www.ijarcsse.com

Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Cloud Computing: Security Challenges & Encryption Practices

Dr.A.Padmapriya, M.C.A., M.Phil., Ph.D
Department of Computer science and Engineering,
Alagappa University, Karaikudi, INDIA

P.Subhasri, (M.Phil, Research Scholar) *
Department of Computer science and Engineering,
Alagappa University, Karaikudi, INDIA.

*Abstract— **Cloud computing is a new era of the modern world. Reasons for development of cloud computing are different people and different purpose depends upon the demand. The improvement of the cloud technology also increases the security issues twice. So we need to solve the security issues in the cloud technology. In this paper, we have discussed about cloud computing security mechanisms and presented the comparative study of several algorithms. In future we are going to propose a new plan to solve security issues for both cloud providers and cloud users.***

Keywords— Cloud, Security, Encryption algorithms, Security issues

I. INTRODUCTION

Cloud is a broad solution that delivers IT as a service. Cloud computing is an internet based technology uses the internet & central remote servers to support data and applications. It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access. Cloud computing also provided shared resources like electricity distributed on the electrical grid. Before cloud computing, websites and server based applications were executed on a specific system. The cloud computing flexibility is a function of the allocation of resources on authority's request. And the cloud computing provides the act of uniting.

A cloud is a large pool [1], of easily and accessible virtualized resources, such as hardware, development platforms and/or services. These resources can be powerfully re-configured to arrange properly to a variable load scale, and also permitting for an optimum resource use. This pool of resources is constituting a type exploited by a pay-per-use model in which guarantees are hold out for acceptance by the infrastructure supply by means of usage Service-Level Agreements(SLA). In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the remote server at some other place.

A cloud is a pattern of parallel and distributed system be composed of a collection of interconnected and virtualized computers that are dynamically stipulation and presented as one or more unite computing resources established on service level agreements found amongst negotiation between the service supplier and consumer. It uses remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way.

The concept of cloud computing is linked closely with those of Information as a service (IaaS), Platform as a service (PaaS), Software as service (SaaS) all of which means a service-oriented architecture. Here comes the first benefit of the cloud computing i.e. it reduces cost of hardware that could have been used at user end. As there is no need to store data at user's end because it is already at some other location. So instead of buying the whole infrastructure required to run the processes and save bulk of data you are just renting the assets according to your requirement. The similar idea is behind all cloud networks [2].

II. SECURITY ISSUES IN CLOUD COMPUTING

A. Security Issues:

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user [3] can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud.

This leads to affects many customers who are sharing the infected cloud. There are five types of issues [4] raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues

1. Data Issues:

Whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data.

Data stealing is a one of serious issue [15] in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server.

Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire.

Solution: "*Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behavior of the cloud supplier and as a result he is confident that data is handled. Also very efficient data integrity method [13] in cloud computing."*

2. Privacy Issues*:*

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

Solution: *"Authentication [7] is a best solution for the privacy issue. Authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet."*

3. Infected Application:

Any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

Solution: *"To prevent [8] cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server."*

4. Security issues:

Cloud computing security must be done on two levels. One is on provider level and another is on user level. The user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action.

Solution: *"Cloud computing service provider should make sure that the server is well secured [17] from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user. A cloud is good only when there is a good security provided by the service provider to the user."*

5. Trust Issues:

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. So the vendor uses this marvelous application should make trust. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

B. Cloud Services:

Cloud computing provides different services rather than a unit of product. The basic six types[6] of the services are as follows,

Web based cloud services: These services exploit certain web service functionality, rather than using fully developed applications. (i.e.) it includes an application programming interchange for Google maps, and also the payroll or credit card processing.

Saas (software as a service): It is one of the ideas to providing a given application to multiple tenants, typically using the browser saas solutions are common in sales, HR and ERP.

Paas (Platform as a service): This is different types of saas. You run your own application but you do it on the cloud provider's infrastructure.

Utility cloud services: There are virtual storage and server options that organizations can access on demand, even allowing the creation of a virtual data centre.

Managed services: This is maybe the oldest iteration of cloud solutions. In this concept, a cloud provider utilizes an application rather than end users. (i.e.) Anti-spam services or even application monitoring services.

Service commerce: These types of cloud solutions are a mix of saas and managed services. Common implementations include expense tracking, travel ordering or even virtual assistant services.

C. Current Trends in Cloud Security:

Prince jain [14] have proposed the parameters that affect the security of the cloud then it explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, and infected application and security issues. It also provides tips for tackling these issues and problems such as Control the consumer access devices, Monitor the Data Access, Share demanded records and verify the data deletion, Security check events.

F.A.Alvi et al [5] reviewed the security privacy & trust issues of cloud computing. They have proposed some surveys conducted by IDC that show the motivation for the adoption of cloud computing. Also identifies the issues and the solution to overcome these problems. It also contain the security model named security access control services SACS is analyzed through the Hadoop map reduce framework and the experimental results are obtained that compare the system performance with SACS model and without SACS model. Once the attack starts up, the performance which using security model is better than not using one. So the cloud computing with the proposed security model has the more stable performance when facing the attack threat, especially a variety of stacks at the same time.

Mandeep kaur and Manish mahajan [9] reviewed the Encryption Algorithms to enhance the Data Security in Cloud Computing. They have proposed to access a cloud based web application that will try to eliminate the concerns regarding data privacy; segregation. They also suggested different encryption algorithms like - AES, DES, RSA and Blowfish to ensure the security of data in cloud. They also stated that the research will be conducted using Java runtime of Google App Engine, i.e. JDK 1.6,Eclipse IDE,Google App Engine SDK 1.6.0 or higher.

Sara Qaisar and Kausar Fiaz Khawaja [16] proposed Network/Security Threats and Counter Measures for cloud computing. Cloud computing improves organizations performance by utilizing minimum resources and management support, with a shared network, valuable resources, bandwidth, software's and hardware's in a cost effective manner and limited service provider dealings. Basically it's a new concept of providing virtualized resources to the consumers. Consumers can request a cloud for services, applications, solutions and can store large amount of data from different location. But due to constantly increase in the popularity of cloud computing there is an ever growing risk of security becoming a main and top issue. This paper is going to present the comparative study of implementing encryption algorithm for securing the cloud.

III. ENCRYPTION METHODS FOR DATA SECURITY IN CLOUD

Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval. The following three papers analyze the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage.

3.1. Implementing DES Algorithm in Cloud for Data Security

Neha Jain and Gurpreet Kaur [11] described Data security system implemented into cloud computing using DES algorithm. This Cipher Block Chaining system is to be secure for clients and server. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases. The algorithm steps are follows.

1. Get the Plaintext.
2. Get the Password.
3. Convert the Characters into binary form.
4. Derive the Leaders (L1 to L16) from the Password.
5. Apply the Formula to get the encrypted and decrypted message.

In order to secure the system the communication between modules is encrypted using symmetric key. Though many solutions have been proposed earlier many of them only consider one side of security; the author proposed that the cloud data security must be considered to analyze the data security risk, the data security requirements, deployment of security functions and the data security process through encryption. The main contribution of this paper is the new view of data security solution with encryption, which is the important and can be used as reference for designing the complete security solution.

3.2. Data Security in Cloud computing using RSA Algorithm

Parsi Kalpana, Sudha Singaraju[12] have proposed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. The purpose of securing data, unauthorized access does not allow. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In the proposed Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

3.3. Homomorphic Encryption Applied to the Cloud Computing Security

Maha TEBAA et al [10] have proposed an application of a method to execute operations on encrypted data without decrypting them which will provide the same results after calculations as if the authors have worked directly on the raw data. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When the author decrypts the result of any operation, it is the same as if they had carried out the calculation on the raw data. In this paper cloud computing security based on fully Homomorphic encryption, is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. The author work is based on the application of fully Homomorphic encryption to the Cloud Computing security considering: The analyze and the improvement of the existing cryptosystems to allow servers to perform various operations requested by the client. The improvement of the complexity of the Homomorphic encryption algorithms and compare the response time of the requests to the length of the public key.

IV. RESULTS AND DISCUSSIONS

The comparison table considers the important cloud computing security characteristics such as,

- Key used

- Scalability
- Security
- Authentication type

Comparison [19] among the RSA, Homomorphic encryption algorithms and DES, The Homomorphic encryption algorithm and DES are scalable but RSA is not scalable. The security [18], the DES is fully secured for both providers and client side but RSA security applied client side only likewise Homomorphic encryption algorithm security applied cloud itself only.

The following table characteristic precedes the insecure issues. So we are using the effective authentication plan to provide stronger security for both cloud providers and consumers.

TABLE 1

CHARACTERISTICS OF EXISTING ENCRYPTION ALGORITHMS

Character-istics	***DES Algorithm***	***RSA Algorithm***	***Homomorphic Encryption***
Platform	Cloud computing	Cloud computing	Cloud computing
Keys Used	Same key is used for encryption and decryption Purpose.	Different keys are used for encryption and decryption Purpose.	private key is used(without decryption)
Scalability	It is scalable algorithm due to varying the key size and Block size.	Not scalable	scalable decryption
Security applied to	Both providers and client side	Client side only	Cloud providers only
Authentica tion Type	Message authentication used	Robust authentication implemented	Authentication never used

V. CONCLUSION

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability among others. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect is on performance of computing and for them cloud provides a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. So, as per the perspective of different users, the security point of view is different.

This paper analyses the importance of security to cloud. We compared three algorithms namely Data Encryption Standard (DES), RSA, Homomorphic encryption for data security in cloud. They are compared based on four characters; key used scalability, security applied to, and authentication type. In future we are going to propose a backup plan to solve security issues in both cloud providers and cloud consumers.

REFERENCES

[1] Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.

[2] Cloud computing methodology, systems and applications lizhe wang, rajiv ranjan.http://www.unitiv.com.

[3] Gartner: Seven cloud-computing security risks InfoWorld 2008-07-02.

[4] C.N. Höfer and G. Karagiannis, “Cloud computing services: taxonomy and comparison”, Internet Serv Appl (2011)

[5] F.A.Alvi, B.S.Choudary, N.Jaferry,”Review on cloud computing security issues & challenges”, iaesjournal.com, vol (2) (2012).

[6] Furht,B., and Escalante,A. (2010). Handbook of Cloud Computing. New York: Springer http://searchcloudcomputing.techtarget.com/definition /private-cloud

[7] Jagpal Singh,Krishnan lal and Dr.Anil kumar Shrotiya, Journal of Computer Science and Applications., ISSN 2231-1270 Volume 4, Number 1 (2012), pp. 1-7. http://www.irphouse.com

[8] Kevin Hamlen, Murat kantarcioglu, Latifur Khan and Bhavani Thurasingham, International Journal of Information Security and Privacy, 4(2), p.p(39-51), April-June 2010.

[9] MANDEEP KAUR, MANISH MAHAJAN, “using encryption algorithms to enhance the data security in cloud computing, “International journal of communication and computer technologies”, ISSN Number: 2278-9723.

[10] Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI, “Homomorphic Encryption Applied to the Cloud Computing Security”, Proceedings of the World Congress on Engineering 2012 Vol 1 WCE 2012, July 4 - 6, 2012, London, U.K

[11] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security ", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.

[12] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA [15] http://www.mytestbox.com/miscellaneous/cloud-computing-grid-computing-utility- computing-list-top-providers/

[13] Priyanka Arora, Arun Singh and Himanshu Tyagi,"Evaluation and Comparison of Security Issues on Cloud Computing Environment", (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, p.p (179-183), 2012.

[14] Prince jain, "security issues and their solution in cloud computing ", International journal of computing & business research, ISSN (online):2229-6166.

[15] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal," A Survey on Security Issues in Cloud Computing". IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[16] Sara Qaisar and Kausar Fiaz Khawaja," CLOUD COMPUTING:NETWORK/SECURITY THREATS AND COUNTERMEASURES", ijcrb, JANUARY 2012 VOL 3, NO 9.

[17] Security analysis of cloud computing :(http://cloudcomputing.sys-con.com/node/1330353).

[18] VAMSEE KRISHNA YARLAGADDA and SRIRAM RAMANUJAM, "Data Security in Cloud Computing", Vol.2 (1), p.p (15-23) (2011).

[19] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.