SECURING CLOUD DATA USING CRYPTOGRAPHY

[1] M.Janaki, [2]Dr.M.Ganaga Durga

[1]Research Scholar, Bharathiar University,

Assistant Professor, Dr.Umayal Ramanathan College for Women, Karaikudi, Tamilnadu, (India)

[2]Research Supervisor, Bharathiar University,

Assistant Professor, Government Arts College for Women, Sivaganga, Tamilnadu, (India)

ABSTRACT

Cloud Computing provides services at either free of cost or low cost to the small and medium business enterprises. Although it gives more advantages to the user, the security issues is a barrier for the cloud usage. More and more researches is needed in this area to develop true security solutions which will solve the problem of security issues. The main security problem is ensuring data confidentiality of data at rest or data during transfer in the cloud. The privacy of communications between the sender is very important which can be provided with disassembling the data before transmission. This paper summarizes the various security issues in the cloud and describes the possible solutions to overcome the problems. Cryptography is justified as a better solution for obtaining data confidentiality in this paper.

Keywords: Cloud Computing, Security Issues, Data Confidentiality, Cryptography, Substitution Cipher

I. INTRODUCTION

Computing becomes a model that consists of services delivered in manner similar to traditional utilities such as water, electricity, gas and telephony such services are accessed by the users based on their need by ignoring where the services are hosted are how they are delivered. Cloud computing is such an paradigm that delivers utility computing and enable the users to accesses the application from anywhere in the world. The cloud offers several benefits like fast pay for use, scalability, data storage solutions, lower cost , and rapid elasticity[1]. Though the cloud offers several advantages still there are some risks that makes it unreliable. Cloud computing moves the user data to the large data centers, where the management of data and services are not to truth worthy. The security challenges posses by the cloud or data confidentiality, data interigity, data loss and theft identity management and issues related to authentication[2] . Though cloud computing provides better resource utilization using virtualization techniques and which reduces much of the work load from the user, it is fraught with security risks. To address the problem, in this paper we explore a solution based on cryptography. Cryptography is the art of secret writing which enables as to hide the sensitive data in the cloud. Hence the confidential data should be encrypted before storing it in the cloud and it can be decrypted during the retrieval[4].

1.1 Related Work

Yanpei Chen, Vern Paxson, Randy H. Katz have explored the new issues that affects the cloud computing security and argued mutual audibility between providers and users will provide a better solution to make cloud

reliable. Hyokyung Chang and Euiin Choi have discuss above the challengers security in cloud computing and suggest encryption technology will be suitable for overcoming cloud security issues. Jianhua Che , Yamin Duan, Tao Zhang, Jie Fan have a made a study on security models and strategies of cloud computing and survived the popular security models available along with the advantages and disadvantages. Liang Yan, Chumming Rong, and Gansen Zhao have adopted a new techniques based on identity based cryptography which provides data security.

II. CLOUD COMPUTING

The term " Cloud was coined from the computer network diagrams which is used to hide the a complexity of the infrastructure involved cloud computing is an internet based delivery model which provides a services, computing and storage for the users in all their areas including financial health care and government. There are five main characteristics makes the cloud computing model as a better technology[3]. The first characteristics of the cloud computing is On-demand self-services without long delays. The second characteristics is Broad network access via standard platforms such desktop, laptop, mobile etc. The Third characteristics resource pooling across multiple customers . The fourth one is rapid elasticity which meets the maximum demand . And last one is the measured service that is pay per use.

2.1 Deployment Models

Cloud can be deployed into three categories such as public cloud, private cloud and hybrid cloud. The public cloud is a general cloud in which a service provider makes a resources such as applications and storages available to a general public over the internet. The main advantages of using a public cloud services are maximum scalability and minimum cost[6]. The disadvantage of using public cloud is the security risks which makes it unreliable. So storing sensitive information in the pubic cloud should be avoided. The private a cloud is the personal cloud created a and operated by single organization. The advantage is its reliability since the uses belongs to the single organization. The disadvantage is minimum scalability which can serve only for limited customers and expensive. A hybrid cloud will combine several private clouds and public clouds to share data. It enjoys the combined advantages both private and public clouds but very hard to make it reliable[8]. Maintaining data confidentiality and controlling the access requires additional techniques.

