], [25].

II. HOW DOES CLOUD CRYPTOGRAPHY WORK?

Cloud cryptography is based on encryption, which uses computers and algorithms to jumble text into ciphertext [7], [26], [27]. The ciphertext can then be deciphered with a series of bits and converted to plaintext with the use of an encryption key [4], [28] [8]. By encrypting data stored in the cloud, cloud cryptography provides the same level of protection. It can secure critical cloud data without causing data transfer to be delayed [1], [29]. To strike a balance between security and efficiency, many businesses specify various cryptographic protocols for cloud computing [3], [30]. Cyber-attacks and data breaches have the same impact on cloud computing services as they do on traditional IT assets. A cloud security breach is an example of spear-phishing, in which a cybercriminal employs an email phishing scam to target a specific individual. Cloud cryptography is one method for improving the security of your cloud services. This article will teach us about Cloud Cryptography, how it works, and what advantages it offers [17], [31].

III. TYPES OF CLOUD CRYPTOGRAPHY

The two most well-known types of cloud cryptography are symmetric encryption and asymmetric encryption [5] [6], [32]. Both provide the same level of security and are used similarly for data privacy protection purposes on the cloud storage platforms. promise the operating system, or by programs that find flaws in the software code [**?**].

In addition, Cloud cryptography normally uses public key cryptography, which makes the data available to anyone who has access to the network on which it is transmitted [2], [33]. This means that any program or user with Internet access can read this data [2] [11]. Encrypted files can be stored on a central server or cloud storage and downloaded onto other computers without any protection [9], [34].

A variant of cloud cryptography is a system for communication between data centers (between server farms) where SSL or SSH is used to secure the transfer of data [8], [35]. This is particularly important in large organizations as one data center can be a single point of failure that would result in the loss of sensitive information such as intellectual property, customer database and other company assets. Cloud storage can also be used in combination with VPNs [1] [5] [7], [36].

Advantages of Cloud cryptography are as follow: -

i. The information is kept private for the users. Hackers are less likely to commit cybercrime because of this [1], [37].
ii. If an unauthorized person tries to make changes, the organization is instantly notified. And only the people with cryptographic keys are allowed to access [10].
iii. With the emergence of this new trend in IoT, there is also a growing need for security within these networks. One form of security that is becoming increasingly popular within the IoT ecosystem is Cloud cryptography [3].
iv. Data receivers can determine if the data is corrupted, allowing for an immediate response and solution to the attack [7].
v. Cloud crypto services allow devices to be easily secured while keeping costs low and allowing scalability [1] [3].

IV. CLOUD SECURITY CHALLENGES

Cloud users appear to be at conflict with the openness of the computer environment and, consequently, the distant centralization of personal multi-user resources. Even though the appliance context normally has to be steady and continuous in order to maintain the privacy and trust of user resources, sensitive data is the problem that arises the most as a result of the computing environment's openness. is vulnerable to several security problems coming from different sources [4].

Cloud Computing is widely utilized due to its numerous services such as pay on demand, minimum or no understanding of Cloud Computing services, and no need to invest money in acquisition; infrastructure upkeep; human resources; software and hardware [18].

Dynamic environment: Cloud environments are elastic, so maintaining timely visibility of virtual instances is a challenge. [16]

Protecting such settings requires continuous detection, security assessment, and proactive action.

Boundary explanation: Geographic distribution of multi - cloud environments across many environments and places makes it challenging to manage assets from a central location.

Failure in the management of physical security: If your company loses control over physical security, you oversee securing your data and workloads both in transit and at rest.

Organizations must keep up with the most recent vulnerabilities and take appropriate action as needed because the public cloud is virtualized and multi-tenant [16].

The following are the top security threats in cloud:

I. Breaches of information
II. Identities, credentials, and access are not managed effectively
III. A lack of security in APIs and interfaces
IV. Several vulnerabilities exist in the system
V. Hacking into an account
VI. Insiders with a malicious intent
VII. Threats that persist over time
VIII. Information loss

It is critical to recognise that cloud security is a joint responsibility between you and your cloud provider. According to statistics, the main dangers to data security are not cloud providers, but rather business users, hackers, and IT workers.

