JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Special Issue No.-11, May (2024) pp 219-229 ISSN (Print) 0973-8975

MATHEMATICAL FOUNDATIONS OF DATA SECURITY IN CLOUD ENVIRONMENT

Nidhi Arora[1], K. D. Sharma[2], Ashok Sharma[3], Tania Bose[4], Renu Bala[5] Madhu Aneja[6]

[1] School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.

[2, 4] Department of Applied Sciences, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.

[3] Department of Computer Science & IT, University of Jammu, Jammu India.

[5,6] Department of Applied Sciences, Institute of Engineering and Technology, Chitkara University, Punjab, India.

Email: [1]er.nidhi152@gmail.com, [2]krishandutt.sharma@chitkara.edu.in, [3]drashoksharma@hotmail.co.in, [4]tania.bose@chitkara.edu.in, [5]renu.bala@chitkara.edu.in, [6]madhu.aneja@chitkara.edu.in

Corresponding Author: **K D Sharma**

https://doi.org/10.26782/jmcms.spl.11/2024.05.00015

(Received: March 22, 2024; Revised: May 3, 2024; Accepted: May 19, 2024)

Abstract:

Cloud computing is a prominent technology that allows clients to access the required data to accomplish their tasks on any machine with an internet connection. Although it is an emerging technique in the information technology world, it is facing some challenges also. Data security has become a big hindrance in the growth and promotion of cloud services. As data resides in different places all over the world, data security and privacy have become major areas of concern about cloud technology. Mathematical modelling acts as an important aid to examine and alleviate possible attacks or hazards on cloud models. The paper reviews several security areas and issues related to the cloud computing environment. It also aims to focus mathematical models on security issues that arise from the use of cloud services. Various threats to the data security for a faithful cloud environment are also discussed. Various methods that ensure cloud privacy and security of the data are also reviewed.

Keywords: Cloud Computing, Cloud environment, data security, Confidentiality, and integrity, Mathematical modelling, Threats in a cloud environment

I. Introduction

Cloud computing is based upon an urge for network access to shareable computing resources named as software services, network services, various servers, and applications. There is an intermediate service provider through which users can directly access the service without any further need to contact the server. Therefore, Cloud computing is the technique to provide on-request services that too with minimal cost.

There are three widely used service models in the cloud environment. These models can be adapted as and when required.

Software as a service (SaaS): Different service providers avail various software services to the client that enable access to various applications running on the cloud. For example, Ajax, NetSuite, etc.

Platform as a service (PaaS): In this kind of service, resources are provided to the client to perform the different tasks. For example, Google Apps and Heroku.

Infrastructure as a service (IaaS): To avoid the cost and complexity of buying and managing physical servers, the complete infrastructure is provided to the client by the service providers.

Cloud computing is similar to grid computing. Diverse resources are coordinated and controlled together with the linked OS with the aim to produce pumped-up computing facilities when cloud computing merges the storage and the computing devices supervised by unique OS to supply facilities such as huge levelled storage of data and speedy computing services to users.

Cloud Systems provide various features such as low cost and high storage. These are the most flexible systems with high mobility. Both the academic and industrial world are widely benefited through this approach. Cloud computing technology has created a separate picture to run businesses all over the world. Besides being a very promising approach, there are still many problems with clients and organizations storing and accessing the data in the cloud. The most common obstacle is data security, along with other problems such as trust, privacy, and other legal matters.

On the top, it is the cause of worry to the users who are most dependent on the data which is distributed on different machines, servers, and other storage devices. As, Cloud computing offers on-request services through cloud service providers via the internet, which facilitates the end users to fulfill their business needs.

It reduces the cost for them. Many data security techniques are applied to secure the data which is further needed to be revised. It is based on two factors such as storage and computing. Many reputed companies such as Amazon, Google, and Microsoft

are implementing this technology. Cloud is of different kinds such as private, public, and hybrid cloud.

1. **Public cloud** belongs to the service provider in which different users can access its services.
2. **Private cloud** belongs to a company in which only authorized users can access the service
3. **Hybrid cloud** is derived after the merging of both the above private and public clouds.
4. **Community Cloud** This infrastructure has been shared by various organizations which is managed by a third party and may be deployed within the organization.

The main problems in cloud computing comprise management, tracking, and security of the resources. Different techniques have been introduced by various researchers for the security and privacy of the data.

II. Threats in Cloud Computing

Cloud computing offers numerous benefits, but like any technology, it also comes with its own set of security threats. Some common threats in cloud computing include data loss, data breaches, insufficient identity credentials and access management, DOS attacks, etc.

