Prevention of EDoS Attack on Cloud Data using Dual Access Control Strategy

Shruti Anilrao Jari , Dr.Ranjit R Keole, Dr. Avinash P Jadhao, Naresh Vinod Wankhade
ME (Computer Science and Engineering) Scholar, Dr. RGIT&R, Amravati, India
Head of Department, Information Technology, HVPM's CET, Amravati, India
Head of the Department, Computer Science & Engineer DRGIT&R, Amravati, India
Lecturer in Information Technology, Government Polytechnic Amravati, India

Abstract: Data owners can distribute protected data utilizing cloud storage of legal person with maintaining accessibility control rules concealed using the Ciphertext-Policy Attribute-Based Encryption approach with a confidential access security strategy. Moreover, a technique to restrict clients from gaining subsequent data and provides the owner's limited amount of data on objects that create a dispute of interest or someone whose pairing is critical is still to be investigated. In this research, examine the fundamental relationships between these specific data items, establish the idea of the confidential documents set restriction, and suggest CP-ABE access control system for the confidential data set restriction with concealed properties. This approach entails a somewhat concealed, extendable restriction strategy. To improve protection, the responsibilities of implementing the access control mechanism and the restriction strategy are split into 2 autonomous units in proposed design, thanks to the clearly defined responsibilities concept. After the scheme has been established, the data holder can substantially update the personal data collection restriction design using the concealed restriction strategy.

Keywords: Data Security, Ciphertext, Confidential Data, Cloud Storage, Data Owner, Data Integrity, Authentication, Non-Repudiation, Confidentiality

I INTRODUCTION

Cloud Computing is well and truly the technology enabler for dynamic, on-demand service delivery of Internet services and computing resources to corporates and end-users. Cloud computing is referred to in different ways and approached from a variety of perspectives. As compared to traditional Information Technology services, Cloud services offer unlimited computing, storage, and networking resources, with easy to pay options bundled with significantly enhanced service availability, reliability, and reduced costs for infrastructure implementation and management

Ensuring the safety and security of information and communication technology and infrastructure has become a persistent race between the cyber attackers or black hats and the ethical hackers or defenders. With the rise of cyber-attacks on Cloud systems, service providers, web hosting, and Internet data carriers are required to ensure the highest consideration to the novel challenges posed by cyber-attacks like Distributed Denial of Service and Malwares. With new attack vectors and novel threats on the rise, corporate enterprises are required to protect infrastructure from the advanced attack methods being employed

Thereby, cryptography is the study of securing information and textual data by transforming users' messages to a cryptic non-readable type and also known as converting plaintext to ciphertext, and then going to execute a decryption process that restores the original plain text. Cryptography can be used to provide the appropriate safety measures for user data.:

Data Integrity: Integrity relates to preserving and ensuring the security and integrity of users' data, as well as its adoption of the computer technologies that hold, interpret, analyze and access user information [1].

Authentication: The procedure of verifying a user's digital credentials is known as authentication. It's the process of connecting a collection of unique privileges with just user requests.

Non-Repudiation: This is the guarantee that a person, agreement, and individual never dispute the legitimacy of convey a data that user created

Confidentiality: Becoming secretive or harbouring secret information is a condition

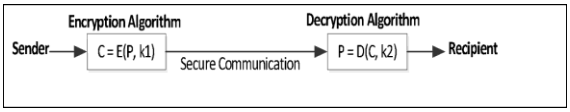

Fig 1- Process of Encryption and Decryption

Figure 1 illustrates the process of transforming plaintext data (P) into non - readable text (C) called as encryption and transforming that cipher-text back to plain text (D) utilising a collection of Cryptographic Techniques (E) and cryptographic keys (k1 and k2), as well as the decryption of the data (D) that reverses and generates the initial plain-text from the ciphertext.

This can be interpreted as $Ciphertext = E\ \{P, Key\}$ $and\ Plain\ text\ C = D\ \{C, Key\}$ciphertext

II PROPOSED SYSTEM

In CP-ABE approach, characteristics represent a crucial element in authorization compliance. As a result, extra dataset constraint-based properties can be utilised to address the condition. We employ dummy variables [9] in this approach since the further variables are solely used to manage the SDS restriction and therefore have no special meaning [10].

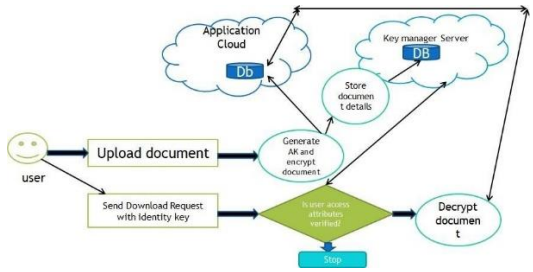

Figure 2 – Architecture of Proposed System

Figure 2 shows the complete architecture of proposed system with various entities to provide security to data.

