SECURITY INCURSION AND CRYPTOGRAPHY QUICK FIX FOR DATA ACCUMULATED IN CLOUD STORAGE

[1] K.Ketzial Jebaseeli, [2] Dr.V.G.Rani
[1]Research Scholar, [2]Associate Professor
[1]Department of Computer Science
[1,2]Sri Ramakrishna college of Arts and science for women, Coimbatore, Tamil Nadu, India

***Abstract*: **Cloud computing dictate the IT business in Modern years. It furnishes many favors to the people who are not having adequate gauge footing for computing trade. Computational capabilities are contributed in virtualized aspects. Numerous datacenters are allotted for organizing and preserving the end users' data. Various Data centers are established in distant terrestrial point in the world. Cloud service provider is composed and manages the data center of the cloud where users' data are stored. Some specimens of cloud service providers are IBM, Amazon, Google applications etc. User doesn't have any authority or immunity on their data occupied in the cloud not even knows the region of the data in the cloud. This outlook of the cloud brings many security affiliated issues on the data depot in the cloud. The huge dispute in the cloud is Security. Cloud data are outbreak by abettor or stranger in distinctive methods. This paper characterized the various descriptions of attacks on cloud data. It also states cryptography quick fix method to assure the data from different incursion. Security is approached by various criterions like validation, authorization, confidentiality and integrity.

Keywords -Cloud computing, Attacks, Cloud storage, Cryptography

I. INTRODUCTION

Cloud computing affords envision resources to the end-users where application software or server functioning in the cloud server so the end-users can access the software in their regional machine. The resources are allocated to the users depend on their need. The major leverage of the cloud is to provide large virtual accumulation to the user [1].Cloud handles the storage space in a wise manner. It gives volume of virtual area to store the data. The data can be accessible by the user at anyplace in any number of times. Cloud lessens the cost of hardware backing, technical adepts and privilege of database. It provides platform to the small-scale and intermediate endeavors to begin their business [2]. Though, Cloud has many detriments by virtue of security. The organizations are stumbling to setup their data in the cloud storage as a result of security issues are the major concern in cloud storage [3].Security issues are appeared by the attack which is created by the hackers on the data saved in the cloud storage. Hackers are either powerful bureaucrat from cloud service provider or other end-user of cloud storage. Numerous security schemes are proposed by different analyst. Security constraint is an important part in the usage of cloud storage, because it curbs many of the attacks on data from hackers [4].

II. PHASES OF DATA SECURITY

Cloud is the rapid thriving technology but it acquire security related issues for data preservation, the extant schemes could not dispatch effectively due to the security issues from the cloud service providers [5][6].

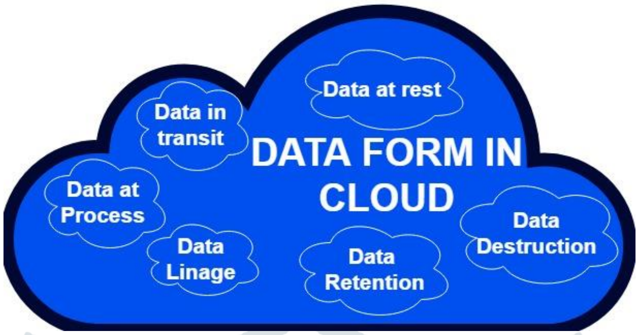

Fig.1

The above given Figure 1 depicts the data in cloud can be in any formation. Data security consists of provocation and ultimately large number of defects and disquietudes yet to be recognized. Data preservation is a critical security issues for the most of the organizations [7].The administration of the data service may not be extensively reliable and the enterprises don't have control over the data by reason of data centers are located faraway. In addition, data are stored in mutitendancy environment. So user data at rest where the data is saved in substantial storage should not be revising. Enciphering the data may be solution for this, but in a grip of PaaS and SaaS models, enciphering of data are consistently not feasible therefore contingency of illegitimate access is very high.[8] Moreover, data must be firm while moving to the server. It must not be viewed or modified by alternative user. Therefore, it requires a suitable encryption algorithm and secure protocols. Certainly, data linage behaves towards maintaining the data source and detention of data in order to prevent from data loss and to persuade the purity of data[9].