Security of the data: There are many risks in cloud computing: confidentiality, privacy, and trustworthiness. Security is achieved by merging various key factors such as a) confidentiality - prevention of the uncertified exposure of information, b) morality, the prevention of the uncertified amendment of information, and c) availability, the prevention of uncertified retaining of data and useful information.

Data security is a very crucial component in the present era of extended and protracted vision of cloud computing. It is further categorized into different parts: safe methods, tracking of the server, confidentiality of data, and ignoring malicious actors. There are various security techniques applied yet they are not enough to overcome the malicious activities of unauthorized users.

Integrity of the data: Integrity of the data means safeguarding the data from malicious acts such as deletion or amendment of data. To achieve data integrity, ACID properties (atomicity, consistency, isolation, and durability) must be followed by the transactions. Encryption techniques like Data Encryption Standards, Advanced Encryption Standards, etc. are meant for such kinds of concerns. PKI infrastructure is needed to manage these concerns. Repositories are encrypted by using the public key and embedded by labels linked with each client. The client or user keeps the private code segment of the key and is authorized to decode the labels encoded with the public segment. This kind of technique is costly to process but good for storage or archival.

Another type of technique for encryption, referred to as Homomorphic Encryption makes the cipher text able to be processed in a public environment without decoding it. Cloud utility providers are required to ensure integrity for the storage of data. Erasure Coding, a kind of distributed data and network coding has been used for fault tolerance and data availability. For transferring the data securely over networks, Transport level security (TLS) is measured. System Authorization is the next step in data control which determines the level and state up to which data can be controlled by the system. Unauthorized users should not harm the data and therefore, it must be stored securely to maintain data integrity and accuracy. The next technique to protect the data is digital signatures and strategies like RAID. There should be a third-party supervision mechanism among users and service providers that may keep a check on both.

Confidentiality of the data: Confidentiality is important for the clients for storage of their privileged data in the cloud. So, the data should be encoded before outsourcing so as to protect it from illegal access or attacks. Various approaches such as access control and authentication are applied to ensure confidentiality of the data. The most popular method for hiding data while maintaining customer information is data anonymization.

Availability of the data: Data availability refers to how much time the service provider guarantees that the data and services are available. The cloud service provider should make the data available in case of failures such as system failure, natural calamities, etc. The cloud utility resources provided by third-party vendors may also store and manage the data.

III. Security concerns

There are various security issues in the cloud environment that include risks such as loss of data, interference in services, malicious attacks from outsiders, etc. The following points discuss these security issues:

Trust by the clients: Client data must be protected from malicious users either by applying security algorithms or authentication practices. This will keep the customers' trust and reassure them that their data is secure.

Authentication of User: There must be provision for authenticated users so that only they can have access to powerful computing systems in a cloud environment. In this way, authentication rights are to be provided to legitimate users.

Loss of Data: Sometimes data can be modified or deleted by unauthorized users. And if there is no backup of the related data, it might cause big problems for the cloud users.

Session hijacking: In these types of attacks, generally attacker hijacks the session of legitimate users in bad intention of gaining their credentials.

Misuse of Cloud Services: Service providers offer a trial period of access to their

services free of cost. Some malicious actors misuse these services and resources during this time.

IV. Methods to ensure data security in cloud computing

Encryption: In this case, data is encoded and information can be accessed by the authorized user. Various algorithms like "hashing Algorithm" are applied in this case. Message digest and digital signatures are also implemented to achieve the methods.

Holomorphic Token: It refers to the secure editing of outsourced data in the cloud. Organizations can make use of the coherence services offered by the cloud provider and save and store data in an encrypted format in a public cloud through holomorphic encryption.

Striping Algorithm: This technique load balances the data across several disks to expedite data processing. Various segments of disks are maintained on which data is stored sequentially in different segments containing files.

Data Concealment: Data of legitimate users can be concealed to protect it against potential attacks. Data concealment also maintains the confidentiality of the data. The overall volume of real data is being increased besides providing enhanced security for private data. It aims at saving the original data from non-legitimate uses. Watermarking is another method for ensuring data authenticity.