Application Cloud: The application cloud is the data storage entity to share the data to users.

Data User: The data user is the ownership of the data items, which distributes to the cloud database during cryptography according to authorization settings.

User: The user has authority to access cloud server's protected files.

Key Manager Server (KMS): The Key manager server generate both the keys (private/public). This is regarded to somehow be semi-reliable. The Key manager server is only allowed to look at the data user's data objects, access policy, and constrained guidelines while it is performing valid responsibilities allocated to it through another individuals.

Attribute Verification: The data constraints for sensitive data items are enforced by the Attribute Verification entity. It's regarded to be semi-reliable. The Attribute Verification monitoring carries out activities that have been delegated to it by another objects, although it has access to the data user's objects. Some other important assumptions regarding the Attribute Verification monitoring were that it would trash the partly decoded cipher - text if the user is likely to breach some Attribute Verification constraint when access the relevant data item

CP-ABE Access Control Approach

SN	File Size (KB)	Existing System		Proposed System	
		Uploading Time (sec)	Downloading Time (sec)	Uploading Time (sec)	Downloading Time (sec)
1	562.85	1	1.4	0.5	0.8
2	48.56	1.3	1.5	0.7	0.9
3	43.58	1.5	1.7	1	1.2
4	15.69	1.7	2	1.3	1.5
5	10.35	2	2.5	1.5	1.8

Table 1 – Comparative Performance Analysis

The methods below are part of the accessing control strategy for the data constraint with the concealed authentication and authorization and the constraints strategy. For data items which are not subject to the dataset limitations, we eliminate the accessibility control mechanism in this approach. Following are some constraints performed for access control.

$Setup$ (1) –> ($PKKMS$, $MKKMS$), (PKS , MKS), ($PKDATA$, $MKDATA$). The KMS generate the both keys for data. The KMS monitors the output of both keys.

Key-Generate: $Key(MKKMS, S)$ –> SKu. The KMS gives the $MKKMS$ and list of attributes $S \in 2$ att\(0) as input and SKu is a private key for the user u.

Encryption: $Encry(PKKMS, PKS , PKDATA, M, T)$ –> CT. The data user takes $PKKMS$, PKS , and

$PKDATA$ to encrypt the data files M. CT is the ciphertext.

Decryption: $Decry(CT", SKu) -> M$. The user takes CT" and SKuas I/P and O/P files M if the process of data decryption is completed.

III RESULT ANALYSIS

Performance Analysis

The full model takes approximately of 5 seconds to complete all of the processes in this scenario. The fastest hardware arrangement takes 2 seconds to encrypt a 10 KB file. This model is quick enough to use in today's cloud computing systems. Functioning with the framework at various times and with various users, as well as single files of varying sizes, the contents change from one another. The overall model's implementation will require varied amounts of time. The length of the software varies based on the file size. A few of the numerous users' results is displayed in the tables.

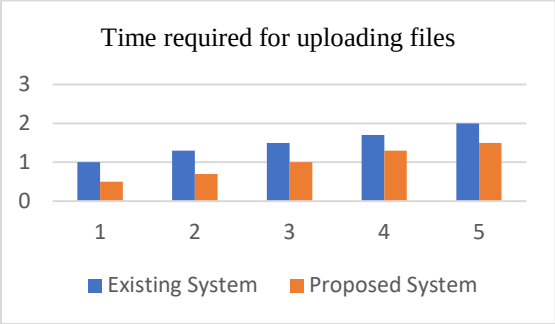

Figure 2: Time required for uploading the file

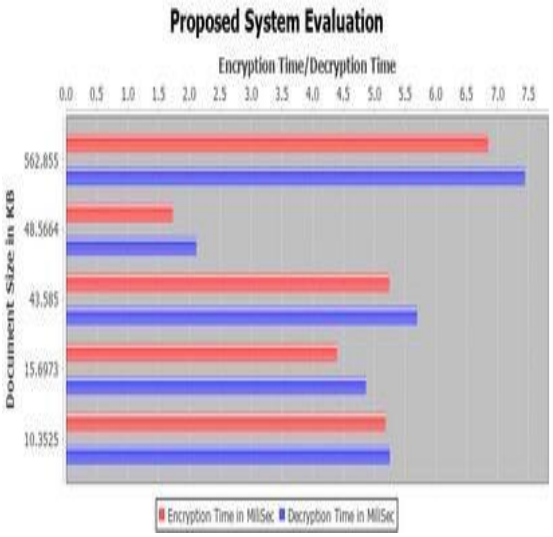

Figure 3- Encryption Time of Proposed System

IV CONCLUSION

The limitation arose from the cloud data security policy, and provided an access control scheme for generalized restrictions for cloud storage in this research. The proposed method uses CP-ABE approach with a disguised access mechanism. To dealt with the cloud security limitation by introducing fictional qualities and enlisting the help of a third party: the data monitoring. To impose the security restriction of data, a public/private key is encoded in data frames in which forces the cloud server to deliver the partly decoded encrypted data to the cloud for the next complete decoding process. To avoid industrial malpractice or errors, the cloud server monitoring is important for enforcing both the authorization and restriction policies. The proposed strategy is safe and reliable, according to the safety, policies confidentiality, reliability, and usability evaluations.