III. DATA FORTIFICATION IN CLOUD

Data Fortification in cloud is a key factor, perhaps difficult for the cloud user to accurately examine the action of cloud dealers and as an outcome they are convinced that data is knob in a constitutional way, but it is does not like this dispute is reinforce in case of various conversion of data[10]. Counter measures for this incursion is that an end user of cloud should inspect the establishment and management of data. Faulty data removal is very threat in cloud computing. Actually the data's are not removed because of data replications in other servers. Counter measures for this issues is to allow query to erase the whole data along with its replicas [11].

Cloud data are outbreak by abettor or stranger in distinctive methods. Abettors can be workers, administrator, collaborators who are able to access the entire data with their privilege are called as abettors [12]. Abettor's incursions are prepared by these persons to damage or to displeasure information about the end user or providers and include every kind of incursion which can be run from within.

Strangers are users from exterior to the cloud surroundings they attempt to enter into the cloud to create an incursion [13]. Strangers are interlopers who can criminally come in into the cloud. However, these kinds of incursion are taking place to steal other user's sensitive information in the cloud. Suitable verification mechanism might defend the outsider's attack [14].

IV. CRYPTOGRAPHIC METHODS FOR CLOUD STORAGE

The method of encryptions involve by means of cryptographic algorithms and cryptographic key for converting plain text to cipher text. In the study of Cryptography various methods are used for enciphering and deciphering [15]. These methods can be usually classified into two groups, i.e Symmetric key cryptography and Public key cryptography [16].

Symmetric key cryptography can be called as single key cryptography or conventional cryptography. Single key is used for encryption and decryption. Figure 2 represents the basic model for conventional encryption technique.

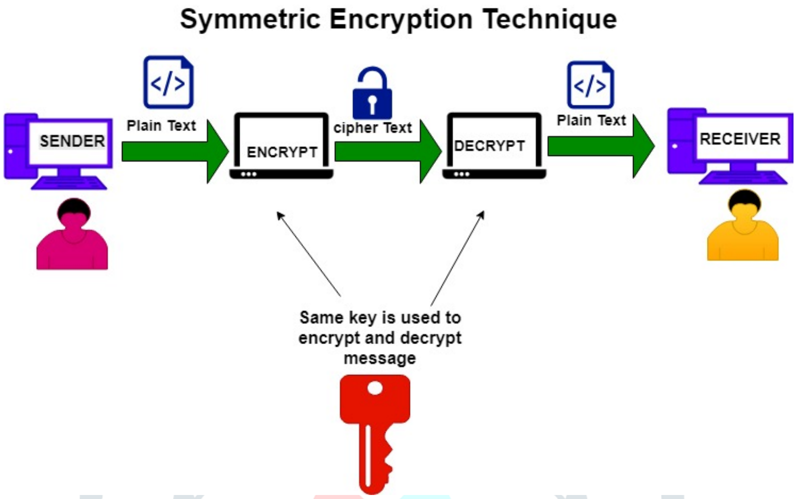
Symmetric Encryption Technique
SENDER
Plain Text
ENCRYPT
cipher Text
DECRYPT
Plain Text
RECEIVER
Same key is used to encrypt and decrypt message

Fig.2

In common, there are two kinds of symmetric cipher, which is stream ciphers and block ciphers. Stream cipher is a single key cipher where original texts are merged with pseudorandom cipher digits stream [17]. In stream cipher every ordinary digit is encrypted one at a time with the equivalent digit of the cipher stream. According to Alfred et al. [18], Real-time applications of stream ciphers are pay TV and DVD content encryption. In Block cipher, the original text is encrypted and decrypted single block at a time.

Public key cryptography can be called as asymmetric key encryption or public key encryption. Here, two keys are used for encryption and decryption. One key can be used for encryption and another key is used for decryption. In this model, sender and receiver must have two keys; public key (which is known) and secret key (which is kept private).Figure 3 represents public key crypto system.