V. Mathematical models and the cloud security

One way to describe security risk is the sum of the likelihood or frequency of security employing their product, the danger incident, and the extent of its aftermath (Saripalli et al., 2003). It is difficult to assess the likelihood of attacks on the existing cloud security because of the inadequately updated data. For instance, in the event of spoofing attacks, it is essential to know how frequently these assaults occur across all corporate systems. These kinds of data aren't easily accessible, though. Attacks against web applications account for more than 60% of all online attack efforts, according to SANS. These flaws are frequently used to turn trustworthy websites into malevolent ones that distribute content that includes client-side exploits. Of the Verizon Business data breach cases that were looked into in 2015, 29% involved the use of default or easily guessed passwords (RSA: Five Top Internet Security Threats, 2012). Backdoor malware, which accounted for 26% of exploits, was followed by SQL injection assaults (13%), key loggers and spyware (18%), exploiting backdoors or command and control channels (23%), and using stolen log-in credentials (24%). If we assume that a given server system is accessed t times for SQL queries in a day, and that x of those events were injection attacks, we can compute the probability P of a security hazard.

The mean of risk or the expected value of the threat λ, is given as:

$$\lambda = \sum_{i=1}^{n} x_i p_i$$

The probability of the occurrence of the next k threat on security can be calculated by using the Poisson approximation,

$$P(k) = e^{-\lambda t} \frac{(\lambda t)^k}{k!} \text{ where } k = 1, 2, \ldots n$$

Once the probability of threat on cloud security is calculated, it would be useful to identify high-risk threats on cloud security.
Suppose, there is a Virtual Machine through which viruses may enter into the system and attacks may occur. As the resources are being shared, it may also affect any virtual machine on the cloud which can also be any physical machine. Once it is affected, then it may damage other virtual machines which ultimately disturbs the entire cloud. In certain situations, the Las Vegas Randomised Algorithm (LVRA), which guarantees that "you will always get a solution if there is a solution at all," is employed.

The main task is to imitate the first attack in successful manner. Stochastic modelling is sometimes applied to judge the expected outcomes within a forecast to anticipate what conditions may be there in different situations. There may be a case when each virtual machine is allocated to one physical machine whereas a physical machine can be assigned to multiple virtual machines. It is presumed that when users submit requests for cloud resources, they do so simultaneously and without knowledge of one another's bids. Later on, the resources are allocated to them that depend on the proportion of the bid.

Block Cipher: A symmetric encryption algorithm known as a block cipher is used to encrypt data in fixed-size blocks, usually 64 or 128 bits at a time. It is commonly used in cloud security to protect sensitive data stored in the cloud. The data is encrypted before it is transmitted to the cloud and decrypted when it is retrieved by the authorized user. Blowfish and AES (Advanced Encryption Standard) are two well-known block ciphers. There are several ways to use block ciphers, including CBC, ECB, CTR, OFB, and CFB modes of operation. Block ciphers can be used in various modes of operation such as ECB, CBC, CFB, OFB, and CTR. The choice of mode of operation along with key size and block size determines the strength of encryption.

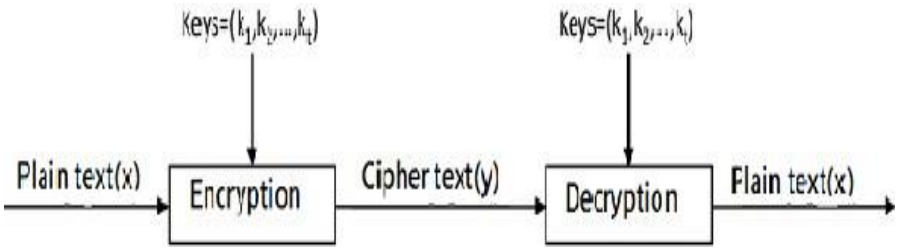

Fig 1: A mathematical model for block cipher

Stream Cipher: In terms of cloud security, a stream cipher is a kind of encryption technique that, encrypts data bit by bit or byte by byte. The plaintext data is encrypted using a keystream—a stream of pseudo-random numbers produced by this kind of cipher. A secret key is used to create the keystream, which the cipher then utilizes to encrypt data in real time as it is being transferred or stored in the cloud.

One example of a popular stream cipher in cloud security is the Advanced Encryption Standard (AES) in counter mode (AES-CTR). This mode uses a block cipher, such as AES, in combination with a counter to generate the keystream. Every plaintext block causes the counter to increase, and the resulting keystream is used to encrypt the plaintext.

Because of their high efficiency, stream ciphers are a good fit for real-time applications like voice and video over IP. They can also be used to encrypt data sent across erratic networks, such as wireless networks, because of their ability to adjust quickly to changing network conditions.

However, they are not as secure as block ciphers when it comes to protecting large amounts of data, as they rely on a small secret key to encrypt large amounts of data.

