INTERNATIONAL JOURNAL · ENGINEERING RESEARCH ·

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 27th Aug 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-08

DOI: 10.48047/IJIEMR/V10/I08/15

Title AN ENHANCED LATTICE BASED DATA SECURITY IN CLOUD ENVIRONMENTS

Volume 10, Issue 08, Pages: 94-102

Paper Authors

Sathish Kumar Gundala, Dr. A. Ramesh Babu

AN ENHANCED LATTICE BASED DATA SECURITY IN CLOUD ENVIRONMENTS

Sathish Kumar Gundala, MTech,(Ph.D)
Research Scholar , Department of computer science, Chaitanya Deemed to be University,
Email: sathishgundala86@gmail.com

Dr. A. Ramesh Babu, MTech, PhD.
Professor , Department of computer science , Chaitanya Deemed to be University,
Email: rameshadloori@gmail.com

Abstract---The model of "cloud computing" is regarded as the software revolution. Cloud storage users retain large volumes of their private data, where they often face dangers. While user data is not entirely controlled, consumers require a solid data management system with comprehensive security measures. Consumer data storage protection is a complex and challenging procedure. Different security risks must be secured from user data. There is a lot of misunderstanding as to whether the user's personal information is confidential. Encrypting data can be an effective option prior to retrieval. This study utilises a hybrid data protection system with security containment characteristics. A novel technique for assigning functions and duties using the lattice model has been explored. In this model. In this strategy, an upgraded cloud security approach based on gateways ensures effective access to private information. This model uses a CloudSim simulator in which the virtual machine is produced and applied and tested with a configuration balance. The proposed method is safer and easier for users to submit or update their papers. This research employed the greatest possible means of comparing techniques. The experimental results show that the proposed system is more efficient.

Keywords---Cloud Computing (CC), Cloud Security(CS), Cloud *Environment(CE), Lattice Based Security(LBS), Data Security(DS), Data Storage Security(DSS)*

1. Introduction

Cloud computing comprises of an on-demand infrastructure pool that allows the user to use any of these resources without incident or problems. The pricing of cloud services generally relies on how many resources they use[1]. As a result, cloud providers provide enhanced services, however some darkness prevents them from delivering greater standards of performance owing to their varied terms and conditions[2]. The cloud offers several advantages, including on-demand services, the lack of data storage hassles and the ability to access stored data without location-specific charges, which makes it especially attractive to the two client groups above[3-4]. Third-party Cloud infrastructure handles and stores data for the clients (as opposed to a service within the company itself), but relieves them from liability. The cloud computer offers numerous advantages over any data kept on a traditional computer platform, however the data is subject to many external assaults. Although it is crucial for cloud providers to keep data secure, they must be able to continuously grow to meet new and rising demand. Sometimes cloud providers may not offer clients with the accurate or comprehensive information, for example, cloud providers conceal data failure incidents [5-6].

CC is the next generation technologies in the Internet that provide all the computing capabilities for consumers, determines their individual needs through a subscription to an environment, therefore offering everything they need for commercial activities. The consumers will be able to acquire the computing tools they need when they need them by buying internet services instead of purchasing a pre-defined server or device[7]. We offer flexible auto service capabilities on demand in the cloud, broad network connectivity, scalable resource pooling and real-time response. We also already recognized essential aspects of the cloud, such as self-service, calculation, pre-based networking, and wide-ranging elasticity[8]. The value of cloud storage is that it gives users access to data and services anywhere and every time, which appeals and transfers their responsibilities over time to customers who operate in multiple places. It provides numerous advantages as its infrastructure expenses are minimal, very scalable, no maintenance is required and just requires a proportional use. The long-term retention is another major use in cloud computing, which is characterized by the amount of work once written and always recovered[9-10]. As long as the data is maintained and handled appropriately, there is no need to increase it, it must also maintain a demand for retrieval and conformance. to implement cloud modelling, involving the public cloud, the proprietary cloud and a combination of private and group cloud computing Due to the rapid trend in cloud computing and the shift of responsibility towards cloud service providers (CSPs), the most positive aspects of cloud computing are becoming obsolete, and contribute to decreasing power levels and the inability of users to use them fully to perform critical activities within their records[11].