Implement Cryptography in Cloud Computing

Physical control of cloud data is not conceivable. Cloud encryption is a method of using codes to safeguard data and communication. Cloud data encryption is used to protect sensitive data and ensure asset transfer without slowing data transmission in order to balance efficiency and security, several digital behemoths, like Google, and Amazon, create cryptographic algorithms for cloud computing [5].

The adoption of the Cloud Computing concept may be delayed by security and privacy concerns among cloud customers. These considerations include safeguarding and limiting access to vast volumes of stored data, ensuring privacy, and managing access to the services supplied... Indeed, the service provider is ultimately responsible for the implementation and execution of security features [18].

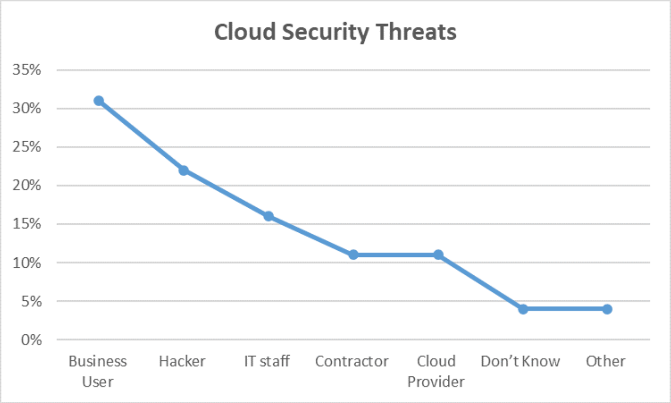

FIGURE 2: Cloud Security Threats

There are a number of different algorithms out there and the main distinction is whether the data is private or available to everyone.

Private Key - In cryptography, a private key, also known as a secret key, is a variable that is used with an algorithm to encrypt and decode data. Only the key's generator or those authorized to decode the data should have access to the secret key. Private keys are crucial in symmetric cryptography, asymmetric cryptography, and cryptocurrency [13].

Public-key in cryptography, also known as asymmetric cryptography, makes use of two keys: a public key and private key. The public key can be shared with anyone, whereas the private key should remain secret at all times, even from people who want to be encrypted. Public-key cryptography is mainly used for encryption - if someone wants to send you a message, they can encrypt it using your public key, but only you can decrypt it using your private key.ed to digital assets stored on cloud services like Dropbox or iCloud [**?**].

Public-key cryptography allows us to exchange confidential information in a secure way, it is applied when encrypting data, and the process is quite simple.

The encryption process involves [**?**] :-

1) Find a key that can encrypt the data we want to protect;
2) Encrypt the message with the key; and
3) Decrypt the message using a different key that only we have access to. This usually involves using two keys - one private and one public (also known as asymmetric cryptography).

The methods involved in security architecture can be class

It can be majorly categorized into two types which are: -

I. Symmetric Algorithm
II. Asymmetric Algorithm

Key difference between Symmetric & Asymmetric is as follows:-

The main disadvantage of symmetric cryptography is that two different keys are required for encryption and decryption. That means that the sender and receiver have to exchange their keys in advance [7]. The process is repeated every time we want to encrypt or decrypt data. Due to the complexity of the implementation, symmetric cryptography is slow and not generally used for on-the-fly encryption [2].

	Symmetric Algorithm	**Asymmetric Algorithm**
Technique	Old Technique	Modern Technique
Key Length	128- or 256-bit key size	RSA 2048 bit or high key size
Data Size	Used to transmit big data	Used to transmit small data
No. of keys	Single	Two
Security	Less Secure	More Secure

Quantum cryptography is another type of asymmetric cryptography, which uses entangled quantum states between a sender and receiver to transfer a message - this makes classical wiretapping impossible, as it would destroy the quantum state. Quantum cryptography uses photons (light particles) as its medium so it's sometimes known as photon-based cryptography [9].

V. ARCHITECTURE SOLUTIONS ON CLOUD SECURITY

Cloud Security Center is built on a platform for cloud computing that is compliant with the security architecture for cloud computing. The web servers, front-end servers, and back-end servers in the cloud data center were then linked to the cloud security center. File encryption of the later plaintext files, as well as data integrity checks on front-end and back-end ciphertext files and digital signatures [9]

There are two components to the cloud computing platform. The cloud data center's front end is the first. The stern is the opposite. The front end of cloud computing is linked to a web server. The front-end and back-end are connected by a solitary gatekeeper device. The ciphertext file is transferred to the data center's back end by the gatekeeper's data ferry function, where it is processed to create the data encrypted file [7].