REFERENCES

[1]Mrs. Kavya B S, Shrilakshmi P V, Sushmitha N, Yamuna S., "Multi-Keyword Search Methodology for Cloud Data", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 4, April 2017.

[2]Pawan Kumar Tanwar, Ajay Khunteta, Vishal Goar, "Design and analysis of new multi-keyword ranked search schema called SSEDU in cloud computing", International Journal of Engineering Science, Special Issue, Vol. 26, December 2017.

[3]Ziqing Guo, Hua Zhang, Caijun Sun, Qiaoyan Wen, Wenmin Li, Secure Multi-Keyword Ranked Search over Encrypted Cloud Data for Multiple Data Owners, The Journal of Systems & Software (2017), DOI: 10.1016/j.jss.2017.12.008

[4]Parameshwar Rao D, S. Balaji, 2014, Secure Multi-Keyword Search over Encrypted Cloud Data, International Journal of Engineering Research & Technology (IJERT) CSECONF – 2014 (Volume 2 – Issue 14), 2014.

[5]Arunima Ratankumar, "Privacy-Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data", International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835 Volume-3, Issue-9, Sep.-2016.

[6]Hua Dai, Xuelong Dai, Xiao Li, Xun Yi, Fu Xiao, Geng Yang, "A Multibranch Search Tree-Based Multi- Keyword Ranked Search Scheme over Encrypted Cloud Data", Security and Communication Networks, vol. 2020, Article ID

7307315, 15 pages, 2020. https://doi.org/10.1155/2020/7307315

[7]D. Pradeepa, Dr. P. Sumathi, "Efficient Multi-User and Multi-Keyword Ranked Search Scheme for Encrypted Cloud Data", International Journal of Advanced Trends in Computer Science and Engineering, 9(3),May – June 2020, PP 2913 – 2917

[8]Yan-Yan Yang, Bei Gong, Zhi-Juan Jia, Ya-Ge Cheng, Yu-Chu He, "Research on the Ranked Searchable Encryption Scheme Based on an Access Tree in IoTs", Wireless Communications and Mobile Computing, vol. 2021, Article ID 3265934, 10 pages, 2021. https://doi.org/10.1155/2021/3265934

[9]Abdulaziz Aborujilah, Shahrulniza Musa, "Cloud-Based DDoS HTTP Attack Detection Using Covariance Matrix Approach", Journal of Computer Networks and Communications, vol. 2017, Article ID 7674594, 8 pages, 2017. https://doi.org/10.1155/2017/7674594

[10]NurmamatHelil, Kaysar Rahman, "CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy", Security and Communication Networks, vol. 2017, Article ID 2713595, 13 pages, 2017. https://doi.org/10.1155/2017/2713595

[11]A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, “Cloud security defence to protect cloud computing against TTP-DoS andXML-DoS attacks,” Journal of Network and Computer Applications, Vol. 34, no. 4, pp. 1097– 1107, 2011.

[12]S. Alsowail,M. H. Sqalli,M. Abu-Amara, Z. Baig, and K. Salah,“An experimental evaluation of the EDoS- shield mitigationtechnique for securing the cloud,” Arabian Journal for Scienceand Engineering, vol. 41, no. 12, pp. 5037–5047, 2016.

[13]M. N. Kumar, P. Sujatha, V. Kalva, R. Nagori,A.K.Katukojwala,and M. Kumar, “Mitigating economic denial of sustainability(EDoS) in cloud computing using in-cloud scrubber service,” in Proceedings of the 4th International Conference on Computational Intelligence and Communication Networks (CICN ’12), pp. 535– 539, Uttar Pradesh, India, November 2012.

[14]I. M. Mary, P. Kavitha, M. Priyadharshini, and V. S. Ramana,“Secure cloud computing environment against ddos and edosattacks,” 2014.

[15]C. N. Modi and D. Patel, “A novel hybrid-network intrusion detection system(H-NIDS) in cloud computing,” in Proceedings of the IEEE Symposium on Computational Intelligence in Cybersecurity (CICS 13), pp. 23–30, April 2013.