International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

EFFICIENT AUTHENTICATION USING MERKLE HASH TREE ALGORITHM IN JELASTIC SERVER

KARTHIKA R , ARCHANA DEVI R, SUGANYA T, NIVETHITHA K
DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
PANIMALAR ENGINEERING COLLEGE, CHENNAI, INDIA

Article Received: 02/03/2015 | Article Revised on:08/03/2015 | Article Accepted on:10/03/2015

Karthika R

Archana Devi R

Suganya T

NIVETHITHA K

ABSTRACT

"Secret image authentication" describes the process of obtaining a digital representation of a secret image and comparing it to a stored digital version of the image in the cloud database. The digital secret image templates can be stored in database and used in place of traditional password for secure access. Secret image authentication is a significant security element popularly used in several applications, providing uniqueness and acceptable performance.In existing system, the keys are used for authentication purpose which is in encrypted form and was stored in the cloud database. The hacker may decrypt the key using some advanced technique which results in loss of data storage security, computation auditing security as well as privacy cheating discouragement. In this project a new approach of remote user secret image authentication using the concept of Merkle Hash Tree (MHT) has been proposed. The data owner stores the file in an encrypted form using Advanced Encryption Standard (AES) in the cloud server. The cloud user has to register with the owner along with the personal details and secret image. The user name, password and root signature will be sent to the registered mail id by using the Simple Mail Transfer Protocol (SMTP). In the client side, the secret image template is split into eight shares using image processing technique Boundary Splitting Algorithm.The splitted eight shares are given as inputs to merkle hash tree where in each share has to undergo hashing function and hence root signature is generated and stored in the cloud server. The user has to submit the root signature for authentication purpose. The signature is generated in the cloud serviceprovider and thus verified with the stored signature in the cloud. Symmetric key is used to provide additional security when the users want to access the files stored in the cloud database. Thus misuse of sensitive data can be avoided and this provides an effective and efficient user remote authentication with the cloud.

KEYWORDS: Merkle Hash Tree, Advanced Encryption Standard, Jelastic Server, Boundary splitting, Authentication, Root signature, Symmetric key

I. INTRODUCTION

Cloud computing has been envisioned as the emerging architecture of the IT enterprise due to its on demand self-service, ubiquitous network access, location-independent resource pooling , rapid resource elasticity and usage-based pricing . The fundamental aspect of cloud storage computing model is that data is being centralized or outsourced into the cloud without the burden of local hardware and software management. This field has the innovation of new technologies which has its application in day-to-day life. Security and privacy are very important issues in cloud computing. It is the computing service provided over the Internet. some of the current trends in cloud computing are Hybrid clouds, BYOD, Platform- as- a-service(PaaS), Identity management and protection, web-powered apps.

Cloud computing focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated as per demand. This can work for allocating resources to users. This approach should maximize the use of computing power thus reducing environmental damage are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications. Cloud computing is the delivery of services of computing a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices over a network. Cloud computing is the delivery of services of computing a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices over a network. The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service oriented architecture, autonomic and utility computing have led to a growth in cloud computing.

A decentralized access control technique with anonymous authentication [1], which provides secure data storage in clouds, user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials.Only valid users are able to decrypt the stored information.

The auditing protocol protects the data privacy against the auditor by combining the cryptography method with the bilinearity property of bilinear paring. Multicloud batch auditing protocol[2] does not require any additional organizer. It can also support the batch auditing for multiple owners. The Auditing scheme incurs less communication cost and less computation cost. The protocol supports the batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

Attribute-based encryption (ABE) technique and Fine-grained access control provides a Patient-centric framework[3] and a suite of mechanisms for data access control. Framework for secure sharing of personal health records in cloud computing.The Patients shall have complete control of their own privacy.It also reduces the complexity of key management.

The Identity-based authentication protocol[4] is more lightweight and efficient than SSL Authentication Protocol (SAP). It provides greater scalability which is very suitable for the massive scale cloud.It allows the users with an average or low-end platform to outsource their computational tasks to more powerful servers.

MuR-DPA a Novel public auditing scheme[5] scheme can support fully dynamic data updates, authentication of block indices and efficient verification of updates for multiple replicas at the same time. It provides enhanced security against dishonest cloud service providers and incurs much less communication overhead for both update verification and integrity verification of cloud datasets with multiple replicas.

