RESEARCH ARTICLE OPEN ACCESS

Enhancing Cloud Security through Two Way Authentication with Attribute Based Encryption and Blowfish Algorithm

Mrs. M. Prashanthi
Assistant Professor
Department of Computer Science
CMREC, kandlakoya
Hyderabad – India

ABSTRACT

As we know that cloud computing is one, which is a type of internet based computing, which provides shared computing processing resources and data to computers and other devices on demand. We can say cloud computing is known as the most affordable internet paradigm for small scale business entrepreneurs. Services provided by the cloud computing are large attractive and helpful for small and medium sized enterprises owners to perform their operations in desired applications. Nowadays protecting data from the cloud is becoming very big issue so that here some possibilities are there those are one – time password and email based verification while a user logging into corresponding website or cloud data. So that we restrict a user with these (one-time password and e-mail verification) methods. Increasing of cloud computing has given opportunities for hackers to steal sensible data from the database. To stop hacking activities of a secure data management has been developed and introduced in this project. The cloud owners who are managing enterprise will have the services of cloud computing and stores data into cloud servers. To restrict cloud un-authorized users blowfish encryption algorithm is used.

Keywords:- Cloud Computing, Data Access; Attribute Based Access, Blowfish Encryption Algorithm.

I. INTRODUCTION

One of the most trusted business is cloud computing for small scale enterprises with unlimited facilities or resources with most economical range in the internet .Cloud computing provides software as a service, infrastructure as a service, database as a service and platform as a service. Cloud computing is the best infrastructure to provide cloud servers to the cloud consumers. The cloud consumers has their own customers, these cloud consumers using cloud computing servers for data sharing and These combinations of two methods sharing of sensitive data with the customer .These cloud users are using the cloud services for their operations according to their requirements.

These cloud users will store data or information and share some sensitive data to their customers. So that all these activities are to be in secure manner and providing quality of data to the different users.

II. BACKGROUND

In this project we are going to provide security to the cloud users by attribute based encryption and Blowfish algorithm from cloud computing consumers to its customer's .This project is incorporated with the following features.

The project is rich with attribute based encryption, Blow fish Mechanism to achieve the measurable safe and secure cloud computing data management. In this, project will provides controlled access to the end users from the cloud data management. Here cloud computing data management Is going to restrict the end users who are accessing data without getting proper permissions or without knowledge of cloud service providers.

III. PROPOSED SYSTEM

The main goal of the project is to restrict the end user with encrypted mechanisms like attribute based

encryption and Blow fish encryption mechanisms which provides security to the cloud data by restricting the end users while they(end users ,who are going to access the cloud data without getting proper permissions from service providers)are getting proper registration and while logging into the cloud to be accessed .This Blowfish mechanism is fully restricts the end users from unauthorized access of the cloud data.

IV. CRITICAL ANALYSIS

Data management in cloud computing with safe and secure by applying blowfish encryption. This project is rich with granting user access to the specific users of the enterprise owner and apply the attribute based encryption algorithm and Blowfish algorithm to restrict the user to access unwanted data and upload malicious data.

These two methods increasing the users and giving access permissions to the Database made the project to consider as the best database management project in cloud computing with proper security. Here the user is restricted via 2 methods. One is one time password and other is Email based confirmation. These are the two ways to restrict the unauthorized users of the cloud data.

Here the Blowfish Algorithm helps to restrict the unauthorized users and which replaces the RSA and DSA encryption Algorithms. This is somewhat better to restrict the unauthorized users by using the Blowfish Algorithm. This Project is designed and developed in Visual n studio with .Net frame work to exemplify the cloud operations in simulation Environment.

V. IMPLEMENTATION

The Implementation of the project is done in the .net frame work. This project is running in the IIS Server to exemplify the cloud Environment.IIS server is replicating the cloud environment and the user s and cloud service providers will achieve their duties consequently. The Implementation of the project is done in IIS server with the configuration of host for the web based application. This application should be accessed by different systems connected in LAN.

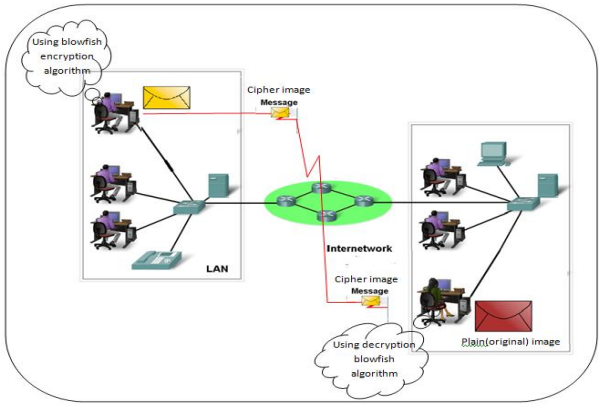

Figure: Blowfish encryption

VI. RESULTS

The output results have been evaluated here unauthorized users are restricted by using Blowfish and Attribute based access Encryption Methods. Here the user has been restricted by one time password and e-Mail based confirmation this project enable the user to access a specific attribute allocated by the data owner of cloud consumer.

The date management with safe and secure access to the user has been established by using the attribute based Encryption and Blowfish Mechanisms .Here th e user policy will be made to specific user with the user name and password. The user be performing the access of the data through the confirmation of email and one time password .the date managed with attribute access rights and user right of entry have restricted the user's to interrelate with the server to upload any malicious data.

The cloud computing environment has been created with the help of SQL Server 2008 database and .Net Framework the attribute based encryption algorithm and Blowfish algorithm has been designed and developed using ASP.Net, C# and ADO.Net.

VII. CONCLUSION AND FUTURE WORK

Now a day's increasing huge amount of data in the cloud. Different services are providing data access to the users, but still facing so many problems with un-authorized

users, here we can say that ,how the data increasing in the cloud , in the same way un-authorized users also increasing day-by-day. This is the fact of current situation. In this project there are some methods those are two-way-authentication (OTP and E-Mail). With these two methods we can restrict un-authorized users .In future work, we can implement user image reorganization based techniques and there are unlimited solutions to restrict un-authorized users.

REFERENCES

[1] Alan g. konheim. 2007. Computer security and cryptography. by john wiley and sons, inc.

[2] Alfred j.m., paul v. c. and scott a. v. 2001. Handbook of applied cryptography. Fifth addition.

[3] Bruce Schneier. 1996. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C. Wiley Computer Publishing, John Wiley and Sons, Inc.

[4] B. Schneider. 1994. Applied Cryptography, John Wiley and Sons, New York.

[5] B. Schneier. 1994. Description of a New VariableLength Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag. pp. 191-204.

[6] Oppersmith Don. 1994. The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development. 38(3): 243-250.

[7] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25

[8] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2003.

[9] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACMConf. Computer and Communications Security (CCS), Alexandria, VA, 2005

[10] SecureCloud™ Securing and Controlling Sensitive Data in the Cloud by Trend Micro

[11] Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing by Shucheng Yu, Cong Wang, KuiRen and Wenjing Lou

[12] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00, 2000.