1.2 Data Storage in Cloud Environment

Cloud storage is a paradigm for data storage in which the digital data is kept in logical pools, while the physical storage covers numerous servers (and frequently places), and where a hosting firm generally owns and manages the physical environment. These cloud storage providers are responsible for ensuring that the data is available and accessible while protecting and executing the physical environment[12]. Persons and organizations buy or lease the providers' storage space to store user, organisation or application data.

Cloud
Storage

Fig 1.1: Basic cloud data storage system [13]

Cloud storage services can be accessible via a co-located cloud computing service, an API or API-utilised apps like cloud desktop storage, cloud storage gateway or web-based content management systems. It is built into highly virtualized infrastructure and, as with accessible interfaces, flexibility and scalability, multiple tenancy and measured resources[14], is similar wider cloud computing. Off-site (Amazon S3) cloud storage services can be used or implemented onsite.

1.2.1 Some advantages of storing data in cloud environment

Companies simply have to pay for their storage, usually an average use over a month[15]. This does not indicate that cloud storage is lower, but that operational expenditures are more expensive than capital.

- Cloud storage companies may reduce their energy use by up to 70% and make them greener. At the vendor level they deal with greater energy levels and so equip them to reduce costs.
- Data protection and storage access are fundamental to the object storage architecture, and so extra technology and effort and expense to increase availability and protection can be avoided depending on the application.
- Maintenance storage duties such as acquiring more storage capacity are discharged to a service provider's duty.
- Cloud storage offers customers quick access via a web-service interface to a wide range of resources and applications housed within another organization's infrastructure.
- Cloud storage may be used to copy virtual machine images from the cloud into locations or to import a virtual machine image to the cloud image library from the location on site. Cloud storage may also be used to transport virtual pictures from user accounts to data centers.
- Cloud storage may be utilised as a natural catastrophe proof backup, because 2 or 3 separate backup servers usually exist.

1.3 Data Security in Cloud Environment

Cloud computing security is a developing sub-domain of computer security, network security and information security more broadly. This refers to a wide range of policies, methods and controls for the protection of data, applications and related cloud computing infrastructure[16].

Cloud computing and storage solutions provide consumers and companies many ways of storing and processing their data in third-party data centers. In a range of services models (SaaS, PaaS and IaaS) organizations employ Cloud and deployment methodologies (Private, Public, Hybrid, and Community).

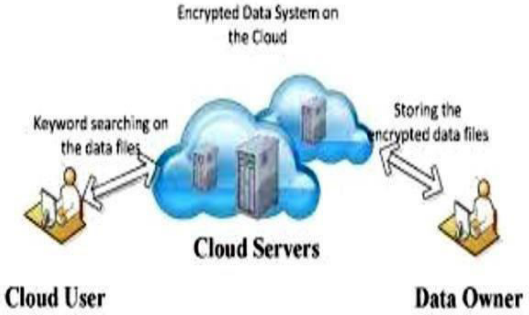
Encrypted Data System on the Cloud
Keyword searching on the data files
Storing the encrypted data files
Cloud Servers
Cloud User
Data Owner

Fig 1.2: Basic structure of Cloud data security system [17]

However, the security problem has become most important when the cloud becomes fully controlled by all information and data[18].

The most important component of security is confidentiality, integrity, authentication, authorization, non-repudiation and availability.

