iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IX **Month of publication:** September 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Handover Key Management for Re-Authentication in Cloud Technology for Accessing Data Classes

P Dileep Kumar Reddy[1]
[1]*Lecturer Department of CSE JNTUA College of Engineering, Anantapur*

Abstract*: Cloud Technology is most widely emerging area in today's world, especially in IT sectors. Security is also a challenging task in accessing various classes of data in cloud technology. The existing system introduced a novel key generation and authentication schemes for classes and also introduced a tri-partite authentication scheme. As the cloud data can be accesses from anywhere and these data may be of various formats or classes. Each class of data requires re-authentication of the user or client. This paper presents a novel Handover Key Management (HKM) technique for re-authentication of data classes. This new technique helps clients for ease access of different data classes with respect to prioritized data classes. While developing HKM technique, many parameters are considered are security aspects like token authentication, generating keys for encryption and decryption of data and so on.

Index Terms: Security, Data Classes, Re-Authentication, HKM.

I. INTRODUCTION

Cloud Computing (CC) is the way of accessing resources over a network channel. The resources may be any of these such as Software, Hardware or an Infrastructure and also may be data of various classes. The different formats of data are called as Data classes. This technology is growing rapidly in today's world. The resources also called as services. These services can be provided by the cloud service provider. There is Service Level Agreement (SLA) between the service provider and the client.

The cloud services can be provided for days, weeks, months or yearly agreement. The use of this technology helps IT Sector to reduce its cost and time. This technology works most efficiently with the help of internet. If there is poor internet connectivity then the service might be properly delivered to the client.

The different formats of data that is structured or unstructured data can be categorized into different classes. The classes may be private, public and limited access which has been already introduced. Whenever the client is accessing some resource over a network channel, client must be authenticated in different levels.

All the data in a cloud centre is encrypted at the time of storage. Sometimes, if it is a public cloud, then the data is not enrypted. The data classes in any cloud can't be accessed until and unless the successful authentication of the client. Re-Authentication is required, if the client needs to access another class of data. The problem raises here, that is the way of authentication from one class to other class might be different and also moving or shifting from one class to other is called as Handover Authentication.

Data classes of one type will be accessed many times per day or some other classes of data may not be accesses at all. With this the cloud technology is facing the critical challenges for establishing secure communication of the most frequently accesses data class. For optimizing cost, partitions of data classes are done. There are many algorithms used for providing secure access to the clients,

This paper objective is to deal with HKM for Re-Authentication of various cloud data classes. The novel technique is proposed to handle this kind of situation. This technique is given in detail in the section of proposed system.

II. LITERATURE SURVEY

In this [1] paper, a new tripartite key assignment scheme is introduced for cloud data classes. And also tri-partite authentication scheme & graph is proposed for easier access of various cloud data classes. This paper presents the extension of the referred paper which is not introduced. A novel scheme is proposed for HKM for Re-Authentication of cloud data classes. The HKM issue is not addresses and developed in existing system.

Key generation and management is also addressed in the existing system. The problems on cloud data classes as well as authentication techniques are also taken into consideration while designing the model.

In different classes of data, how the keys are generated and managed at the time of authentication is discussed in [2]. This paper addresses the problem and given a solution which can be used temporarily. A cryptographic key generation scheme for multilevel data security is given in [3].

Honey pot cloud framework is used for classifying each data classes into four classes. There are many parameters are considered for providing security for data classes and then varied accordingly to the sensitivity of the class of data. These are addressed in [4] and proposed a three way classification of the data: Public, Private and limited access based on three cryptographic parameters [5].

III. PROPOSED SCHEME

This paper objective is to introduce a new Handover Key Management (HKM) for Re-Authentication of cloud data classes. HKM involves the process of exchanging keys from one data class to other data class simultaneously for re-authentication and continuing the access over data classes. The steps to be followed for HKM are:

A. Initiallyassume that the client is already authenticated and accessing a frequently queried data class.

B. Now immediately, client got the requirement of accessing another class of data. Then again, client must be re-authenticated for accessing that another data class.

C. The idea introduced here is storing the existing key in a database and making reuse of same key for authentication another data class.

D. This can be done by using secure authentication and the process may be like TLS handshake.

E. The similarity feature is established and re-authenticated the client. With this implementation, the number of keys can be reduced and key generation can be done only for one time per client.