Cryptographic primitive for fine grained access control shared data. The attribute revocation becomes so complicated by using Cipher text Policy Attribute Based Encryption (CP-ABE) [6]. It is the provably secure against cipher text attack. Enables the authority to revoke user attributes with minimal effort

II. EXISTING SYSTEM

In existing system, the keys are used for authentication purpose which is in encrypted form and was stored in the cloud database. Even though the keys are in encrypted form the hackers may use some advanced technique to decrypt the keys and

can access the data, modify the data or even result in loss of data. Due to this the security level will be decreased and gives less efficiency. The keys are generated using key generation algorithm which does not make the efficient process and makes cheatable cloud computation and privacy cannot be achieved. It also results in loss of data storage security, computation auditing security as well as privacy cheating discouragement. The computation cost is maximized due to optimization problem.

III. PROPOSED SYSTEM

In the proposed system a secret image authentication is done using the concept of Merkle Hash Tree (MHT) algorithm. The data owner stores he file in an encrypted form using the Advanced Encryption Standard (AES) algorithm in the cloud server. The cloud user has to register with the owner along with personal details and secret image. The user name, password and root signature will be sent to the registered mail id by using the Simple Mail Transfer Protocol (SMTP) .The Secret image template is split it into eight shares using image processing technique Boundary Splitting Algorithm and are given as inputs to Merkle Hash Tree. Hence the root signature is generated and stored in the Jelastic cloud server (Jelastic cloud is a public cloud which is used to access the file stored in the Jelastic cloud database with valid mail id and password). If the users want to access the Jelastic cloud, user must give the same mail id and password which is given during registration. If the given mail id and password is correct then the user can access the data or else can't access the data.The user has to submit the root signature for authentication purpose. The signature is generated in the cloud service provider and thus verified with the stored signature in the cloud. If the user's given root signature are matched to the root signature stored in the database ,the user can login in to the server and can access and modify the files stored in it. Thus, provide efficient authentication and security. By using the Symmetric key Encryption method the owners create the secure key and send to the user. Whenever the user wants to access or decrypt the file store in the Jelastic cloud database, the user must enter the same key with which the file is encrypted and stored in the database. Thus the misuse of sensitive data can be avoided and this provides an effective and efficient user remote authentication with the cloud.

IV. MODULES

1) Jelastic Server Module
2) Owner Authentication Module
3) File Authentication Module
4) File Upload Module
5) File Access in Jelastic Cloud Module.

1) JELASTIC SERVER MODULE

Jelastic team has created a plugin in netbeans development platform that simplifies the process of application management and development in jelastic platform. User install the Jelastic netbeans pluggin into the netbeans. The owner can add the project into the cloud database. If the user want to access the jelastic cloud, must give the user id and password which is sent to the user's mail id. If the given mail id and password is correct the user can login into the server .

2) OWNER AUTHENTICATION MODULE

This module explains the owner's part in the Jelastic cloud. The owner check the user' personal details and secret image given during registration. The secret image template is split it into eight shares using image processing technique Boundary Splitting Algorithm and are given as inputs to Merkle Hash Tree. Hence the root signature is generated and stored in the Jelastic cloud server.

3) FILE AUTHENTICATION MODULE

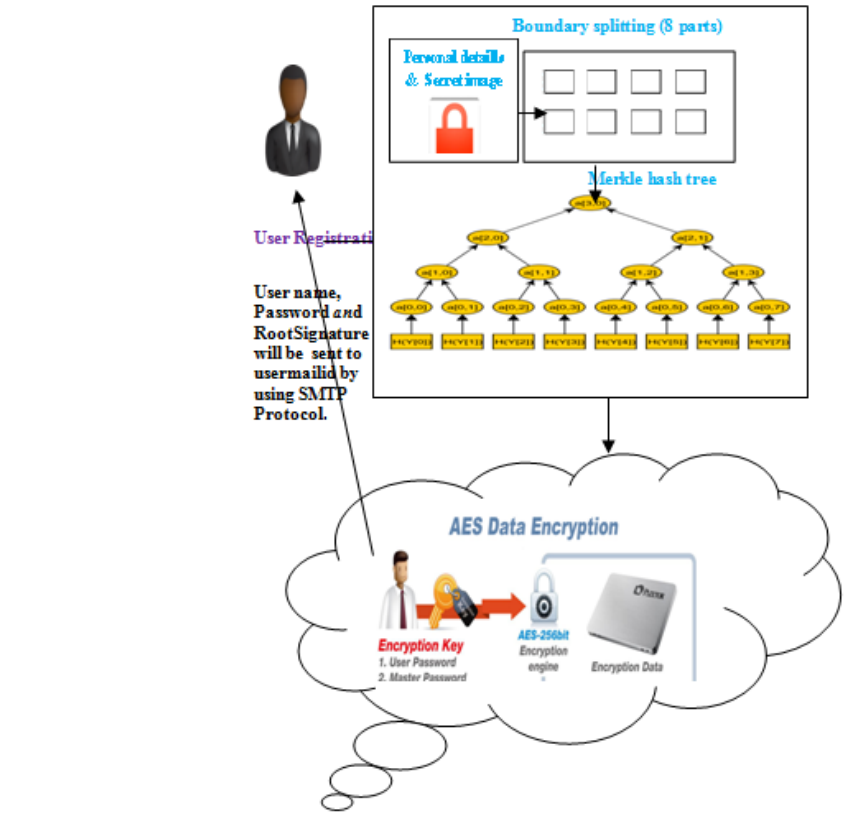
Root signature will be saved in encrypted format in the Jelastic server using Advanced Encryption Standard [AES]. The user name, password and root signature will be sent to the registered mail id using Simple Mail Transfer Protocol (SMTP).If the user's given root signature are matched to the root signature stored in the database ,the user can login in to the server and can access the files stored in it. Thus provide efficient authentication and security.