2.2 Delivery Models

Cloud computing utilizes the three delivery models by which different type of services or delivered to the end user. The three delivery models are Software as a Service(SaaS) , Platform as a Service (PaaS), Infrastructure as a Service (IaaS)[7]. SaaS is a software deployment model where application are remotely posted by the service provider and made available to the users on demand over the internet. This models offers improved operational efficiency and reduced cost The challenges faced by SaaS is customers concerned about data security because vulnerability in the applications will lead to loss of sensitive data and money. IaaS is a infrastructure deployment model which provides hardware resources such as Virtual servers and allows to pay only for the resources used. The small business organizations need not invest heavy amount to upgrade hardware resources since IaaS offers this in affordable cost. IaaS provides basic level security but it requires higher level of security[9]. PaaS is a platform deployment model which offers integrated set of developer environment which includes Os and Middle ware. This model abstracts a everything away from the view of

developers and provides a complete software development life cycle management from planning design, building application, testing to maintenance. The dark side of PaaS is its advantages itself can be helpful for a hackers to go behind IaaS application.

III. SECUCRITY ISSUES IN CLOUD COMPUTING

Usually users depend on cloud providers for the security measures. The cloud service providers should protect one users data from other users. The following a key elements should be carefully consider before application development and deployment process during the cloud usage. The security issues are Data security , Network Security , Data locality, Data integrity, Data segregation, Data access , Authentication and Authorization , Data confidentiality , Backup and Identity Management[10] .

The cloud service provider must adopt additional security checks to ensure data security through the use of strong encryption techniques and fine-grained authorization to control access of data. All data flow over the network has to be secured to prevent leakage of sensitive information, which can be achieved using strong network traffic encryption techniques[11]. Consumers use the application provided by the cloud and process their business data. But they don't know where the data is getting stored due to data privacy loss a various country locality of stored data becomes an issue hence service provider must be able to provide exact location of data of the customer. Data integrity is easily achieved in a standard alone system using data base constraints and transaction. In order to maintain data integrity in a distributed system a Central Global transaction manager can be used. Each application in the distributed system should participate in the global transaction through a resource manager. Multiple users can be stored their data using applications provided by SaaS, which makes data of various users to reside at the same location. Actually this allows intrusion of data of one user by another user through hacking[13]. Hence a boundary must be fixed for each users data and segregating data of different users is archived. Most of the small and medium business company are storing their employee information in some Lightweight Directory Access Protocol (LDAP) Servers Each organization have its own security policy to denote who among the employees have access to a particular set of data the SaaS model must be flexible to accept a policies given by the organization the SaaS customers must be remembered to disable accounts as employees leave the company and enable the accounts as come on board[12]. Cloud computing involves the sharing or storage of personal information buy the users on remote servers operated by service providers the confidentiality of personal and sensitive information is a serious issue that must be taken care. All sensitive data enterprise data is regularly backed up for quick recovery in case of dishausted strong encrypt schemes can be used to protect the backup data from accidental leakage of sensitive information Identity management deals with controlling the users access to the resources through the established identities

IV. CRYPTOGRAPHY

Encryption is a method of hiding data so that it cannot be read by anyone who does not know the key. The key is used to lock and unlock data. To encrypt a data one would perform some mathematical functions on the data and the result of these functions would produce some output that makes the data look like garbage to anyone who doesn't know how to reverse the operations [14]. Encryption can be used to encrypt files that the owner feels are too sensitive for anyone else to read. Private Key means that the same method is used to encrypt and decrypt. If someone knows what method was used to encrypt the message then that person can decrypt the

message. Private Key encryption has the benefits of being very fast. A disadvantage to private key cryptography is that the key must be communicated beforehand. Public key cryptography is also known as asymmetric cryptography which was created to eliminate the shortcomings of private key cryptography [15]. The biggest advantage of public key cryptography is that no prior communication needs to take place between the recipient and the sender. Public key cryptography works like this, everyone has two keys, a public key, which the entire world has access to, and a private key, which only the owner knows.