The architecture for proposed system as follows:\

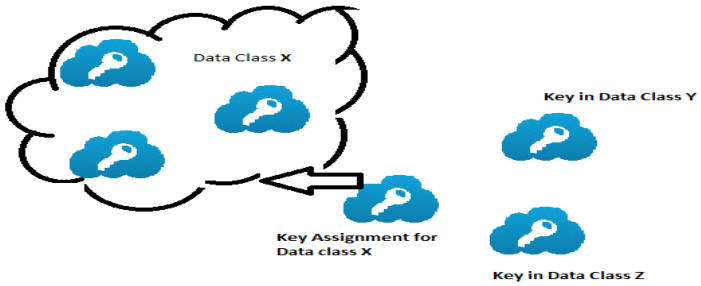


Fig: Architecture for Proposed Model

The encryption schemes and signatures are all same as existing system. Only HKM is addressed in this paper for efficient handling of keys and re-authentication of the clients.

IV. PERFORMANCE VISUALIZATION

The following visualization of graphs indicates the performance measured with the help of this new scheme of managing keys for accessing data classes. The analytics of accessing data classes with less re-authentication as shown in the following graph:

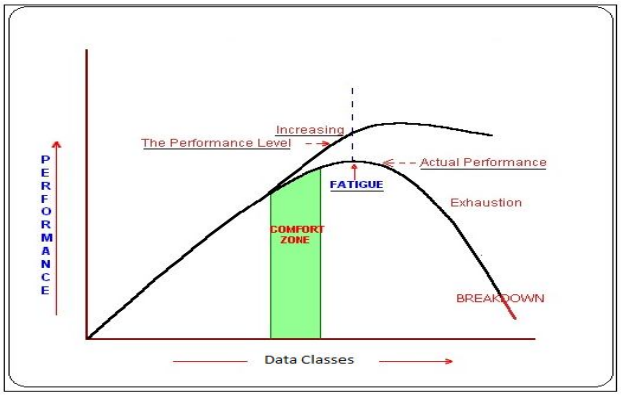


Fig 5.0 Performance Visualization

V. CONCLUSION

In this paper, HKM is introduced for ease of managing problems of handover of key while accessing the different cloud data classes in re-authentication. This proposed scheme helps the client to access the different data classes easily with less time and more security.

REFERENCES

[1] Mr. P.Dileep Kumar Reddy , Dr. R. Praveen Sam, Dr. C. Shoba Bindu, "A Tripartite Partite Key Assignment Scheme For Security Of Cloud Dataclasses", Journal of Theoretical and Applied Information Technology, 15 th July 2017. Vol.95. No 13.

[2] WassimItani; AymanKayssi; Ali Chehab "Privacy as a Service: Privacy- Aware Data Storage and Processing in CloudComputing Architectures", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Pages: 711 & 716, DOI: 10.1109/DASC.2009.139.

[3] Md. Rafiqul Islam; Mansura Habiba, "Agent based frame work for providing security to data storage in cloud" 2012 15th International Conference on Computer and Information Technology (ICCIT), Pages: 446 451, DOI: 10.1109/ICCITechn.2012.6509712

[4] Sandeep K. Sood , "A combined approach to ensure data security in cloud computing', ELSIVER, Journal of Network and Computer Applications, Volume 35, Issue 6, November 2012, Pages 1831–1838.

