INFORMATION AND NETWORK SECURITY WITH CRYPTOGRAPHY.

Prof. Amruta Harshal Salvi (Master of Computer Application)
Department of Information Technology and Computer Science
S.P.Hegshetye College of Arts Commerce and Science, Ratnagiri, Maharashtra, India

Abstract -Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is an essential part in order to secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Present a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among geographically dispersed physical devices and clients. Also propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, it divides a File into fragments and encrypts this fragment, and replicates the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is get to the attacker. Meter Data Management System will check integrity of stored data and replace the tempered data with original one.

Keywords-Cloud security, Cipher text-policy attribute-based encryption, circuits, fragmentation, and replication.

I. INTRODUCTION

1.1 Background

Cloud-assisted cyber-physical systems (Cloud-CPSs; also known as cyber-physical cloud systems) have broad applications, ranging from healthcare to smart electricity grid to smart cities to battlefields to military, and so on . In such systems, client devices (e.g., Android and iOS devices, or resource constrained devices such as sensors) can be used to access the relevant services (e.g., in the context of a smart electricity grid, it may include utility usage data analyzed and stored in the cloud) from/via the cloud. However, client devices generally have less computing capabilities and hence, are unlikely to have adequate security (technical) measures in comparison to the conventional personal computers (PCs).From the existing work survey, we can deduce that both security and performance are critical for the next generation large-scale systems, such as clouds. Therefore, in this project, we collectively approach the issue of security and performance as a secure data replication problem. We present Division and Replication of Data in the Cloud for Optimal Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the T-coloring.

1.2 Motivation

The increasing volumes of medical images and medical records, the healthcare organizations put a large amount of data in the cloud for reducing data storage costs and supporting medical cooperation. Since the cloud server may not be credible, the file cryptographic storage is an effective method to prevent private data from being stolen or tampered. Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security is main aspect to protect all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

Network security can be divided mainly into four closely associated areas: authentication, secrecy, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized

users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the check summing techniques that we encountered in reliable transport and data link protocols. Cryptography is an emerging technology, which is important for network security. The widespread use of computerized data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorized access while in storage or transmission. Due to continuing advancements in communications and eavesdropping technologies, business organisations and private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques, which , until very recently, were exclusively used by the military and diplomatic communities. Cryptography is a vital of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages. Computer systems and networks which are storing, processing and communicating sensitive or valuable information require protection against such unauthorized access[1].

1.3 Basic Terminology of Cryptography

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc.. Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing. The information that we need to hide, is called plaintext , It's the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message in the sender before encryption, or it is the text at the receiver after decryption.
The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text.

Cipher is the algorithm that is used to transform plaintext to cipher text, This method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data. The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program.

II. LITERATURE SURVEY

1.Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei DaiConcluded "CHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability"in which going to use concept of cost efficient cloud selection from this paper. We are also referring Heuristic Data placement algorithm for cloud selection. Cloud data storage redefines the protection issues under attack on customer's outsourced data. From a customer's end of vision relying upon a solo Service Provider for his retrieved data is not confident. In this project, a novel information hosting scheme (named CHARM) which integrate two key functions desired. The first is selecting several suitable clouds and a proper redundancy plan to store data with minimized financial cost and certain ease of use [10].

2.Jun Feng, Yu Chen, Wei-Shinn Ku, Zhou SuConcluded "D-DOG: Securing Sensitive Data in Distributed Storage Space by Data Division and Out-of-order keystream Generation"in whichThe concept of fragmentation and encryption at user side is referred from this paper. This technique provides security at host level, at network level and at cloud server [6].

3.Mazhar Ali, Student Member Concluded DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security in which Concept of T-coloring graph for fragment placement as well as algorithm for fragment placement has been referred from this paper. When fragments are lost with help of replica it can cover [7].

