International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.509

e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3451-3453

Exploring Various Approaches for Secure Data Storage in Cloud Environments

Aswathy N Rajan[1], Anoopa Ravindran[2], Avani S[3], Anithamol K P[4]
[1,2,3,4]Assistant professor, Department of CA, Saintgits College of Engineering (Autonomous), Kottayam, Kerala, India.
Email ID: *aswathy.nr@saintgits.org[1], anoopa.r@saintgits.org[2], avani.s@saintgits.org[3], anithamol.kp@saintgits.org[4]*

Abstract

Cloud computing has modified the way the data is stored and accessed. Even if the shared nature of cloud environments may leads to security challenges. This paper provides a comprehensive overview of various strategies used and using for securing data at rest in the cloud environment. This paper delve into the core ideas of data encryption, access control mechanism and data integrity, studying there strengths, drawbacks and accessibility to different cloud aspects. This paper also deliberate emerging trends like homomorphic encryption and block-chain based solutions, which offer innovative approaches for enhancing data privacy and security. By analyzing this approaches in depth, this paper identify the optimal strategies for protecting sensitive data stored in the cloud.

Keywords: *Cloud Computing, Data Security, Encryption, Access control*

1. Introduction

Cloud Computing is a transformative technology which redefined the traditional way of computation, data storage, memory management, server management and infrastructure management etc . Cloud computing delivering the computation services such as storage , servers, software etc over the internet which benefits massive scalability and availability. Advantages such as cost-effectiveness, massive scalability, large memory capacity, remote accessibility and availability, automatic backup and disaster recovery, and real time collaboration has driving the companies increasingly rely on cloud storage. So that robust security strategies are essential to protect data at all levels of cloud computing life cycle such data in-transit, data-at-rest, data lineage, data remanence. Despite the numerous advantages of cloud computing, it is accompanied by significant security challenges for stored data. Some of the security challenges faced by the cloud stored data due to its shared nature are data breach, data loss and corruption, data privacy, third party risk etc. Malicious actors can exploit vulnerabilities in the cloud environment to steal the sensitive data.

2. Background

2.1. Encryption

Data encryption is a security mechanism which transforms the plaintext into cipher text for protecting sensitive data from unauthorized access. It include use of various cryptographic algorithms which scramble the plain text to unreadable format so that no one can decrypt the data without the correct decryption key. An encryption algorithm is a mathematical function which convert the plain text to ciphertext. Two Primary encryption techniques are there namely symmetric encryption and asymmetric encryption. Symmetric Key encryption uses same key for both encryption and decryption process while asymmetric key encryption uses different keys named public key and private for encryption and decryption respectively. Hybrid encryption combines the features of both symmetric and asymmetric encryption where symmetric key is used for encryption and the symmetric key will be encrypted using public key of the recipient.

2.2.Access Control

Access Control is a critical component in cloud data security which prevents unauthorized access of cloud hosted data and services. Different types of access control mechanisms are existing such as Role-Based Access Control (RBAC), Attribute Based Access Control (ABAC) and Identity Based Access Control (IBAC). Role-Based Access Control (RBAC) is a granular access control approach where access will be granted based on the role in an organization. Attribute Based Access Control (ABAC) is a flexible and dynamic access control mechanism in which access will be given based on the attributes of the user, environments and resources. Identity-Based Access Control (IBAC) which eliminate the use of password-based authentication by using digital certificates for authenticating users and devices.

