Cloud Cryptography and Data Security

Gourav Bansal
Kurukshetra University

***Abstract*-Cloud computing is indeed an instrumental technology in our daily lives; it uses the Internet to provide applications and transfer and maintain data. It is critical to provide an eco-system that aims to protect data and applications within the cloud; networks must be protocols that use robust algorithms to protect applications and data. Data security and encryption are regarded as the most important discoveries, although their growth in the past entirely independently now that reality has shown a direct link between them. This article analyzes some of them and compares them to others. Cloud cryptography encrypts data in the cloud to keep it safe. To avoid privacy violations, hacking, or malware infection, cloud cryptography employs a variety of precautions such as hashing and symmetric and asymmetric key-based algorithms. Further, data-in-transit and data-at-rest are the two types of cloud cryptography that any organization's cyber security plan should contain.**

Keywords- Encryption, data, network, security, protocols, symmetric cryptographic algorithms, asymmetric cryptographic algorithms, hashing functions.

1. INTRODUCTION

Cloud technology services, like other IT resources, are vulnerable to data breaches and cyber-attacks. Spear-phishing is a type of cloud cyber-attack in which a malicious user uses an email phishing hoax to target a particular user [1]. When the targeted individual clicks the link in a phishing attack, they subject themselves and their employer to a hacking incident, affecting millions of people. This is where cloud cryptography comes into play here. Cloud cryptography protects data stored in the cloud by encrypting it. Numerous safeguards are being included in cloud cryptography to prevent data breaches, hacking, or malware infection. Clients may use pooled cloud services safely and efficiently since all data held by cloud vendors is encrypted. Cloud cryptography protects sensitive data while allowing information to be sent quickly. It is entirely predicated on encryption, in which data is jumbled into ciphertext with the help of computers and protocols [2]. This encrypted data may subsequently be deciphered using a series of bits and converted to plain text using an encryption key. Cloud encryption is innovative since it protects your data once it leaves your company's IT system. This ensures that your data is safe no matter where it travels through your cloud computing services. Cryptography safeguards data instead of the locations where it is held, resulting in a higher degree of cyber security for your company.

2. TYPES OF CLOUD CRYPTOGRAPHY

Data-in-transit and data-at-rest are the two forms of cloud cryptography that should be included in every organization's cyber security strategy. The term "data-in-transit" refers to data that is in the process of being transferred between two or more endpoints. The HTTP and HTTPS protocols that safeguard the data channel a user uses when accessing multiple websites online are a typical kind of data-in-transit cloud encryption that you can observe while using a web browser [3]. They achieve this by enclosing the secure channel with an SSL (secure socket layer), a tier of cryptography. When data is transmitted between a user's endpoint and the terminal for the website being viewed by the user, the SSL inside the HTTPS or HTTP encrypts the user's data as well as the website's data so that if the user's channel is compromised, the malicious user will only see encrypted information. Confidential data stored in company IT infrastructure like cloud storage devices, servers or disks are referred to as data-at-rest [3]. You may impose access control by encrypting data while it is being kept by only providing decryption keys to authorized personnel. Anyone seeking to retrieve your data-at-rest will be presented with encrypted files instead of unencrypted.

3. CRYPTOGRAPHIC TECHNIQUES

There are three principal techniques employed in cloud cryptography: hashing, symmetric and asymmetric key-based algorithms. Contemporary cryptography is predicated based on hash functions. This refers to cryptographic machinery for transforming extensive unsystematic data into condensed fixed-size data. The hash value is the data outcome of the hash algorithm. Hash functions work in a one-way manner and do not require any keys to operate. The one-way technique ensures that computing the input from a particular outcome is difficult [4]. Seeding sub-keys in critical establishment rules plus algorithms, message/checksum veracity checks, production of pseudorandom numbers, source integrity services through MAC, and generation and verification of digital signatures are some of the most common uses of hash functions. Compared to any other data structure, hashing offers a safer and more customizable method of finding data. It is more proficient than arrays plus lists. This method can retrieve data in 1.5 probes in the extreme range, including everything saved in a tree [4]. Unlike other data structures, hashing does not specify the performance.