Polyalphabetic cipher was first used by Leon Battista Alberti. He used the substitution method of shifting multiple alphabets for a single alphabets later Johannes Trithemius have invented the tabula recta and Trithemius cipher in his work polygraphia. Using of a separate key was introduced by Glovan Batlista Bellaso. He has added a repeated "Counter Sign Key" known as a key for more security. Blasie de vigenere have created a method called viginer cipher which is auto key cipher along with the table generated with 26 alphabets. The table contains 26 X 26 rows and columns with shifted alphabets from A to Z. Francis Beaufort has found reciprocal cipher with a small modification of vigenere cipher. Along with the alphabets the 10 numerals from 0 to 9 are added in the table by Gronsfeld and its known as Gronsfeld cipher. One of the most important assumptions in modern cryptography is Kerckhoff's Principle. In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used. This principle was enunciated by Auguste Kerckchoffs in 1883 in his classic teatise "La Cryptographic Militaire". The enemy can obtain this information in many ways such as encipher/decipher machines can be captured and analyzed. The security of the system should therefore be based on the key and not on the obscurity of the algorithm used.

V. DISCUSSION

The security risks in the cloud is lessoning its usage, hence a solution to be found to make it reliable. Several researches are going on to overcome the challenges in cloud computing. Usage of cloud computing seems to be more helpful to several small and medium business enterprises. Let us tabulate the opportunities and challenges faced by cloud deployment models in Table 1.

Table 1. Cloud Deployment Model Opportunities and Challenges

Deployment Model	Opportunities	Challenges
Public Cloud	Less expensive	Dos Attacks
	High Scalability	Attacks on Virtual Machine
	Easy Setup	Placing Malicious Code
Private Cloud	Reliable	More Expensive
	Improved Efficiency	Low Scalability
	Access Control	Hard Setup
Hybrid Cloud	High Scalability	Risk of Multiple cloud Tenants
	Cost Effective	Access Control
	Hide Architecture detail	Identity Management

The above table gives a thorough understanding about the advantages and disadvantages of public, private and hybrid clouds. Cost effectiveness and scalability are the maximum opportunities in the cloud, which also brings

the cloud attacks. The same can be obtained for the SaaS, PaaS and IaaS. The opputunities and challenges of cloud delivery models are tabulated in Table 2.

Table 2 Cloud Delivery Model Opportunities and Challenges

Delivery Models	Services	Providers	Opportunities	Challenges
SaaS	Software	Sales Forces	Improved Efficiency and Reduced Cost	Loss of Sensitive data and money
PaaS	OS, Middle Ware, Storage	Google	Upgrading hardware without heavy investment	Requires higher level security
IaaS	Hardware, Servers	Amazon Web Services	Abstraction of architecture details	Easy Hacking

The above table summarizes the available opportunities to use and corresponding threats to be taken in to account so that user can safeguard their sensitive information from the cloud attacks. Though the service providers will provide the security concerns to some extent, it is user's responsibility to encapsulate their data travelling through the cloud.

The ten important security issues are tabulated in the Table 3. along with the possible security solutions. This table can give a better idea for the cloud user to choose the remedy for protecting their confidential data form the malicious third party.

Table 3 Security Solutions

Security Issues	Solutions
Data security	Strong Encryption Algorithms Fine-grained authorization for Access Control
Network Security	Strong Network traffic encryption techniques
Data locality	Capability to provide location of the user data
Data integrity	Central Global transaction manager Service level agreement Different levels of availability
Data segregation	Ensure Clear Boundary for each user's data
Data access	Providers Incorporate organization policy
Authentication and Authorization	Customer should remember employee accounts
Data confidentiality	Providers terms of serviced policy Examination of users records for evidence for criminal activity
Backup	Strong Encryption techniques
Identity Management	Access control based on identities

The above security problems usually happens in the cloud storage, either when the data is at rest or when the data travels through the cloud. Taking the remedial action is important otherwise confidential data will be hacked by unauthorized users. The table also describes the required solutions to resolve the security issues.

Guaranteed service provider policies, Strong encryption techniques, Identity based access controls will be the best solutions for sealing data in the cloud.