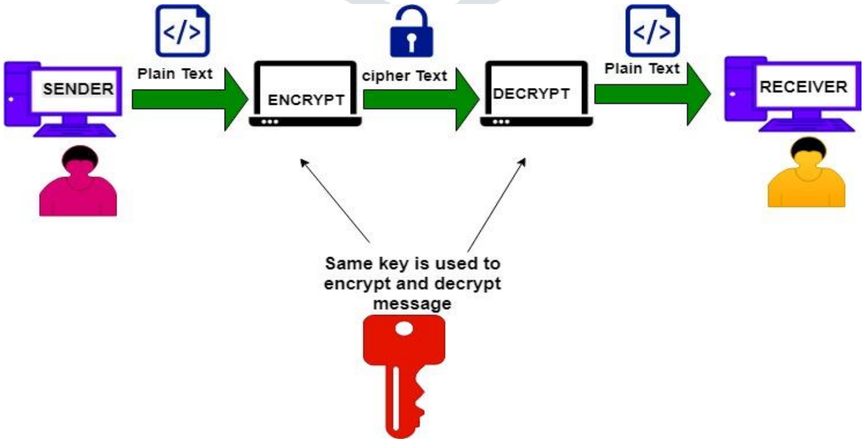

Fig.3

V. TYPES OF INCURSION IN CLOUD COMPUTING

Security of cryptosystem is depends on the key. Cryptographic incursions are intended to undermine the security of cryptographic algorithms and they are used to decrypt the data without access to the key. The following section present different kinds of incursion encountered in cryptography algorithms.

A. Meet-in-the-Middle Attack

The other name of this attack is Known-Plaintext attack. The attacker use two different keys to the original text with various mixture of keys and decrypt the cipher text along with a new set of keys to get the original message.

B. Man in the Middle Attack

This type of incursion occurs when the secure socket layer is not accurately installed when two parties are communicating each other then there is an opportunity for third-party to hack all the data communication among them. Consequently, Counter measures are needed to guard the data from middle man.

C. Brute force Attack

The technique which is implicated in this attack is trial-and-error method used to find information such as a user password or Personal Identification number. Here, computerized software used to generate a huge number of successive guesses to get back the desired data.

D. Dictionary Attack

The word “Dictionary” is mention to the attacker draining all of the word in the dictionary in an attempt to recover the password.

E. Birthday Attack

This attack belongs to the set of brute force attack. It utilizes the mathematics techniques of the birthday problem in probability theorem. A number of permutations are calculated to get the data from the communication.

G. Denial of services

Here, the incursions are created by sending continuous request to the server in order to make server idle. So the server is not able to respond to the normal clients. Counter measures are required to shortlist the privileges of the user that are associated to the server.

H. SQL injection attack

This attack uses SQL malicious code to retrieve the data from database. An intruder uses some special character to revisit the data.

VI. SECURITY PROBLEMS AND RESOLUTION

Security risk is the major concern when end user makes an outsourcing on the cloud. There are numerous security problems concerned in the cloud computing. They are data safety, network protection data locality, data separation, data access etc [19]. Particularly, among these security problems, privacy is the most significant restriction to secure the data in cloud. Privacy for cloud storage ensures providers do not be trained any data about the users.

The biggest concern is to guard the data in data storage from illegal access. In some convention scenarios, the threat of data being disclosed, vanished, tainted, stolen is deplorable when the data control is moved to the resource administrator some counter measures must handle by the cloud providers. To preserve the data in the cloud storage, at present a standard cryptographic methods are applied to the user data in the cloud. Cryptographic methods plays vital role in the data security. The end-user information must be encrypted in trusted surroundings before moving to the untrusted cloud storage. Cryptographic encryptions like symmetric and asymmetric encryption are used to secure the data in the cloud.

VII. CONCLUSION

Cloud affords many benefits to its customers yet it has security issues because of cloud upgradation.Data outsourcing are extensively admired due to computing power of cloud. At the same moment, protection for outsourcing data is a matter for all the cloud users. This paper talks about different incursion on data in the cloud. These incursions are created by abettors or strangers. The incursions created by abettors are difficult to find and rectify. Attacks that are created by outsiders are too identified and to provide some authentication mechanism. Confidentiality is concession due to abettors attack on the cloud. New cryptographic techniques are to address the abettors attack in the cloud. Formerly, these threats are inscribe then cloud users and cloud providers will get more profit from the cloud.

