ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Implementation of Shared Authority Based Privacy Preserving Authentication Protocol in Cloud Computing

Judith Nita M, Rajaprabha M N

Student, School of Information and Technology, VIT University, Vellore, TamilNadu, India

Assistant Professor, School of Information and Technology, VIT University, Vellore, TamilNadu, India

ABSTRACT: Cloud computing is one of the popular technologies that aims to provide delivery and storage capabilities as a service to users. In general terms we can define cloud computing as the one that delivers services that are hosted over the web. Cloud services provide on-demand applications while ignoring the limitations of the native infrastructures. During the information accessing, different users can be in a mutual relationship which stresses on the importance of knowledge sharing in order to attain better performance. The existing security solutions generally focus on authentication procedures where a user's private knowledge cannot be accessed without proper authorization, however neglecting the privacy issue. This could reveal user's private information regardless of the information access permissions being granted or not. Therefore, we can use SAPA protocol in which shared access authority is achieved by anonymous access request matching mechanism to handle the privacy issue in cloud.

KEYWORDS: Cloud computing, authorization authentication protocol, security, privacy preservation, shared authority

I. INTRODUCTION

Cloud computing is a popular IT architecture in the current trend, which offers exclusive data storage with on-demand services and network access round the clock. This architecture can be witnessed as a service which could be software, infrastructure or a platform available anytime anywhere for the users. Despite being popular and powerful cloud computing faces downfall in areas of privacy and security. Traditional approaches concentrate on the authentication procedures to witness remote access of data on demand. But eventually a user may want to access or share data for better results, which in turn brings security and privacy concerns in cloud storage. In order to overcome this, Shared Authority based Privacy preserving Authentication protocol (SAPA). This protocol is exclusively used for handling the privacy issues in cloud storage. Shared access authority is achieved by anonymous access request matching procedure with four important attributes namely, User privacy, Authentication, Forward Security and Anonymity [1].

User privacy is achieved when any unrelated user cannot wild guess a user's access interests. Only if they both possess a mutual interest they will be allowed to share by the cloud server. Authentication is achieved when a legal and registered user can access his data and any other data cannot deceive him. Anonymity is achieved when any unrelated entity cannot find out the data transferred and communication state even by interception through open communication channel. Forward security is achieved when any miscreant cannot guess the previous communications with the currently held data of any two sessions. Attribute based access control is used to make sure that the users can access only his data. Thus this protocol is well suited for multi-user collaborative cloud applications since it does not compromise the user's private information.

II. RELATED WORK

In [2] ENISA has proposed that "Complexity of risk evaluation" is one of the major privacy challenges in cloud computing. The complexity of the services gives rise to a number of unidentified parameters. Service consumers and

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

providers are careful while providing and consuming services. The real challenge encountered in this scenario is checking the lifecycle of data processing and its conformity with officially authorized frameworks. Some of the following questions are needed to be answered in order to find the risks to privacy: Who are the stakeholders involved?, Where the data is stored?, How data is duplicated?, What are the stakeholder roles and responsibilities?, What are the rules for data processing?, How the service provider will reach the desired level of privacy and security? They have suggested that every user can have an apparent policy as how to the personal data is to be processed and the stakeholders have to specify the needs for cloud that meet the desired level of privacy. ENISA in Europe suggest understanding the shift in balance in terms of accountability and responsibility in key functions and conformity with the laws [2]. In [3] authors suggest that developing and implementing proactive strategies or measures to promote better compliance with the laws of privacy regarding the personal data processing. This can be done through procedures that detect and prevent breaches in systems. Literally, there is no accepted definition for PETs, but in general we can consider technologies with the following qualities are PETs, reduce privacy risks, data held about the users are minimal, allow the users to have control over their information. Therefore, by implementing the PETs the requirements of the proactive measures could be met. And they can protect the privacy over the personal data and prevent from undesired processing. These PETs include tools like anonymisation, encryption, pseudonymisation, transparency enhancing tools. In [4] authors have proposed that "Client Based Privacy Manager" helps in reducing the data leakage and loss of privacy of the sensitive data. Some the major characteristics of the privacy managers are: Data Access: The Manager contains a separate module for accessing personal information by the users in the cloud. This is an auditing procedure that checks accuracy and privacy violations. Obfuscation: This is done by the users on the required fields before being sent to the cloud using a user chosen key that the service providers are not known of. Feedback: This module keeps track of the data being transferred and data usage. Preference Setting: Allows the users to set preferences over their data thereby giving greater control. The major advantage is that it solves automation and end user problems. The disadvantages are, it requires full co-operation of the service provider and sufficient computing resources for obfuscation. In [5] authors have proposed that for Anonymous data sharing between the parties an algorithm is developed to generate ID numbers ranging from 1 to N. And the assignment of these ID's is anonymous so that the members do not know about it and maximum care is taken to avoid collisions. These procedures are carried out without a trusted third party. Newton's identities and strum theorem to develop secure sum. Usage of finite polynomials enhances scalability and Markov chain finds the required number of iterations. In [6] authors have proposed that in recent years, the number of mobile users in the society has risen dramatically. The privacy aware authentication scheme provides security and flexibility to the users to make use of various cloud services from various providers using a single private key. A bilinear pairing cryptosystem and nonce generation is used to enhance the security strength of the scheme. In addition to it, it also provides user intractability, mutual authentication, exchange of keys, anonymity and so on. This scheme reduces the memory space usage on the respective cloud service providers. The Smart card Generator serves as the key distributor for providers and mobile clients or users. Also, the scheme does not involve the SCG service in the user authentication procedure. It also reduces the processing time of the authentication process in terms of computation between providers and TTP. Formal Performance analysis tasks are conducted and the scheme is found to be efficient and secure. In [7] authors have suggested that due to the growing Security needs in the world the mentioned security algorithms have been surveyed and it is found that each has its own pros and cons. But, out of them AES algorithm is found to be efficient. Some of the Advantages are more secure, supports larger key size, faster in terms of hardware and software, 128-bit key size makes it less prone to attacks, suitable for cloud. Some of the Disadvantages of other algorithms are less secure, slow in terms of speed, small and medium key size. In [8] authors have suggested that due to the growth of cloud, security has become a vital part of cloud computing. Malicious activities and vulnerabilities are inevitable. The key purpose is to verify if AES provides better security than other algorithms. By implementing it, it is witnessed that it provides less memory consumption and computation time. Some of the Advantages are high performance, speedy key setup, key agility, less memory, instruction level parallelism, no cryptanalysis attacks have been proved. On comparing with other algorithms, AES eliminates weak keys, which is found is DES. During performance analysis it is found that AES has an advantage over other algorithms in terms of execution time [9]. Also over RC2, RC6 and blowfish with time consumption [10].