3. Exploring Encryption Technique Used in Cloud Storage

ManishKo the, Harshal Karandikar, Nikhil Vani, Sumit Ta mkhane [1] proposed an encryption model named Attribute Based Encryption (ABE). Attribute Based Encryption is a powerful cryptographic technique to secure sensitive data and access over cloud data. In ABE a central authority will generate a master key and a public key. Users are given unique identities, defined by their attribute and issued private key associated with these attributes. The owner of the data will encrypt the data using the public key and the set of attributes which defines the access policy. User can decrypt the data only if their private key contains the attributes sufficient to satisfy the access policy. There are two types of Attribute Based Encryption techniques, named Key-Policy ABE(KP-ABE) in which the access policy is embedded within the user's private key and cipher text is associated with a set of attributes ,also user can access the cipher text if their private key satisfies the required access control and Ciphertext-Policy ABE(CP-ABE) in which access policy is embedded with cipher text , user's private key is associated with attributes and user can decrypt the cipher text if their attributes satisfy the access policy embedded in the cipher text. Advantages of Attribute Based Encryption are fine- grained access control by enabling complex access policies, dynamic access policies, massive scalability, strong security and privacy. Swati V.Thakre, Prof. K.K Chhajed, and Prof. V.B Bhagad[2] proposed a frame work for protecting sensitive data by using RC4 as encryption technique, PKG generator for key management and access control. The proposed system includes four components : the client, sanitizer, cloud and the Private Key Generator. Data blinding is the primary step where client identifies and blinds the information and blinded data is replaced with special markers. Sanitization is the procedure where sanitizer receives the blinded document, sanitizes the sensitive information and replaces the blinded markers with the legitimate data. Later the sanitized document will be uploaded to cloud. Liang Liu and Jun Ye [3] presented a homomorphic universal re-encryption scheme that leverages Identity Based Proxy Re-encryption. Homomorphic encryption is a cryptographic technique which permit arithmetic computations on cipher text. Identity Based encryption is a cryptographic technique where user's public key can be any arbitrary string such as email, phone number etc. Identity Based Proxy Re-encryption is cryptographic technique that performs transformation of a ciphertext encrypted for one user into a cipher text encrypted for another user. The re-encryption process is implemented by a re encryption key which is derived from the identities of sender and receiver instead of their public key. Homomorphic encryption is employed to safeguard the master secrets. However fully homomorphic encryption can hinder performance. A new identity based proxy re-encryption scheme has been proposed that works to minimize the workload on the user side by assigning the responsibility of re-encryption key generation to the proxy server. This technique is very essential for ensuring security in communication and data transfer over heterogeneous network infrastructure in modern times. Avinash Shukla,Sanjay Silakari and Uday Chourasia[4] proposed a security mechanism in cloud storage that utilizes Attribute Based Encryption(ABE). Their proposed system incorporates improved lockbox algorithm and Advanced Encryption Standard for increase the confidentiality. The computation time and cost will be less. In lockbox algorithm technique data is encrypting using a key whereas an improved lock box algorithm enhance the data confidentiality by strong key generation, enhanced key management, increased encryption strength, Resilience to attacks. AES is a widely used approach with robustness, efficiency and flexibility. Combined technique of AES and lockbox algorithm can achieve data encryption with strong encryption key, AES encryption key can be encrypted using improved lock box algorithm so that key remains protected even if data is compromised.

Conclusion

This paper looked into various approaches for secure data storage on cloud environment. In cloud environment data security is very important. Encryption plays a vital role in protecting sensitive information from unauthorized access. Symmetric and Asymmetric method provide effective solution for data protection , hybrid encryption combines the strength of symmetric and asymmetric encryption and thus by providing more security on the data stored in the cloud. Access Control mechanisms like Role-Based Access Control and Identity Based Access Control ensures that only authorized users will access the data. Innovative encryption techniques are proposed to enhance cloud data security. Homomorphic encryption and Identity Based Proxy Re-Encryption technique implemented advances features. The Integration of AES with lockbox method strengthens encryption mechanism. These techniques collectively contribute to addressing the challenges of data security in cloud environments.

References

[1]. ManishKo the, Harshal Karandikar, Nikhil Vani, Sumit Ta mkhane :Attribute Based Encryption with verifiable Outsourced decryption.International Research Journal Of Engineering and Technology .(2016).

[2]. Swati V.Thakre, Prof. K.K Chhajed, and Prof. V.B Bhagad, “Key Based Encryption scheme for Secure Data Sharing on Cloud”International Research Journal Of Engineering and Technology

[3]. Liang Liu and Jun Ye :”HoneyGen: A Homomorphic Univeral Re-encryptor for Identity-Based Encryption”,International Journal of Network Security(2016).

[4]. Avinash Shukla,Sanjay Silakari and Uday Chourasia, “A Secure Data Storage Over Cloud using ABE Approach.” International Journal of Computer Applications(2017)