Cryptographic card chips include digital signature protocols, authentication protocols, cloud computing end data encryption / decryption protocols, signature verification protocols, as well as symmetric encryption algorithms, symmetric key generation algorithms, and a set of fixed symmetric keys [1].

VI. CONCLUSION

One such disadvantage of Cloud cryptography is that it is a relatively new field and research in this area is still ongoing. The technical feasibility for cloud cryptography has been demonstrated, but there are still considerations about the possible legal implications that may arise from using such services. Cryptography is the mathematical process of transforming information into a code, also known as encryption. The result is a function that scrambles data so it can only be unscrambled using special software. Encryption makes sure that data remains secure and invulnerable - it's one of the fundamental ways we try to protect our privacy in this day and age. One example of potential legal concerns arising from the use of cloud crypto services is the transfer of information beyond national jurisdiction. This can be seen as a potential breach to laws that protect certain data, for example information about transactions between businesses or personal information about individuals. Another concern may be in relation to the physical location and regulation of data storage that occurs within a cloud computing environment.

REFERENCES

[1] Jaber, Aws & Zolkipli, Mohamad. (2013). Use of cryptography in cloud computing. 179-184. 10.1109/ICCSCE.2013.6719955

[2] Kumar, S., Singh, S. K., Aggarwal, N., & Aggarwal, K. (2021). Evaluation of automatic parallelization algorithms to minimize speculative parallelism overheads: An experiment. Journal of Discrete Mathematical Sciences and Cryptography, 24(5), 1517–1528. https://doi.org/10.1080/09720529.2021.1951435

[3] Mishra, A., et. al. (2021). Defence mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommunication systems, 77(1), 47-62. https://www.ijert.org/cloud-cryptography-a-security-aspect

[4] Singla, D., Singh, S. K., Dubey, H., & Kumar, T. (2021, December). Evolving requirements of Smart healthcare in Cloud Computing and MIoT. In the International Conference on Smart Systems and Advanced Computing (Syscom-2021).

[5] Sudhakar Kumar, Sunil K. Singh (2021), Brain Computer Interaction (BCI): A Way to Interact with Brain Waves. Insights2Techinfo, pp. 1

[6] Kumar, S., et. al. (2022). An efficient hardware supported and parallelization architecture for intelligent systems to overcome speculative overheads. International Journal of Intelligent Systems.

[7] I. Singh, S. K. Singh, R. Singh and S. Kumar, "Efficient Loop Unrolling Factor Prediction Algorithm using Machine Learning Models," 2022 3rd International Conference for Emerging Technology (INCET), 2022, pp. 1-8, doi: 10.1109/INCET54531.2022.9825092.

[8] Peñalvo, F. J., Sharma, A., Chhabra, A., Singh, S. K., Kumar, S., Arya, V., & Gaurav, A. (2022). Mobile Cloud Computing and Sustainable Development: Opportunities, Challenges, and Future Directions. International Journal of Cloud Applications and Computing (IJCAC), 12(1), 1-20. http://doi.org/10.4018/IJCAC.312583

[9] Singh, Sunil & Kaur, Kavneet & Aggarwal, Anuj & Verma, Dharvi. (2015). Achieving High Performance Distributed System: Using Grid, Cluster and Cloud Computing. Int. Journal of Engineering Research and Application ,ISSN : 2248-9622. 5. 59-67.

[10] Gupta S. et. al.(2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: Present and future challenges. International Journal of Cloud Applications and Computing, 7(3), 1–43.

[11] Al-Qerem, A., et. al. (2020). IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. Soft Computing, 24(8), 5695-5711.

[12] Singh, K., Setia, H., & Kumar, S. (2021, December). Wi-Vi and Li-Fi based framework for Human Identification and Vital Signs Detection through Walls. In the International Conference on Smart Systems and Advanced Computing (Syscom-2021).

[13] Peñalvo, F. J. G., Maan, T., Singh, S. K., Kumar, S., Arya, V., Chui, K. T., & Singh, G. P. (2022). Sustainable Stock Market Prediction Framework Using Machine Learning Models. International Journal of Software Science and Computational Intelligence (IJSSCI), 14(1), 1-15.

[14] Sunil Kr Singh, R. K. Singh and M. Bhatia, "Design flow of reconfigurable embedded system architecture using LUTs/PLAs," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, pp. 385-390, DOI: https://doi.org/10.1109/PDGC.2012.644985.