The symmetric cryptographic algorithm is an encryption technique that allows authorized users to access both data-in-transit and data-at-rest without manual encrypting and decrypting. Once login credentials are supplied, the method automatically decrypts and encrypts crucial data. Even though symmetric cryptographic techniques are frequently computerized, key management is still required. Based on the cloud service provider a user selects, the company may use several encryption key variants or various encryption keys [5]. If you work with numerous cloud vendors or in diverse cloud environments, your key management system should help you keep track of all of your encryption keys. The term "public-key algorithms" refers to asymmetric-key algorithms. They employ private along with the public, which is mathematically linked. One key is for encrypting data, while the other is used to decode it. A key pair is the coupling of public plus private keys. The possessor retains the private key hidden at all times. The general populace key is made available to the whole community, and anybody can use it. The public key cannot be used to determine the private key. An authenticator binds the public key to identification in most cases. Most asymmetric-key techniques are founded on mathematical problems such as discrete logarithm problems plus the integer factorization problem [5]. The primary benefit of the symmetric algorithm over asymmetric algorithm is that it is more proficient and faster for massive quantities of data; the drawback is that the keys need to be clandestine, which could be problematic in circumstances where decryption and encryption happen in distinct areas and the key ought to be securely relocated between them. On the other hand, asymmetric encryption is the safest encryption method since clients are never obliged to expose or disclose their secret keys, lowering the risk of a hacktivist uncovering a user's secret key during communication.

4. PROS AND CONS OF CLOUD CRYPTOGRAPHY

Some advantages of cloud cryptography include that customers' data stays private, decreasing crimes from cybercriminals, and corporations receiving fast warnings if unauthorized individual attempts to make changes. Access is allowed to people who have cryptographic keys. When data is transferred from one computer to another, it is encrypted to be susceptible. Furthermore, in today's data-driven society, cloud encryption allows enterprises to be aggressive in their security against privacy violations and intrusions. Recipients of data can detect whether the data is compromised, allowing for rapid action and remedy to the assault. Cryptography is also one of the most acceptable storing and sending data since it conforms to industry standards like HIPAA, FIPS, PCI/DSS, and FISMA [6].

On the other hand, some disadvantages of this subject include the fact that cloud cryptography only provides limited protection to data already in transit. To keep encrypted data safe, sophisticated methods are required. Furthermore, the systems must be extensible enough to update, which contributes to the associated costs, and overly protective safeguards can make data recovery challenging for enterprises. Nonetheless, these challenges can be easily overcome by carefully following the laid down guidelines in encryption.

To safeguard against sophisticated attacks in the multifaceted and dynamic settings of virtualization, cloud amenities, and flexibility, businesses and establishments must take a data-centric strategy to secure confidential data. Enterprises ought to deploy data safety resolutions that support dependable fortification of sensitive data, such as cryptographic and encryption key administration for cloud records. A complete platform for cloud security and encryption should also include robust access controls and key management features that enable enterprises to use encryption to meet security goals in a realistic, affordable, in addition to comprehensive manner.

5. CONCLUSION

It is evident that today's world is driven by data, and as a result, cyber security is a significant issue. The success of cloud computing technology is heavily reliant on the safety of users and their data at all times. To achieve this, cloud cryptography techniques such as hashing, symmetric and asymmetric encryption algorithms are employed to provide security. Cloud cryptography, in general, safeguards sensitive data while permitting data to be transmitted fast. It is based solely on encryption, in which data is scrambled into ciphertext using computers and algorithms. There are two significant forms of cloud encryption, namely, data-in-transit as well as data-at-rest. If done well, cloud cryptography has numerous benefits to an organization of any calibre, and the opposite is true. Therefore, cloud cryptography must be properly understood to avoid attacks.

6. 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:jm9RmVwuAaa74WggVF3A4BVQNWD-rT4TiPpzo-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_qw_A0NYJHFbg-LZt1CbmMvMOJox-EV2Sm_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_Journal/article/view/4451