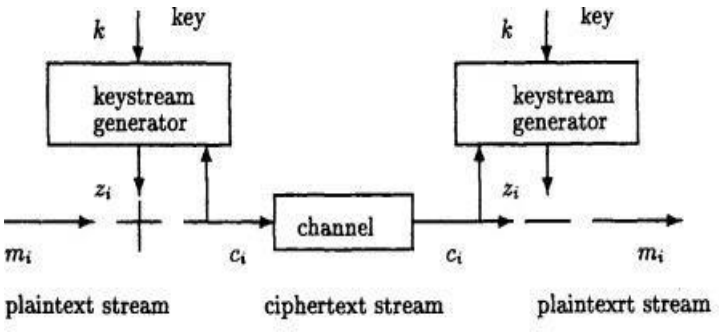

Fig 2: A mathematical model for stream cipher

Hash Functions: Hash functions are a fundamental building block in many cryptographic algorithms used for cloud security. They accept an input (or "message") and output a fixed-size value (also known as a "digest" or "hash value"). Usually consisting of a sequence of bytes, the output is intended to be distinct from the input, meaning that even little modifications to the input will yield drastically different results.

Hash functions provide an important security feature in that it is computationally impossible to identify two separate inputs that result in the same output—a phenomenon known as a "collision." Because of this, hash functions can be used to create digital signatures, where the output is a signature and the input is a message for integrity checks. Hash functions are one-way functions, meaning that it is challenging to determine the original input from the output. This is another significant characteristic of hash functions.

This makes hash functions useful for hiding sensitive data, such as passwords, by storing only the hashed version.

Security threat model

It is not easy to calculate the probability of threats in the security model because of data deficiency. For example, in spoofing attacks, there is a lack of required data. Mathematical modelling has become an emerging technique that provides a better understanding of issues related to security. A sensitivity analysis is performed before choosing any mathematical model which is better suited for the desired problem. There are various parametric values on which behavior and structure of the model rely. The cloud model behavior may also be determined by changing parameters and failure data.

Threats related to security in cloud computing: There are some threats that may attack and damage the individual systems but others may affect the whole system adversely such as unknown risk profiles, Shared technology issues, insecure interfaces & APIs, malicious insiders, data leakage, and account hijacking.

Risk Mitigation: Every kind of threat that is phrased in STRIDE has a corresponding set of expedient techniques used to lower the risk of attacks. STRIDE is an acronym which includes six risk categories such as “Spoofing user identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege”. STRIDE threat modelling provides the mechanism to organize the many possible threats in enterprises. Risk mitigation is the method of planning for disasters and finding a way to minimize negative impacts.

Viral attack in Virtual Machine (VMs): The cloud providers make efforts to segregate virtual machines from the physical machines to preserve the security of data that may be occurred due to viral attack and damage the whole system. But still

there are many barriers in the way of achieving a secure virtual machine. As the resources are shared dynamically among physical systems and virtual systems, they are the major cause of the spread of viruses among the systems.
Revenue maximization models such as stochastic and its distributions for revenue maximization are applied in financial modelling in which random variables are considered.

VI. Algorithms in data protection in the cloud

To safeguard data while it's in transit and at rest, cloud environments employ several mathematical techniques for data security. For data at rest, encryption algorithms like Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) are commonly used. These methods transform plaintext data into an unintelligible ciphertext format using intricate mathematical operations; the data may then be decrypted using the encryption key.

Hash functions like SHA-256, SHA-512, and SHA-3 are also used to secure data at rest. These algorithms take in a plaintext message and output a fixed-length string, called a hash value, which is unique to that message. Hash functions are used for integrity checking and data verification.

Secure communication protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are utilized for data in transit. These protocols use mathematical algorithms to establish a secure connection between two parties and encrypt the data as it is transmitted.

In addition, digital signatures are also used to secure data in transit. Digital signatures use mathematical algorithms like RSA and ECC to create a unique code that is sent with the data, which can be used to verify the authenticity and integrity of the data.

Mathematical algorithms are essential to the security of data in cloud systems. They offer the fundamental security measures that guarantee information is shielded from unwanted access, modification, and disclosure.

VII. Conclusion

With the increase in demand for cloud technology, data security has become a vital challenge in this area. Various techniques have been proposed to save and protect the data to achieve a great level of data security. However, more efforts are needed in this field to make it a success. This field needs to be considered by the research community to gain the trust and reliance of the users. This paper reviews threats and concerns about the security of data and maintaining privacy, which focuses on how to store, manage, safeguard and maintain the data in the cloud systems. Security approaches using mathematical modelling have also been focused on. Therefore, it's critical to choose and implement suitable models for threat detection, system failure, and recovery to design effective security in cloud environments.

Conflict of Interest:

There was no relevant conflict of interest regarding this paper.