[15] Okuhara, Masayuki & Shiozaki, Tetsuo & Suzuki, Takuya. (2010). Security Architectures for Cloud Computing. Fujitsu Scientific and Technical Journal. 46. 397-402.

[16] D. R. Bharadwaj, A. Bhattacharya and M. Chakkaravarthy, "Cloud Threat Defense – A Threat Protection and Security Compliance Solution," 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2018, pp. 95-99, doi: 10.1109/CCEM.2018.00024.

[17] Latifa Ben Arfa Rabai, Mouna Jouini, Anis Ben Aissa, Ali Mili,A cybersecurity model in cloud computing environments,Journal of King Saud University - Computer and Information Sciences, Volume 25, Issue 1, 2013,Pages 63-75,ISSN 1319-1578,https://doi.org/10.1016/j.jksuci.2012.06.002

[18] Tissir, N., El Kafhali, S. & Aboutabit, N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J Reliable Intell Environ 7, 69–84 (2021). https://doi.org/10.1007/s40860-020-00115-0

[19] A. Khaldi, K. Karoui, N. Tanabène and H. B. Ghzala, "A Secure Cloud Computing Architecture Design," 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2014, pp. 289-294, doi: 10.1109/MobileCloud.2014.44.

[20] Okuhara, Masayuki & Shiozaki, Tetsuo & Suzuki, Takuya. (2010). Security Architectures for Cloud Computing. Fujitsu Scientific and Technical Journal. 46. 397-402.

[21] Chui, K. T., et al. (2022). An MRI scans-based Alzheimer's disease detection via convolutional neural network and transfer learning. Diagnostics, 12(7), 1531.

[22] Mishra, A., et al. (2021, January). Classification based machine learning for detection of ddos attack in cloud computing. In 2021 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-4). IEEE.

[23] Tewari, A., et al. (2018, January). A mutual authentication protocol for IoT devices using elliptic curve cryptography. In 2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence) (pp. 716-720). IEEE.

[24] Gupta, B. B., et al. (2018). Assessment of honeypots: Issues, challenges and future directions. International Journal of Cloud Applications and Computing (IJCAC), 8(1), 21-54.

[25] Tewari, A., et al. (2020). An analysis of provable security frameworks for RFID security. In Handbook of computer networks and cyber security (pp. 635-651). Springer, Cham.

[26] Dahiya, A., et al. (2021). How IoT is Making DDoS Attacks More Dangerous.

[27] Chui, K. T., et al. (2021). Extended-range prediction model using NSGA-III optimized RNN-GRU-LSTM for driver stress and drowsiness. Sensors, 21(19), 6412.

[28] Agrawal, D. P., et al. (2018). Recent advances in mobile cloud computing. Wireless Communications and Mobile Computing, 2018.

[29] Gupta, B. B., et al. (2022). Novel Graph-Based Machine Learning Technique to Secure Smart Vehicles in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems.

[30] Gupta, S., et al. (2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. International Journal of Cloud Applications and Computing (IJCAC), 7(3), 1-43.

[31] Alsmirat, M. A., et al. (2017). Accelerating compute intensive medical imaging segmentation algorithms using hybrid CPU-GPU implementations. Multimedia Tools and Applications, 76(3), 3537-3555.

[32] Gupta, B. B., et al. (2015). Cross-site scripting (XSS) abuse and defense: exploitation on several testing bed environments and its defense. Journal of Information Privacy and Security, 11(2), 118-136.

[33] Gupta, S., et al. (2015, May). PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications. In Proceedings of the 12th ACM international conference on computing frontiers (pp. 1-8).

[34] Mishra, A., et al. (2011, September). A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques. In 2011 European Intelligence and Security Informatics Conference (pp. 286-289). IEEE.

[35] Jain, A. K., et al. (2018). PHISH-SAFE: URL features-based phishing detection system using machine learning. In Cyber Security (pp. 467-474). Springer, Singapore.

[36] Tewari, A., et al.. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. International Journal of Advanced Intelligence Paradigms, 9(2-3), 111-121.

[37] Kaur, M., et al. (2021). Secure and energy efficient-based E-health care framework for green internet of things. IEEE Transactions on Green Communications and Networking, 5(3), 1223-1231.