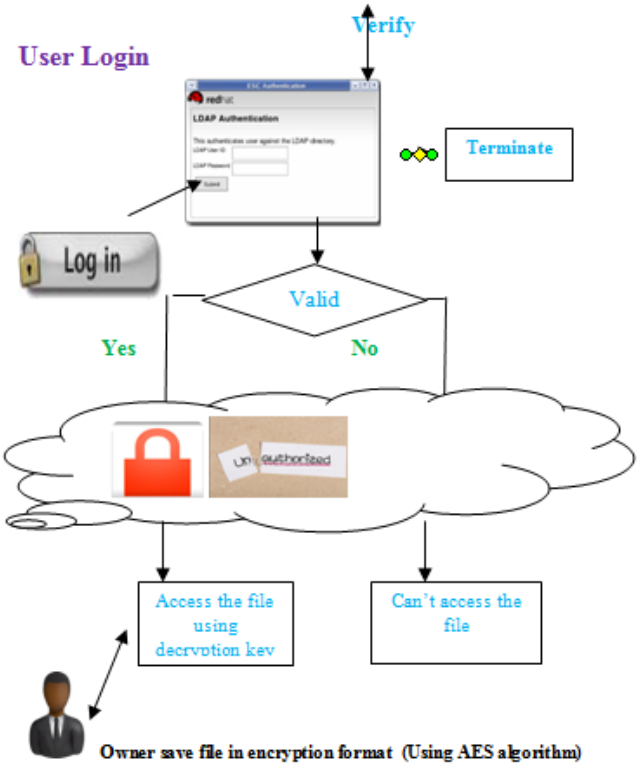
4)FILE UPLOAD MODULE

In this module the owner can upload the file and user requirements to the Jelastic cloud. Using Advanced Encryption Standard file is stored in encrypted format in the cloud database . User can search and view the details and contents using any web browser. User can even upload file, the owner can check and verify all details and images to accept the uploaded files. If authentication process is

successful the uploaded file is stored in encrypted format in the cloud database.

SYSTEM ARCHITECTURE





Owner save file in encryption format (Using AES algorithm)

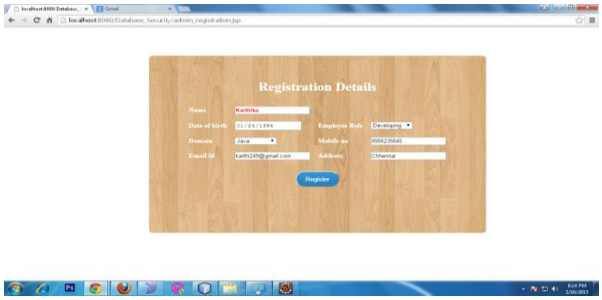
5) FILE ACCESS IN JELASTIC CLOUD MODULE

Users can search the content from any web browser and get response from the server. By using the symmetric key encryption method the owner may create the symmetric key when the file is stored in the database in an encrypted format and send the key to the user. whenever the user wants to access or decrypt the file store in the Jelastic cloud database, the user must enter the same key.