4. J. Han, W. Susilo, Y. Mu, and J. Yan Concluded "Privacy-preserving decentralized key-policy attribute-based Encryption," in which Before storing the data on the cloud

server, the data can be encrypted. Attribute- based encryption technique is a public key encryption which enables access control over encrypted data using different access policies and ascribed attributes. Personal health record (PHR) is an emerging health information exchange model, which is always out sourced to be stored on third party, such as cloud server. Before storing the Personal Health Information of Patients and Doctors the attribute based encryption is applied. A public auditing scheme is used which audits the tampered data on the cloud server. This scheme can totally releases the burden of PHR users about storing and maintaining their data on cloud server [2].

5.JunbeomHur and Dong Kun NohConcluded" Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems" in which Cipher text-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. In this paper, we propose an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control achieved by mechanismof dual encryption which takes use of the ABE and selective group key distribution in each attribute group. We demonstrate how to apply the proposed mechanism to securely manage the outsourced data [1].

6. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang Concluded "Securely outsourcing attribute-based encryption with checkability," in which We proposes an outsourced ABE construction that provides checking ability of the outsourced computational results in an efficient way. Extensive security and performance analysis show that the proposed schemes are proven secure and practical [3].

7.R. Cramer and V. Shoup,concluded "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in which A new public key cryptosystem is proposed and analyzed. This scheme is practical, and can prove secure against cipher text attack under standard intractability assumptions [5].

III. PROPOSED APPROACH

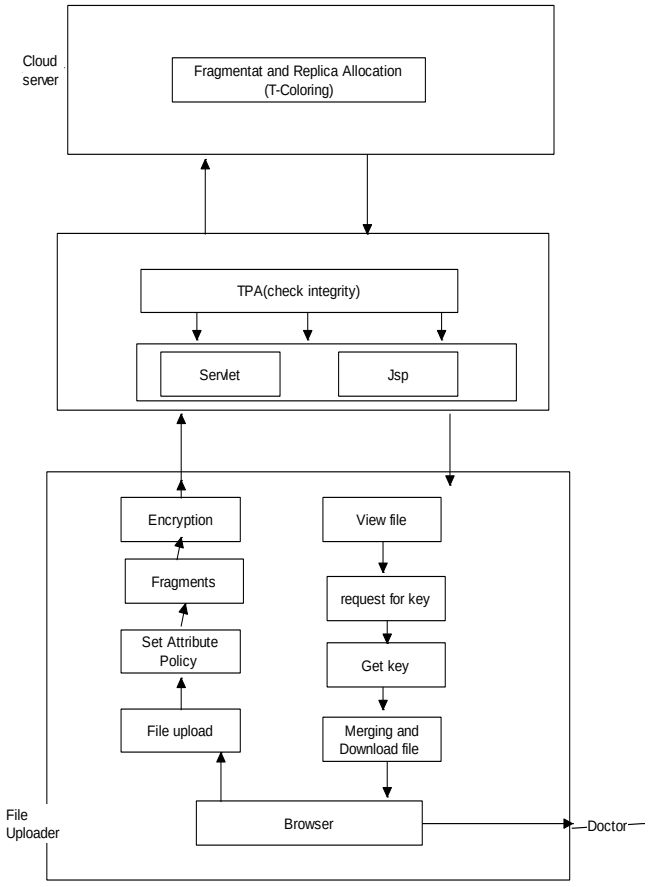

Fig 01: System Architecture

System Overview-

In proposed system Hospital Receptionist will fill patient information and then that patient will allocate to Doctors according to doctors position location and experience. Hospital's patient distributor will assign the patients to doctor by generating access policies considering doctors attribute location and experience after entering encryption key then file will fragment and store with fragment and its replica. When Authenticated doctor login then he will get the file with which his policy attribute matches. Then he can request for the file key and download the file after entering secrete key. Third party auditor will check data integrity of stored fragment that means placed fragment content is changed or not if changed then TPA will inform to admin head about that file. TPA will then replace tempered fragment with original fragment and provide integrity. Integrity will check by hash value of available data on each node.

Head Admin: Admin of hospital will add patient's details and assign that patient to particular doctor by assigning attributes that is specialist and experience and location .He upload the files on cloud. File will fragment and encrypt and stored by t-coloring.