- **Confidentiality:** Confidentiality states that only sender and destination may have access to intended information. • Confidentiality: If an unauthorized individual accesses a communication, it becomes compromised. Data encryption is one of the most common security measures before data is sent to the cloud.
- **Integrity:** it requires the consistency, correctness and confidence of data across its full life cycle. When a communication is altered before it reaches the intended receiver, the message's integrity is lost. Data integrity is preserved by hacking methods, digital signatures and message authentication codes. Integrity concerns are large because of the cloud's multi-tenancy feature.
- **Authentication:** Authentication is a technique by which systems may identify their users safely. The level of access to system resources given to a certain authorized user is determined.
- **Authorization:** Authorization is a key need of information security for the maintenance of referential integrity in cloud computing. It is followed by control and rights over Cloud computing process flows.
- **Non-repudiation:** Non-repudiation is an expansion to the ID/AC service. It does not let the sender of a message to contest the assertion that the message has not been sent. It is used to make sure that the messages sent are received correctly and the sender receives confirmations. In other words, a two-way communication is established between a sender and a recipient.
- **Availability:** the availability principle stipulates that resources should always be available to third parties. The best way to assure availability is by the diligent maintenance of all hardware, repairing hardware quickly when required and keeping a working operating system environment which is free from software conflicts. It is also necessary to update system upgrades.

Cloud computing is a long-awaited computer method with a huge storage capacity. Cloud users often have to cope with a variety of flaws and dangers which might occur in their personal data storage because of their large volume of private data. In contrast to self-contained data, all of which are under total control, user data are always in danger of being changed, and hence significant and robust measures are necessary to maintain data security. It is tough and hence a task to keep the user data secure, therefore preventing any security risks from the user's data. User privacy is difficult to protect when dealing with user information and this is of great importance to companies and their consumers. The main need is to make sure that the data is illegible before it is stored. In this study, a multi-layered protection using the user's lattice security system plus the lattice database association approach for data security is proposed. The current approach to tasks and tasks is utilised, where the lattice paradigm is integrated with the role-oriented project structure of the project manager.

The suggested system was tested with CloudSim. The cloud is used to build, install, manage and maintain the general framework and framework architecture for simulation design and deployment. The library and APIs are built in Java for this programmed. It provides business apps that are cloud based without user participation in the implementation or installation process. It offers numerous ways to align with the business application ecosystem and even complicated operations without human involvement. To secure user data confidentially, a number of layers of protection have been created, which gives a simple way to bring a dataset to life and allows access to rights A thorough evaluation criteria for the systematic assessment of stable systems and commodities have already been provided in the Orange Book. As opposed to the more risky prior security paradigms, the BLP paradigm is best described as a security era. Because of its pure look, the grid is used in this BLP and user data is safeguarded in the cloud.

Lattice-based access enables security and so restricts access to the concept of an attacker. You can prevent and prevent illegal publishing and provide and preserve availability using a grid access monitor. You are protected from hacker attempts. These procedures are up and up according to the data classification scheme. There are two layers of encryption for transit data and one for rest data.

2. Literature Survey

In order to safeguard the customers' sensitive data from an attack, attribute-based encryption is used. It is split into slices before publishing the data. Optimized revocation in the form of slices is delivered and saved in the cloud. Only one slice is retrieved and republished once the content has changed [20] when a revocation is made. In addition to the AES method, the V.S. Mahalle[21] presented a homomorphic algorithm. They uploaded a file to cloud storage utilizing the homomorphic method for data verification without decryption. They did not, however, employ a hybrid method. The grid suggested in the BLP model was utilised in general but not on any particular domain. A grid-based representation of the BLP model is used for health records in our model. Furthermore, the document set and the roles and duties change. Another study[22]N. Singh and P. Deep Kaur suggested that the cloud data be coded in a hybrid manner. But this study uses the AES technique to encrypt the data and encrypts the private key using the RSA algorithm. Data and key encryption and decryption are performed using two distinct approaches. The difficulty, however, is that the hybrid approach is not employed to fully safeguard the data. Moreover, its performance is not as excellent as the technique provided by us, because one algorithm is used for data encryption and another is used for encryption rather than data encryption. This study was conducted for dual data encryption and improved security. K.R.Monisha[23] suggested the establishment of a safe storage system utilising the AES and RSA algorithms. They utilised AES algorithm to encrypt and decode information, and only the key is decrypted using the RSA method. This technique is distinct from ours since both algorithms encrypt and decrypt data. The framework for safeguarding user data saved on the server using hybrid algorithms has been suggested by Mihir Shah and Sujata Pathak[24]. A prototype to ensure data confidentiality and integrity using symmetric cryptography where data is encrypted is proposed by Birago and Isaac Ofori. All operations are carried out on the client side [25]. The Aamrapali Murlidhar Tamgadge and Vikram Raut algorithms[26] discuss protection of submitted data file, video and audio files in the article.