III. PROPOSED WORK

The existing security solutions generally concentrates over the authentication procedures which implies a user's private information cannot be accessed without proper authorization, while neglecting privacy issue during the data

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

sharing. During the information accessing, different users can be in a mutual relationship which stresses on the importance of knowledge sharing in order to attain better performance. Due to mentioned privacy issue, the user's private information could be revealed regardless the access permission being granted or not. In a cloud storage based supply chain management, there will be various interest groups in the system.

Each group has its own users who are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. For instance, consider two groups G1 and G2, if a user from G1 requests data from the user in G2, and if his request is rejected, the user's access desire will be revealed along with nothing obtained towards the desired data fields. A user may not send the access request or withdraw the unaccepted request in advance if he firmly knows that his request will be rejected. Therefore, it is unreasonable to thoroughly disclose a user's private information without any privacy considerations. In order to overcome the privacy issue "shared authority based privacy preserving authentication" protocol (SAPA) can be used for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. It Identifies a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority. And proposes an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism. Encryption techniques are used to provide authorized data sharing among multiple users. Shared authority is achieved by anonymous request matching mechanism without compromising the privacy. Also, attribute based access is used to allow only authorized users to request information and proxy re-encryption is applied by the cloud server to allow knowledge sharing among the multiple users. In order to witness the SAPA protocol we have developed a simple "e-library management system". And we have hosted this system on to the Azure cloud and have realized the efficient working of SAPA.

IV. PROPOSED METHODOLOGY

The architecture of the proposed system is shown in the figure 1.1, which depicts the users and the operations involved. The detailed description of the architecture is explained as follows,

A. *Administrator:*

The Admin is responsible for authorizing the user credentials and provide keys that are used for downloading the files that are uploaded by the librarian.

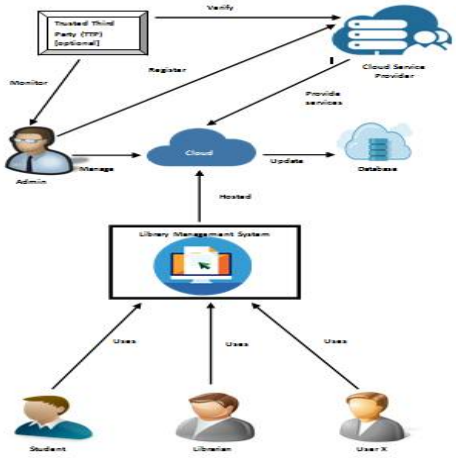

Fig. 1. System architecture

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

B. *User and Access Control:*

The User of the application could be a student or a librarian. A registered student can view his profile and request the books that he wants to use with the key that is given to him by the admin. Librarian on the other hand can accept or rejects the user requests and provide him with the required books.

C. *Cloud Service Provider:*

A Cloud Service provider is typically a company that offers certain cloud computing components like software, platform or infrastructure to an enterprise or individuals.

D. *Encryption and Decryption:*

The files that are uploaded and downloaded are encrypted and decrypted respectively using an encryption algorithm.