Doctor: Doctor will login to system and he will get the file matching to his attribute according to specialist and experience and location. Then he will send request to head admin then head admin will send key on Doctors mail Id. Then doctor will enter key and get file.

Admin: Admin view user details, file details and fragment location also replica location.

Third Party Auditor: TPA stands for Third Party Auditor. Who conducts public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers .He check fragments and replicas integrity stored on cloud.

IV. ALGORITHM

Algorithm 1:Fragmentation

1. Upload file

2. Enter no. of fragments.i.e. Nof= no.of fragments

3. Check file size of source file

4. Fragments=size/Nof

5.End

Algorithm 2:AES Algorithm For Encryption.

AES(advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algorithm is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input(0,1)

secret key(128_bit)+plain text(128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round:10,12,14

Each round consists:sub byte, shift byte, mix columns, add round key.

Output:

Ciphertext (128 bit)

V. EXPERIMENTAL SETUP

For proposed system jdk 7 used and IDE is Eclipse Luna.Server is Apche tomcat 7 .The cloud used is Amazon EC2.The fragmented block will store on cloud.It uses T-coloring to place the fragment.

Graph-

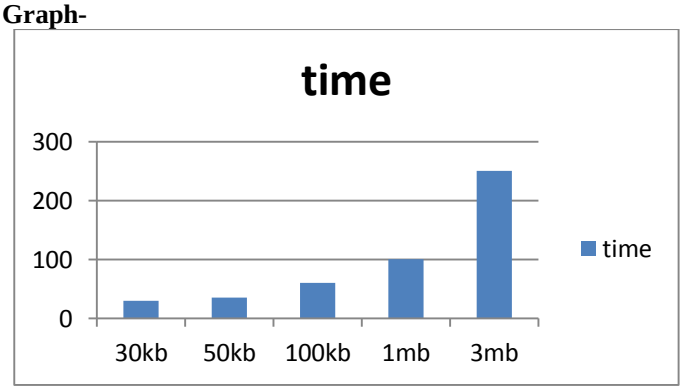

Fig.02 Shows file size on x axis and time (ms)to upload on Y-axis

Explanation: Graph shows size of file and time to upload that file after performing fragment and t-coloring .As size of file increases the time will increase.

Table:

ID	File size	Time to upload (ms)
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Table 01:Time to upload file

Above table 01 gives the information of uploading time for 30kb, 50kb, 100kb, 1mb and 3mb file size.

VI. CONCLUSION

Network Security is the most significant component in information security as it is important and needed for securing all information passed through computers in network. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. In this proposed methodology, a cloud storage security scheme that collectively deals with the security and performance. We firstly present a circuit cipher text-policy attribute-based encryption .The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file. The performance of the proposed methodology was compared with full-scale replication techniques. The system will perform auditing for stored data on cloud.

VII. REFERENCES

[1]. JunbeomHur and Dong Kun Noh," Attribute-Based Access Control with EfficientRevocation in Data Outsourcing Systems", VOL. 22, NO.7, JULY 2011 IEEE.

[2]. J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. ParallelDistrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[3]. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.

[4]. K. Kurosawa and Y. Desmedt, "A new paradigm of hybrid encryption scheme," in Proc. 24th Int. Cryptol. Conf., 2004, pp. 426–442.

[5]. R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," inProc.18th Int. Cryptol. Conf., 1998, pp. 13–25.

[6]. Jun Feng, Yu Chen, Wei-Shinn Ku, Zhou Su ,D-DOG: Securing Sensitive Data in Distributed Storage Space by Data Division and Out-of-order keystream Generation.2010

[7]. Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, BharadwajVeeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, andAlbert Y. Zomaya, Fellow, IEEE,DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security.2015

[8]. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian.Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage. May 2015

[9]. ShristiSharma,ShreyaJaiswal,PriyankaSharma,Prof. Deepshikha Patel, Prof. SwetaGupta.An Approach For File Splitting And Merging.

[10]. Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and YafeiDaiCHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability .2015

[11]. L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[12]. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451. .