REFERENCES:

[1]. Dr. L. Arockiam, S. Monikandan, G. Parthasarathy "Cloud Computing: A Survey", International Journal of Internet Computing, Volume 1, Issue 2, ISSN: 2231 – 6965, October 2011, pp. 26-33.

[2]. Fatima Trindade Neves, Fernando Cruz Marta, Ana Maria Ramalho Correia and Miguel de Castro Neto, "The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors", Proceedings of International Conference of the Portuguese Association of Information Systems - The Information Management in the age of Cloud Computing, 2011, pp. 1-11.

[3]. John, H., L.M. Kaufman and Bruce, P., "Data Security in the World of Cloud Computing", IEEE Journal of Security & Privacy, Volume 7, Issue 4,2009, pp 61-64.

[4]. Dr. L. Arockiam, S. Monikandan, "Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage",International Journal of Current Engineering and Technology, Vol.4,No.3, E-ISSN 2277 – 4106, P-ISSN 2347 - 5161, June 2014, pp. 1265-1270. (IF-2.552)

[5]. Dr. L. Arockiam, S. Monikandan, "AROMO Security Framework to Enhance Security of Data in Public Cloud", International Journal of Applied Engineering Research, Print ISSN 0973-4562, Online ISSN 1087-1090, Volume 10, Number 9, (Special Issue), 2015, pp. 6740-6746.

[6]. Yau SS, An HG., "Confidentiality Protection in Cloud Computing Systems", International Journal of Software Informatics, Volume 4, Issue 4, 2010, pp. 351-365.

[7]. Raman Chawla and Kirti Nagpal, "Data Security Issues & Requirements in Cloud Computing", International Journal of Computing Science and Communication Technologies, Volume 5, Issue 2, 2013, pp. 883-886.

[8]. Kaur A, Manisha Bhardwaj, "Hybrid Encryption for Cloud Database Security", International Journal of Engineering Science & Advanced Technology, Volume 2, Issue 3, 2012, pp. 737-741.

[9]. Shucheng Yu, Wenjing Lou, and Kui Ren, "Data Security in Cloud Computing", Handbook on Securing Cyber-Physical Critical Infrastructure, Chapter 15, Elsevier, Morgan Kaufmann Publisher, 2012, pp.389-410.

[10]. Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy", O'Reilly Media, Inc, 2009.

[11]. Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo,"Secure Data Sharing in the Cloud", Security, Privacy and Trust in Cloud Systems, Chapter-1: Cloud Security, Springer-Verlag Berlin Heidelberg, 2014, pp. 45-72.

[12]. Dimitrios Zissis and Dimitrios Lekkas, "Addressing Cloud Computing Security Issues", Journal of Future Generation Computer Systems, Elsevier Science, Volume 28, Issue 3, 2012, pp. 583-592.

[13]. Dr. L. Arockiam, S. Monikandan," Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 8, ISSN : 2278-1021, August 2013, pp. 3064-3070.

[14]. Dr. L. Arockiam, S. Monikandan, Dr. P. D. Sheba K Malarchelvi, "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage", International Journal of Computer Applications, Volume 88, Number 1, ISSN: 0975 – 8887, February 2014, pp. 17-21.

[15]. Bleikertz S, Sven Bugiel, Hugo Ideler, Stefan Nurnberger and Ahmad-Reza Sadeghi, "Client-Controlled Cryptography-as-a-Service in the Cloud", Proceedings of International Conference on Applied Cryptography and Network Security, Springer-Verlag Berlin, Heidelberg, 2013, pp. 19-36.

[16]. William Stallings, "Cryptography and Network Security: Principles &Practices", 4th edition, Prentice Hall, ISBN: 978-0-13-187316-2, 2005.

[17]. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstore,"Handbook of Applied Cryptography", CRC Press Inc., 1997.

[18]. Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby, "Data Security Model for Cloud Computing", Proceedings of International Conference on Networks, 2013, pp. 66-74.

[19]. Oktay U. and Sahingoz O.K., "Attack Types and Intrusion Detection Systems in Cloud Computing", Proceedings of International Conference Information Security & Cryptology, 2013, pp. 71-76.