3. Existing Method

In cloud environments a lattice-based method was previously used to protect data before they were established. In the original publication, a hybrid grid-based encryption method was used using AES and RSA in Java-written API scripts. The 128-bit AES encryption is acceptable for a wide range of applications, but is not necessary to any application. A password may be not brute, even if just for a little amount of time or power, so the duration is useful even if you run for a limited resource availability. Modes (more than standard cyphers) and Advanced Authentication Standard (more than the Advanced Encryption Standard) (AES). Although it provides more security in certain areas, including brute force assaults in others, it is not sufficient to give the requisite level of protection. Thus, by adding another sheet, the encoding technique Rivest-Adle is added (RSA). The RSA world takes care of both the risk of a Trojan horse and the basic brute force assaults.

4. Problem statement

The existing lattice control technology that uses hybrids AES and RSA has a serious challenge of temporal complexity. While the hybrid AES and RSA algorithms improve data protection, they take a long time to finish the operation, which might raise the danger of data leakage and reduce the dependability of the data storage. Besides this RSA, a sufficient amount of quantum computer space is certainly not. Whereas there is no safety evidence of the algorithm itself in AES. In instances when massive data has to be encrypted from the same machine, the RSA method might be extremely sluggish. It needs a third party to verify that public keys are reliable. Data sent using the RSA method may be compromised by intermediaries who can meddle with a public key system. The AES utilises an algebraic structure that is too simple to perform but also trivial to hack. Every AES block is always encrypted in the same way that the execution time to decode data is increased. AES also occasionally faces problems with hard to implement software.

The hybrid AES and RSA model is a very time-consuming technology that must be addressed with some efficient AES and RSA hybrid technology, such DES, Triple DES and IDEA.

5. Objectives

1. To explore the problems of cloud computing in real time.
2. To improve the current problems in the cloud computing application, analyse the unattended advance approach.

3. Implement the hybrid technology to improve security and time complexity in cloud applications.
4. Compare the strategy proposed with the basic approach.

6. Motivation

Some have claimed that cloud storage in the form of a security paradigm has already begun to develop. Two ways to maintaining data integrity exist for service providers: the first is to ensure that only authorized persons have access to data; the second is to the contrary (leakage) that no one has exclusive access to specific information. If undesirable vulnerability is taken from the customer's details, maintaining secrecy and privacy in the cloud becomes harder. This is why data may be protected before it is saved in order to decrease protection threats. A concise and effective data protection plan has been designed to ensure needless abuse and interference in the consumer community's data. The new concept is to implement hybrid algorithms in a single application after implementing the access control matrix. It offers greater safety than a typical algorithm.

7. Conclusion

Cloud infrastructure is a current, distinct market idea services on demand for multiple companies, utilizing the web rather than being bound into contracts with providers for continual usage. However, with cloud computing the server and servers are centralized in the huge data centre, where data and features of the service are less essential. That's what we shouldn't miss when we look at the operating standard. Cloud storage services are far more useful than conventional storage systems, especially in terms of growth, as well as in connection with portable usage, complexity and functionality, given scalable features, advantages and minimum costs. This article discusses data protection policies and focuses exclusively on storage.

8. Reference

[1] A. Mahendiran, N. Saravanan, and N. Sairam, "A review on leaders in cloud computing service providers and cloud SQL a case study," Res. J. Appl. Sci. Eng. Technol., vol. 4, no.17, pp. 2926–2933, 2012.

[2] Sandra Durcevic, "Cloud Computing Risks, Challenges &amp; Problems Businesses Are Facing," Business Intelligence, 2019. [Online]. Available: https://www.datapine.com/blog/cloud-computing-risks-and-challenges.

[3] A. Rajathi and N. Saravanan, "A survey on secure storage in cloud computing," Indian J. Sci.
Technol., vol. 6, no. 4, pp. 4396–4401, 2013.

[4] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents.," IACR Cryptol. ePrint Arch., 2008.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, doi: 10.1007/978-3-642-04444-1_22.