Reference

I. A. Seccombe, A. Hutton, A. Meisel, A. Windel, A. Mohammed, & A. Licciardi. : 'Security guidance for critical areas of focus in cloud computing'. *Cloud Security Alliance*. Vol. 2(1), 2009.

II. A. Behl. : 'Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation'. *Proceedings of the World Congress on Information and Communication Technologies (WICT '11), IEEE*. pp. 217–222, December 2011. 10.1109/WICT.2011.6141247

III. AL-Museelem Waleed, Li Chunlin. : 'User Privacy and Security in Cloud Computing'. *International Journal of Security and Its Applications*. Vol. 10(2), pp.341-352, 2016.

IV. A NGENZI et al., : 'Applying mathematical models in cloud computing: A survey'. *IOSR Journal of Computer Engineering*. Vol. 16(5), pp. 36-46, 2014. 10.9790/0661-16523646

V. A. Pandey, R. M. Tugnayat, and A. K. Tiwari. : 'Data Security Framework for Cloud Computing Networks'. *International Journal of Computer Engineering & Technology*. vol. 4(1), pp. 178–181, 2013.

VI. D. Chen and H. Zhao. : 'Data security and privacy protection issues in cloud computing'. *Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), Hangzhou, China*. vol. 1, pp. 647–651, March 2012. 10.1109/ICCSEE.2012.193

VII. E. Anwar J. Alzaid. : 'Cloud Computing: An Overview'. *International Journal of Advanced Research in Computer and Communication Engineering*. September 2013.

VIII. F. Gilbert. : 'Proposed EU data protection regulation: the good, the bad, and the unknown'. *In: Journal of Internet Law*. Vol. 15 (10), pp. 20-34, 2012.

IX. H. Zwingelberg, M. Hansen. : 'Privacy Protection Goals and Their Implications for eID Systems*'. In Camenisch, J. (Ed.): Privacy and Identity Management for Life. Springer, Berlin*. pp. 14-31, 2012.

X. J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel. : 'Seeding clouds with trust anchors'. *Proceedings of the ACM workshop on Cloud computing security workshop (CCSW '10), ACM*. pp. 43–46, October 2010. 10.1145/1866835.1866843

XI. K. D. Bowers, A. Juels, and A. Oprea. : 'HAIL: a high-availability and integrity layer for cloud storage'. *Proceedings of the 16th ACM conference on Computer and Communications Security, ACM, Chicago, Ill, USA*, pp. 187–198, November 2009. https://eprint.iacr.org/2008/489

XII. K. D. Bowers, A. Juels, and A. Oprea. : 'Proofs of retrievability: theory and implementation'. *Proceedings of the ACM Workshop on Cloud Computing Security (CCSW'09)*, pp. 43–53,November 2009. 10.1145/1655008.1655015

XIII. L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas and F. AlDosari. : 'A secure cloud computing model based on data classification'. *Elsevier*. Vo. 52, pp 1153-1158, 2015. 10.1016/j.procs.2015.05.150

XIV. M. A. Shah, R. Swaminathan, and M. Baker. : 'Privacy-preserving audit and extraction of digital contents'. *IACR Cryptology EPrint Archive*, vol. 186, 2008. https://eprint.iacr.org/2008/186

XV. M. Z. Meetei. : 'Mathematical model of security approaches on cloud computing'. *International Journal of Cloud Computing*. Vol. 6 (3), pp.187 – 210, 2017. 10.1504/IJCC.2017.086710

XVI. P. Mell and T. Grance. : 'The nistdefinition of cloud computing'. *National Institute of Standards and Technology*. vol. 53(6), article 50, 2009. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

XVII. R. Latif, H. Abbas, S. Assar, and Q. Ali. : 'Cloud computing risk assessment: a systematic literature review'. *Future InformationTechnology, Springer, Berlin, Germany*. pp. 285–295, 2014. 10.1007/978-3-642-40861-8_42

XVIII. S. Bollavarapu and B. Gupta. : 'Data Security in Cloud Computing'. *International Journal of Advanced Research in Computer Science and Software Engineering*. Vol. 4(3), March 2014.

XIX. S. Ali Abbas, A. A. Baqi Maryoosh. : 'Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography'. *Journal of Computer Engineering*. Vol. 17(4), Ver. I, pp. 48-53, 2015.

XX. V. Biksham, Dr. D.Vasumathi. : 'Query based computations on encrypted data through homomorphic encryption in cloud computing security'. *International Conference on Electrical, Electronics, and ptimization Techniques (ICEEOT)*, 2016 .978-1-4673 9939-5/16, 2016.