VI. NEW DIRECTIONS

Ultimate goal is to find the approach to share sensitive data across the cloud by preserving data confidentiality. For this we can use a cryptographic technique to provide a data security on data storage. The new approach is named as CloudSec which concentrates on protecting sensitive data through encryption before storing at in the cloud and perform decryption to retain the original data during retrieval. The steps involved in this approach are,

1. To develop a system that will provide security to cloud storage
2. To establish an encryption techniques for disguising the sensitive data on the cloud
3. To develop the encryption technique for retrieving the original sensitive information from the cloud
4. To generate and manage the keys used for encryption and decryption efficiently
5. To check authentication of users before allowing for encryption or decryption

VII. CONCLUSION

For cloud computing a security issues, the fundamental challenge is securing the sensitive data. A better solution for securing confidential data is using strong encryption techniques. Several encryption algorithm either symmetric or asymmetric is available today. From which algorithm can be chosen individually, two or more algorithms can be combined, a new encryption algorithm can be created, existing algorithm can be revised. Not only the encryption algorithms is important, key generation and management is also to be done efficiently for successful results. Once a better cryptography approach along with good key management concepts is created then cloud computing can be utilized effectively without any security fraught.

REFERENCES

[1] Deyan Chen, Hong Zhao ―Data Security and Privacy Protection Issues in Cloud Computing‖ 2012 International Conference on Computer Science and Electronics Engineering. 978-0-7695-4647-6/12 $26.00 © 2012 IEEE. DOI 10.1109/ICCSEE.2012.193.

[2] Hatim Mohamad Tahir, Tamer N. N. Madi, Mohd Zabidin Husin, Nurnasran Puteh, ―RSA ALGORITHM PERFORMANCE IN SHORT MESSAGING SYSTEM EXCHANGE ENVIRONMENT‖ Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI, 2011,8-9 June, 2011 Bandung, Indonesia.

[3] Peter Mell, Timothy Grance, ―The NIST Definition of Cloud Computing (Draft)‖, Special Publication 800-145 (Draft). Recommendations of the National Institute of Standards and Technology. U.S. Department of commerce. January 2011.

[4] Guojun Wang, Qin Liu, Jie Wu, Minyi Guo, ―Hierarchical attributebased encryption and scalable user revocation for sharing data in cloud servers‖, 2011 Elsevier, doi:10.1016/j.cose.2011.05.006.

[5] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.07.006.

[6] Qi Zhang , Lu Cheng, Raouf Boutaba ―Cloud computing: state-ofthe-art and research challenges‖ J Internet Serv Appl (2010) 1: 7–18. DOI 10.1007/s13174-010-0007-6 © The Brazilian Computer Society 2010, Springer.

[7] Jian wang, Yan zaoh, Jiajin le ―Providing Privacy Preserving in Cloud Computing‖, 978-1-4244-7562-9/10/$26.00 ©2010 IEEE.

[8] Anu Gopalakrishnan, ―Cloud Computing Identity Management‖ SETLabs Briefings VOL 7 NO 7 2009.

[9] Liang Yan, Chunming Rong, Gansen Zhao, ―Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography, CloudCom 2009, LNCS 5931, pp. 167–177, 2009. © Springer-Verlag Berlin Heidelberg 2009.

[10] Nadeem A, Javed M Y, ―A Performance Comparison of Data Encryption Algorithms‖, Information and Communication Technologies, ICICT 2005.

[11] Vipul Gupta, Sumit Gupta, Sheueling Chang, Douglas Stebila, ―Performance Analysis of Elliptic Curve Cryptography for SSL‖, WiSe'02, September 28, 2002, Atlanta, Georgia, USA. Copyright 2002 ACM 1-58113-585-8/02/0009.

[12] Dan Boneh, Matthew Franklin, ―Identity-Based Encryption from the Weil Pairing‖, Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. An extended abstract of this paper appears in the Proceedings of Crypto 2001, volume 2139 of Lecture Notes in Computer Science, pages 213{229, Springer-Verlag, 2001.

[13] Patrick J.Flinn and James M.Jordan, ―Using the RSA Algorithm for Encryption and Digital Signatures: Can you encrypt, Decrypt, Sign and Verify without infringing the RSA patent?‖, ©1997 Alston and Bird LLP.

[14] Cetin Kaya Koc, Tolga Acar, Burton S. Kaliski Jr., ―Analyzing and Comparing Montgomery Multiplication Algorithms‖, IEEE Micro, 16(3):26-33, June 1996.

[15] Stefano Tessaro1, David A. Wilson, ―Bounded-Collusion IdentityBased Encryption from Semantically-Secure Public-Key Encryption: Generic Constructions with Short Ciphertexts‖ An extended abstract of this paper appears in the proceedings of PKC 2014. This is the full version. Work done while the author was a research scientist at MIT CSAIL.