[6] J. Xue and J. J. Zhang, "A brief survey on the security model of cloud computing," in Proceedings - 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, DCABES 2010, 2010, doi: 10.1109/DCABES.2010.103.

[7] Tadapaneni, N. R. (2018). Cloud Computing: Opportunities And Challenges.

International Journal of Technical Research and Applications.

[8] Wang C , Wang Q et al . (2012),Towards secure And dependable Storage Services in Cloud Computing , IEEE Transactions on Services Computing ,vol5(2),220-232.

[9] Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.

[10] Dong B , Zheng Q et al.(2012). An optimized Approach for storing and Accessing small files on cloud storage,Journal of Network and Computer Applications ,35(6),1847-1862

[11] Deahmukh P M,Gughane A S et al.(2012).Maintaining Files Storage Security in Cloud Computing International Journal of Emerging Technology and Advance Engineering ,vol2(10),2250-2459.

[12] Tang Y,Lee P P C et al(2010).FADE: A Secure overlay Cloud Storage System with File assured Deletion ,6th International ICST Conference, Secure Comm.

[13] Rakhi Bhardwaj, Vikas Maral, "Dynamic Data Storage Auditing Services inCloud Computing", in the year of April 2013.

[14] Yogita Gunjal, Prof. J.Rethna Virjil Jeny, "Data Security and Integrity of Cloud Storage in Cloud Computing", in the year of April,2013.

[15] Wang W,Li Z et al(2009).Secure and efficient Access to outsource Data, CCSW '09 Proceedings of the 2009 ACM workshop on
Cloud Computing Security,55-66.

[16] Tadapaneni, N. R. (2016). Overview and Opportunities of Edge Computing. Social Science Research Network.

[17] Ensuring Data Storage Security in Cloud Computing. IOSR Journal of engineering – vol 2 (12) - (2012) 225.

[18] Spillner J, Muller J et al (2012).Creating Optimal Cloud Storage System,future Generation Computer Systems ,vol29(4),1062-1072

[19] Liu, Allan and Yu, Ting, Overview of Cloud Storage And Architecture (2018). International Journal of Scientific & Technology Research

[20] Y. Cheng, Z. Y. Wang, J. Ma, J. J. Wu, S. Z. Mei, and J. C. Ren, "Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage," J. Zhejiang Univ. Sci. C, vol. 14, no. 2, pp. 85–97, Feb. 2013, doi: 10.1631/jzus.C1200240.

[21] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm," in 2014 International Conference on Power,Automation and Communication, INPAC 2014, 2014, pp. 146–149,
doi:10.1109/INPAC.2014.6981152.

[22] N. Singh and P. Deep Kaur, "A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks," Int. J. Database Theory Appl., vol. 8, no. 3, pp. 145–154, 2015, doi:10.14257/ijdta.2015.8.3.12.

[23] K. R. Monisha, "Secure Cloud Computing Using AES and RSA Algorithms,", International Journal of Advances In Computer Science and Cloud Computing, Volume-3, Issue-1, 2015.

[24] M. Shah and S. Pathak, "Hybrid Cryptosystem for Secure for Secure Data Storage," Int. J. Innov. Res. Inf. Secur. Issue,vol.11,pp.1–04,2017,
doi:10.26562/IJIRIS.2017.NVIS10080.

[25] A. Adjei, F. Ofori, B. Birago, and I. Ofori, "Enhancing Security in the Cloud using Encryption in a Client Centric Access Control Mechanism," ,British Journal of Computer, Networking and Information Technology, Volume 1, Issue 1, pp. 19-48, 2018.

[26] A. Murlidhar Tamgadge and V. Raut, "Privacy Preserving of Data Files & Audio / VideoEncryption-Decryption Using AES Algorithm", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 6 Issue:5,pp. 238 - 242, 2018

[27] N. Saravanan , Dr. A. Umamakeswari , Lattice Based Access Control for Protecting User Data in Cloud Environments with Hybrid Security, Computers & Security (2020),doi:doi.org/10.1016/j.cose.2020.10207