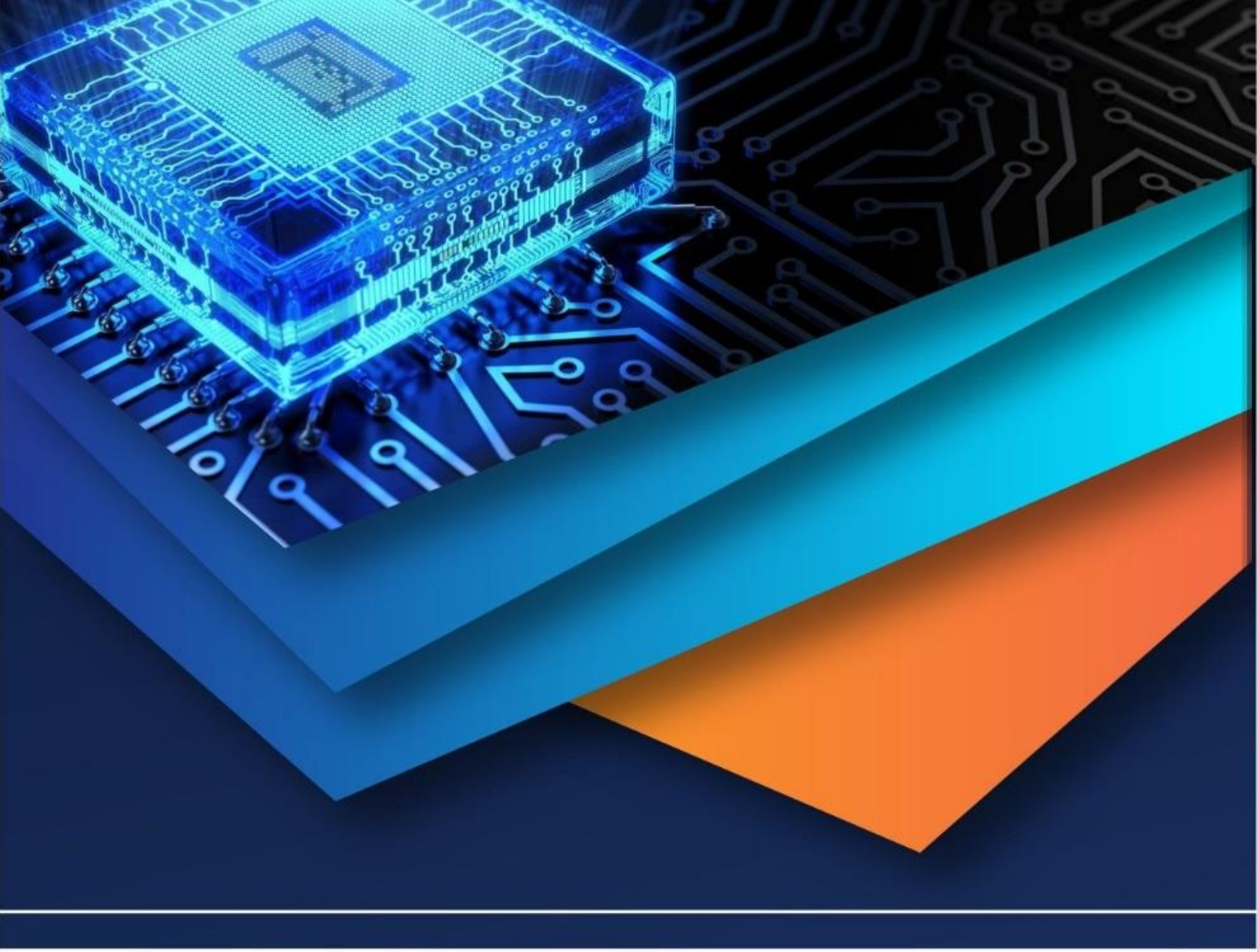
[5] LeinHarn ∗ , Hung-Yu Lin "A cryptographic key generation scheme for multilevel data security", ELSIVER, Computers & Security, Volume 9, Issue 6, October 1990, Pages 539-546.\DongyangXu; FengyingLuo; Lin Gao; Zhi Tangfine grained document sharing using attribute- based encryption in cloudservers" Third International Conference on Innovative Computing Technology (INTECH 2013), pages: 65 - 70, DOI: 10.1109/INTECH.2013.6653703

[6] Yi-Ruei Chen, CHU Cheng-Kang, Wen- GueyTzeng, Zhou Jianying " CloudHKA: A Cryptographic Approach for Hierarchical Access Control in Cloud Computing", International Conference on Applied Cryptography and Network Security (ACNS), 26 Jun 2013

[7] Ran Yang; Chuang Lin; Yixin JiangEnforcing scalable and dynamic hierarc hical access control in cloud computing, 2012 IEEE International Conference on Communications (ICC), Pages: 923 - 927, DOI: 10.1109/ICC.2012.6364473

[8] Jin Li; Xiaofeng Chen; Mingqiang Li; Jingwei Li; Patrick P. C. Lee; Wenjing Lou, secure Deduplication with Efficient and Reli able Convergent Key Management IEEE Transactions on Parallel and Distributed Systems,Year: 2014, Volume: 25, Issue: 6,Pages: 1615 1625, DOI: 10.1109/TPDS.201 3.284

[9] WenGueyTzeny "A time bound cryptographic key assignment service for access control in a hierarchical", IEEE transaction on knowledge Data engineers, Vol 14 No1 , Jan/ Feb 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY