ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

AUTHENTICATION & ISOLATION OF CRYPTOGRAPHIC SERVICES FOR CLOUD COMPUTING

Madhavi Shyamsunder Shinde*[1] and Prof. Mirza Moiz Baig[2]
*[1]M.Tech Student, Department of CSE JD College of Engineering, Nagpur
[2]JD College of Engineering, Nagpur

ABSTRACT
Cloud computing is a virtual environment in which resources of the computing infrastructure are providedas data security and access control when users outsource sensitive data for sharing on cloud servers, which are notwithin the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers,existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to information privacy. This Project proposes a business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service. An authentication method is proposed at a lower level which can be implemented by cloud providers. It is a simple way of authentication which can be utilized by developers along with encryption.

INTRODUCTION
At the present world of networking system, Cloud computing is one the most important and developing concept for both the developers and the users. Persons who are interrelated with the networking environment, cloud computing is a preferable platform for them. The cloud offers many strong points: infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc.

Over the recent years, there is a great advancement in the field of Computer Science. Cloud Computing is the result of advancement in the existing technologies. Cloud Computing is beneficial not only for users but also for large and small organizations. Security issues are the major concern in Cloud Computing.

At the present world of networking system, Cloud computing is one the most important and developing concept for both the developers and the users. Persons who are interrelated with the networking environment, cloud computing is a preferable platform for them. Therefore in recent days providing security has become a major challenging issue in cloud computing. In the cloud environment, resources are shared among all of the servers, users and individuals. As a result files or data stored in the cloud become open to all. Therefore, data or files of an individual can be handled by all other users of the cloud. Thus the data or files become more vulnerable to attack. As a result it is very easy for an intruder to access, misuse and destroy the original form of data. Hence, it is extremely essential for the cloud to be secure. Another problem with the cloud system is that an individual may not have control over the place where the data needed to be stored. A cloud user has to use the resource allocation and scheduling, provided by the cloud service provider. Thus, it is also necessary to protect the data or files in the midst of unsecured processing.

If a cloud system is answerable for both the tasks on storage and encryption-decryptionof data, the system administrators may concurrently obtain encrypted data and decryption keys and there may be thechances of unauthorized disclosure of data. This allows them to access information without authorization and thusposes a risk to information privacy.

OBJECTIVE
Cloud computing security issues
As cloud computing providing the security there has some issues related to security they are as follows:

A. Security
Security is generally a desired state of being free from harm. As defined in information security, it is a condition in which an information asset is protected against its confidentiality, integrity and availability in the desired state

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

and at the right time. Security is an important domain in as far as cloud computing is concerned, there are a number of issues to be addressed if the cloud is to be perfectly secure
Professional hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft .

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services.

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing.

D. Legal Issues

As with other changes in the landscape of computing, certain legal issues arise with cloud computing, including trademark infringement, security concerns and sharing of proprietary data resources.

These legal issues are not confined to the time period in which the cloud-based application is actively being used. There must also be consideration for what happens when the provider-customer relationship ends.
E.Performance interference and noisy neighbor

Due to its multi-tenant nature and resource sharing, cloud computing must also deal with the "noisy neighbor" effect. This effect in essence indicates that in a shared infrastructure, the activity of a virtual machine on a neighboring core on the same physical host may lead to increased performance degradation of the VMs in the same physical host, due to issues

As Cloud Computing has been spreading widely, users and service providers enables to use resource or service cheaply and easily without owning all the resource needed. However, Cloud Computing has some security issues such as virtualization technology security, massive distributed processing technology, service availability, massive traffic handling, application security, access control, and authentication and password. User authentication among them requires a high-guaranteed security. Hence, this paper would like to discuss technologies of access control and user authentication briefly and look at the problems inside.

Along with authentication of user and all other parties involved in the process of data storing, encrypting, decrypting and retrieving another major goal of this project is securing the cloud by isolating the processes of encryption and decryption. This can be done when encryption and decryption will be done separately by different vendors. In this way the keys used for encryption and decryption will be kept secret. The processes will be in control and there will not be much threat to the security.

LITRATURE REVIEW

Cloud Computing Business Model: Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. Cloud computing entrusts remote services with a user's data, software and computation.
Services by cloud computing over the network are:

A. PaaS- In this type of service, Platform is provided to the cloud consumer as a service. For example- Operating System.
B. IaaS- In this type of service, infrastructure is provided to the cloud consumer as a service. For example- Storage area, server physical equipment.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

C. SaaS- In this type of service, Software is provided to the cloud consumer as a service. For example- Microsoft Word, Notepad, Paint, or many other applications.

In the last decade, much development has taken place in the field of authentication models. A number of frameworks, models and architectures have been proposed by researchers.
This Project proposes a business model for cloud computing based on the concept of separating the encryption and decryption service.

PROBLEM DEFINATION

This section addresses the core theme of this chapter, i.e., the security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing.

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The trusted computing group's (TCG's) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user's access privilege is revoked or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within a very short span of time

RESEARCH METHODOLOGY

With the growing popularity of cloud, companies are investing heavily in the research of cloud computing security. In this paper some of the significant and latest research is included which mainly focus on the authentication phase of cloud security. After the thorough review of literature in cloud computing authentication, some new directions and approaches are set forth that can facilitate the researchers in this area.

Research methodology was selected to perform this research. This research methodology is a nominal sequence process of well-defined activities per the referenced paper.

Kerberos method of authentication and a hybrid method using AES and DES for encryption and decryption as a combination will fulfill the purpose of this project.

For authentication purpose,Kerberos method is used. It is a computer network authentication protocol that works based on 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Kerberos is a trusted third-party authentication system that relies on shared secrets. It presumes that the third party is secure, and provides single sign-on capabilities, centralized password storage, database link authentication, and enhanced PC security. It does this through a Kerberos authentication server, or through Cybersafe Active Trust, a commercial Kerberos-based authentication server.

Kerberos is a computer network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.
Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.[1]Kerberos uses UDP port 88 by default.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

A hybrid approach is used i.e. combination of AES and DES algorithms are used to obtain the optimal results. The DES (Data Encryption Standard) is a cryptographic standard. The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key. In cryptography, the Advanced Encryption Standard (AES) cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The integration of AES with DES is to enhance security for input mode as text, image, audio and video. To understand the need for minimizing algebraic attacks on AES there by the idea of integrating AES with DES is proposed. Hence the development of the Hybrid AES-DES algorithm is considered.

OUTCOME

The paper witnesses the evolution of authentication. Research is still in progress finding new methods and schemes to authenticate the user in order to challenge the security threats faced by the Cloud. These new approaches by various researchers offer a good foundation for further research and development in the field of Cloud security.

Here we are focusing on the security goal by enhancing the authenticity of the client along with the vendor responsible for encryption and the vendor responsible for decryption process, since there cryptographic processes will be done separately to reduce the risk of misusing the information of decryption key that will be used. Hencewise, more security will be provided to the cloud environment

CONCLUSION

Cloud service can be accessed by a device that can access the internet, the device may be Laptop, PC, and Smart Phone etc.

If storage and encryption/ decryption are provided by a single service provider than there may be a more chances for unauthorized access of data from high level authority like System administers, as he has access to Decryption key and encrypted data that is stored. This paper proposes a Secured cloud computing model based on separating the cloud computing services into two different service providers. Therefore a contract is to be signed for establishing a cooperation model for providing common services to clients. The main aim of this paper is dividing of authority to reduce operational risk due to which unauthorized access of data.

For cloud computing to be used and spread, users must have a high level of trust in the methods by which service providers protect their data, emphasizing that authorization of the storage and encryption/decryption of user data must be differentiated with two different service providers. The privileges of storing as a service provider include storing user data which is already encrypted through an Encryption/Decryption service.

ACKNOWLEDGEMENTS

This section should be typed in character size 10pt Times New Roman, Justified.

REFERENCES

1. *Authentication and encryption in Cloud Computing*
   Published in: Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference
   Date of Conference: 6-8 May 2015
   Print ISBN: 978-1-4799-9854-8
   INSPEC Accession Number:15403341
   Conference Location:Chennai
   DOI:10.1109/ICSTM.2015.7225417
   Publisher:IEEE
   http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7225417&punumber%3D7193753%26filter%3DAND(p_IS_Number%3A7225373)%26pageNumber%3D2
2. *Review on A Business Model for Cloud Computing Based on aSeparate Encryption and Decryption ServiceGaurav Sinha Thakur1, V Kala21M. Tech Scholar, 2Assistant Professor, Department of Computer Science & Engineering, Maharashtra Institute of Technology(MIT), Aurangabad, Maharashtra, IndiaInternational Journal of Emerging Technology and Advanced Engineering*

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 12, December2014)http://www.ijetae.com/files/Volume4Issue12/IJETAE_1214_69.pdf

3. *Business Model Based on A Separate Encryption & Decryption Services for Cloud Computing*
   1a. R. Kamble, 2sanket Taral, 3prasad Kubade, 4abhishek Wagh, 5nikhil Shete
   Sinhgad Institute of technology and Science, Narhe, Pune 41, University of Pune, Maharashtra, India
   International Journal of Advances in Computer Science and Cloud Computing. http://iraj.in/journal/journal_file/journal_pdf/5-31-139037364412-15.pdf
4. *A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service*
   Authors: Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu, Chien-Hsing Wu
   Published in: • Proceeding ICISA '11 Proceedings of the 2011 International Conference on Information Science and Applications Pages 1-7
   IEEE Computer Society Washington, DC, USA ©2011
   Table of contents ISBN: 978-1-4244-9222-0 doi>10.1109/ICISA.2011.5772349
   http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5772349
5. *Data Security in Cloud Computing Using Separate Encryption/Decryption Cloud Service*
   Authors: Prajakta R Rajapure, Swati N Ranpise, Deepali S Khandzode,Meghana R Kanthale Dept. of Computer Engineering PES's Modern College of Engineering Pune, India
   International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 4 743 – 746
6. *Cloud Computing a Crm Service Based on Separate Encryption and Decryption Using Blowfish Algorithm*
   Rajiv R Bhandari M-Tech Student, Department of IT NRI Institute of Information Science and Technology Bhopal, (MP) India. rajivbhandari@ymail.com Prof.Nitin Mishra Professor, Department of IT NRI Institute of Information Science and Technology Bhopal, (MP) India. nitin.nriist@gmail.comInternational Journal on Recent and Innovation Trends in Computing and Communication Volume: 1 Issue: 4
7. *International Journal of Computer Applications (0975 – 8887) Volume 39– No.18, February 2012 23 the Comprehensive Approach for Data Security in Cloud Computing: A Survey Nilesh N. Kumbhar Virendrasingh V. Chaudhari Mohit A.Badhe*
8. *Securing user authentication using single sign-on in Cloud Computing*
   Published in:Engineering (NUiCONE), 2011 Nirma University International Conference onDate of Conference:8-10 Dec. 2011
   Print ISBN:978-1-4577-2169-4
   INSPEC Accession Number:12571758
   Conference Location:Ahmedabad, Gujarat
   DOI:10.1109/NUiConE.2011.6153227
   Publisher:IEEE
9. *IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 3, No 1, May 2014 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org*
   Critical Review of Authentication Mechanisms in Cloud Computing S.Ziyad1 and S.Rehman2 Department of Information System Salman bin Abdul Aziz University, KSA
10. *Secure user authentication in cloud computing management interfaces*
    Soares, L.F.B. Dept. of Computer. Sci., Univ. of Beira Interior,Covilha,Portugal Fernandes, D.A.B. ; Freire, M.M. ; Inacio, P.R.M.
    Published in:Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International
    Date of Conference:6-8 Dec. 2013
    Print ISBN:978-1-4799-3213-9
    INSPEC Accession Number:14117379
    Conference Location: San Diego, CA
    DOI:10.1109/PCCC.2013.6742763
    Publisher:IEEE
11. *Privacy Protection in Cloud Using RSAAlgorithmAmandeep Kaur, Manpreet KaurAmandeep Kaur et al Int. Journal of Engineering Research and Applications*
    www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 5 (Version 3), May 2014, pp.119-122

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

12. *Hybrid Security Algorithms for Data Transmission using AES-DES*
Jignesh R Patel PG-scholar, TCET Kandivali, Mumbai India, Rajesh S. Bansode Asst.prof, TCET Kandivali, Mumbai India, Vikas Kaul Asst.prof, TCET Kandivali, Mumbai India
International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.2, February 2012 – www.ijais.org
13. *Kerberos: an authentication service for computer networks*
B.C. Neuman
Inf. Sci. Inst., Univ. of Southern California, Marina del Rey, CA, USA
T. Ts'o
IEEE Communications Magazine