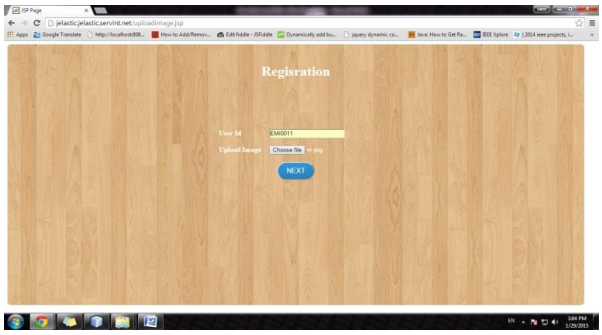
V. SAMPLE OUTPUT

REGISTRATION

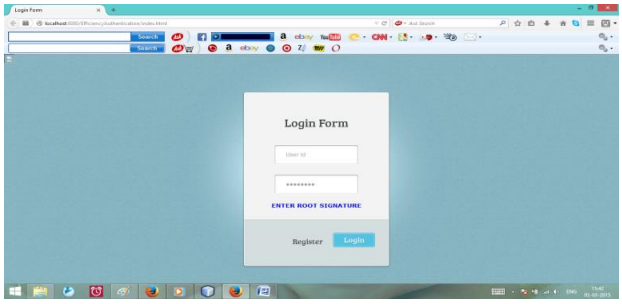
STEP 1: PERSONAL DETAILS



STEP 2: SECRET IMAGE

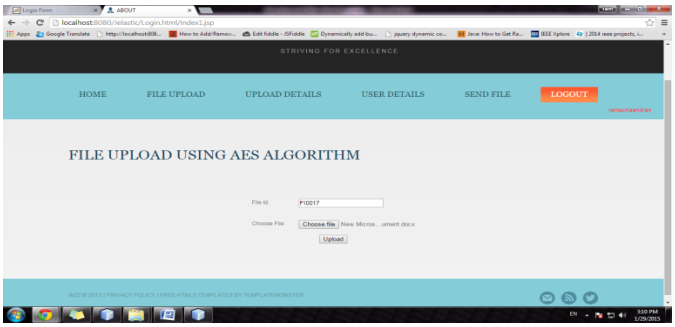


LOGIN

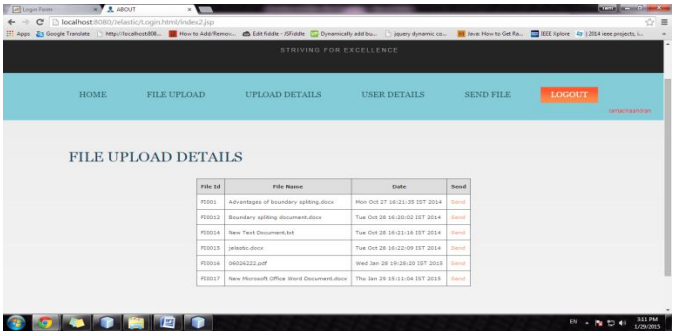


HOMEPAGE

FILEUPLOAD



FILE SHARING DETAILS



VI. CONCLUSION

Secret image authentication is a significant security element that provides uniqueness and acceptable performance.Secret image authentication is done using the concept of Merkle Hash Tree (MHT) algorithm. The data owner stores the file in an encrypted form using the Advanced Encryption Standard (AES) algorithm in the cloud server. The cloud user has to register with the owner along with personal details and secret image.The user name, password and root signature will be sent to the registered mail id by using the Simple Mail Transfer Protocol (SMTP). The Secret image template is split it into eight parts using image processing technique - Boundary splitting algorithm and are given as inputs to Merkle Hash Tree. Hence the root signature is generated and stored in the Jelastic cloud server. If the user want to access the Jelastic cloud, user must give the same mail id and password which is given during registration along with the root signature for authentication. Ifthe given mail id, password and root signature matches with the data stored in the cloud the user can access the data or else can't access the data. By using the Symmetric key Encryption method the owners create the secure key and send to the user. Whenever the user wants to access or decrypt the file store in the Jelastic cloud database, the user must enter the same key with which the file is encrypted and stored in the database. Thus the

misuse of sensitive data can be avoided and this provides an effective and efficient user remote authentication with the cloud.

VII. FUTURE ENHANCEMENT

Here we use the secret image for the authentication purpose because the secret image will differ for each and every individual and that will be their own choice. This provides uniqueness and acceptable performance. In future we can use Fingerprint Authentication which is a significant security element and popular biometric modality which is used extensively in several applications for person authentication. We can even go for iris or face recognition.

References

[1]. Sushmita Ruj, Milos Stojmenovic, Amiya Nayak," Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" Vol. 25, No. 2, FEBRUARY 2014.

[2]. Kan Yang, Xiaohua Jia,"An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", VOL. 24, NO. 9, SEPTEMBER 2013.

[3]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" VOL. 24, NO. 1, JANUARY 2013

[4]. Hongwei Li1, Yuanshun Dai1,2, Ling Tian1, and Haomiao Yang1,"Identity-Based Authentication for Cloud Computing"-2009.

[5]. Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, " Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud" -2013

[6]. Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou" Attribute Based Data Sharing with Attribute Revocation"10 April 2010