https://doi.org/10.46335/IJIES.2022.7.6.1 **e-ISSN: 2456-3463**
Vol. 7, No. 6, 2022, PP. 1-3

International Journal of Innovations in Engineering and Science, www.ijies.net

A Study on Techniques for Access Control and Key Management in the Cloud for Secured Communication

Mr. Ghanshyam S. Nikhade[1],Dr. Tryambak Hiwarkar[2]

[1]Student, [2] Professor, Sardar Patel University, Balaghat (M.P.)

shyamnikhade777@gmail.com

***Received on**: 25 April ,2022* ***Revised on**: 30 May ,2022,* ***Published on**: 1 June,2022*

***Abstract* –** *Cloud computing has originated with the exponential development of internet connectivity and infrastructure access. Cloud is a modern model for providing diverse applications to people on the internet, also referred to as the 'cloud,' for example web production frameworks, servers, storage and content. Cloud infrastructure often offers customers and companies different tools to use cloud technology in an easy and reliable way, without growing computing resources costs. Business may select between private, public or hybrid cloud implementation, depending on specific business requirements and security considerations. Most organizations follow this fast-growing paradigm to satisfy their computing requirements and develop their market. Cloud infrastructure offers tools for digital networks and other software used both by a customer and the businesses of the cloud service provider, such as network capability, storage and server utility. Instead of buying new hardware or services for its commercial uses, this enables consumers to use the cloud network as a commodity, technology and software as a service.*

Keywords- Cloud key Management, Crypto Graphic Schemes, Flexible Key Delegation.

I- INTRODUCTION

Cloud infrastructure design focuses mostly on device product configuration for cloud, hardware, middleware and applications, cloud consumers, cloud storage, and networking. Both these modules are mainly arranged with regard to the use of the cloud consumers and end users. A new paradigm focused on the possibility of holding large amounts of data and software is the cloud computer architecture. The aim is also to include these stored data and applications focused on consumer demands and flawless hardware and software access without substantial expenditure in own software, hardware or infrastructure. Figure 1 shows the cloud infrastructure architecture and the cloud design elements To resolve the security issues in cloud computing applications, access control policies are used as one of the security mechanisms to permit, deny or restricts the access to the cloud computing systems. Also, the existing access control techniques attempted to identify the users who are trying to access the system without proper authorization. According to Anderson (2010), Access Control is the security model which provides several constraints on the user's actions, which is performed in a system based upon the rules described by the access control mechanism. Figure 1.6 depicts the access control view point.

II- ANALYSIS

In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size.

https://doi.org/10.46335/IJIES.2022.7.6.1 **e-ISSN: 2456-3463**
Vol. 7, No. 6, 2022, PP. 1-3

International Journal of Innovations in Engineering and Science, www.ijies.net

Specifically, our problem statement is ―To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts (produced by the encryption scheme) is decrypt able by a constant-size decryption key (generated by 13 the owner of the master-secret key).‖ We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

III- DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

IV- CONCLUSION

How to protect users' data privacy is a central question ofcloud storage. With more mathematical tools, cryptographicschemes are getting more versatile and often involve multiplekeys for a single application. In this paper, we consider how to ―compress‖ secret keys in public-key cryptosystemswhich support delegation of secret keys for different cipher text classes in cloud storage. No matter which oneamong the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is moreflexible than hierarchical key assignment which can onlysave spaces if all key-holders share a similar set of privileges.A limitation in our work is the predefined bound of the number of maximum cipher text classes. In cloud storage ,the number of cipher texts usually grows rapidly. So wehave to reserve enough cipher text classes for the futureextension.

Although the parameter can be downloaded with cipher Texts, it would be better if its size is independent ofthe maximum number of cipher text classes. On the otherhand, when one carries the delegated keys around in amobile device without using special trusted hardware, thekey is prompt to leakage, designing a leakage-resilientcryptosystem [22], [34] yet allows efficient and flexible keydelegation is also an interesting direction.

V- ACKNOWLEDGMENT

A successful & satisfactory completion of any significant task is the outcome of invaluable contribution of efforts by different people in all directions explicitly or implicitly. Vast varied and valuable reading efforts leads to considerable gain of knowledge via books & other informative sources, but expertise comes from collateral practical works and experiences

I would like to thank, my Guide **Prof. Dr. Tryambak Hiwarkar** Faculty Of Engineering & Research Sardar Patel University, Balaghat (M.P.) for his support, encouragement and guidance during the period of my dissertation with a keen interest, enthusiasm and his ever-helping nature from the starting to the completion

of this dissertation.

Last but not the least; I am also thankful to all those who have directly or indirectly helped in completion of the dissertation.

REFERENCES

[1] *Sakshi Chhabra (2020) on "Security Enhancement in Cloud Environment using Secure Secret Key Sharing", Journal Of Communications Software And Systems, Vol. 16, NO. 4.*

[2] *Pradeep. K. V, Vijayakumar. V (2019) on "Secure Key Management System in Cloud Environment for Client data", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5*

[3] *Matthew Campagna, Shay Gueron (2019) on "Key Management Systems at the Cloud Scale", Cryptography, 3, 23; doi:10.3390/cryptography3030023*

[4] *Padinjappurathu Gopalan Shynu, Kumaresan John Singh (2017) on "An Enhanced ABE based Secure Access Control Scheme for E-health Clouds", International Journal of Intelligent Engineering and Systems, Vol.10, No.5*

[5] *Madhura Mulimani, Rashmi Rachh (2017) on "Analysis of Access Control Methods in Cloud Computing", I.J. Education and Management Engineering, 3, 15-24*

[6] *Sultan Aldossary, William Allen (2016) on "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4*

[7] *Kire Jakimoski (2016) on "Security Techniques for Data Protection in Cloud Computing", International Journal of Grid and Distributed Computing, Vol. 9*

1.