E. *File Upload and Download:*

The files are uploaded by the librarian in encrypted format and are downloaded only by the authorized students after decrypting.

F. *Trusted Third Party [Optional]:*

A TTP [Trusted Third Party] is a party who can monitor the data owner activities and files and can verify if the provider is authorized or not.

V. EXPERIMENTAL EVALUATION

The proposed system addresses the privacy issues faced by the legacy systems by using the "Shared Authority based Privacy preserving Authentication" protocol. It strives to identify the problem is cloud storage and solves it by not revealing the user's private information. This authentication protocol paves a way to achieve shared authority by anonymous access requests. And also uses encryption techniques based on the attributes to ensure security and reliability. The system is developed in ASP.Net using C# along with CSS, JavaScript and Html. MySQL 5.7 is used to store data in databases and also the application is hosted on to the Azure cloud. The working of the system is explained below,

A. *Student:*

A student is a registered user of the system. A user can register, in order to access the resources i.e. the e-books. And any other naive user will be allowed to log in without disclosing the user's privacy but, he cannot access any of the resources. A registered user can view his profile, available books and request them. Once he requests the book, the request is sent to the librarian and he has the right to approve the book with specified deadline, after which the book will expire and cannot be downloaded. Once the request is approved the book and the key are encrypted and the request details are recorded. The user can now view the book and download it as shown in Fig.2, during which the book is decrypted and keys are matched. Only if the keys are matched and date has not expired the user can download the book.

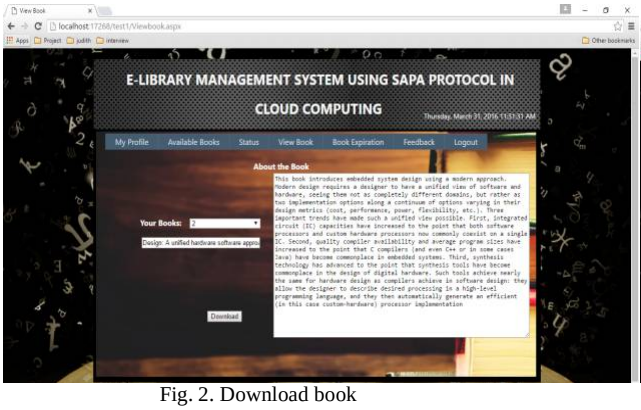

Fig. 2. Download book

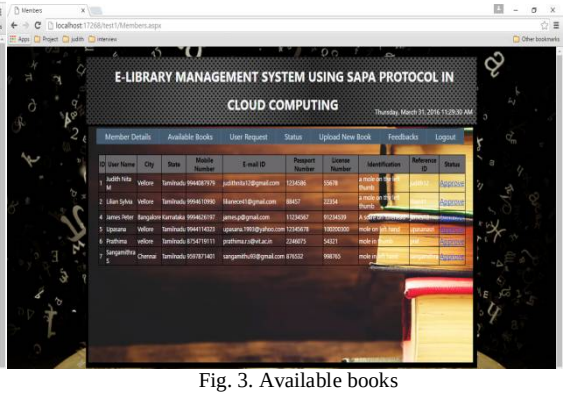

Fig. 3. Available books

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

B. *Librarian:*

The librarian uploads the e-books on to the system. And during each book upload a key is generated automatically and stored with which the book is encrypted. He also approves the user registrations and book requests as shown in Fig 3. He can also fix book expiration for each book so that they cannot be accessed after the stipulated time.

C. *Admin:*

Admin is responsible for monitoring and maintaining the database as in Fig 4. Also he is responsible for authenticating the users during login.

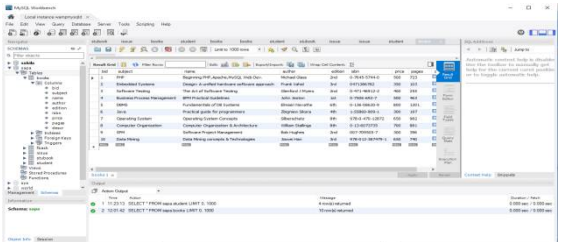

Fig. 4. Database

D. *AES algorithm:*

AES algorithm is the most popular and most used symmetric encryption algorithm. It is said to be six times faster than 3DES (Triple DES algorithm). Since the key size in DES was too small there was a need for a better replacement algorithm. It has increased computing power and it is vulnerable against attacks. 3DES was developed initially to overcome this shortcoming but it was slow. And so AES was developed [11]. Some of the features of AES are,

- Stronger and Quicker than 3DES
- Symmetric key and block cipher
- 128 bit data
- 128,192,256 bit keys
- Less prone to attacks

AES is an iterative cipher based on substitution permutation network. It consists of linked operations involving substitutions and permutations. All its operations are done on bytes instead of bits, which imply that 128 bits of plain text is considered as 16 bytes. These bytes are treated as a matrix with bytes ordered in four rows and columns. The number of rounds depends on the length of the key. Generally, it uses 10, 12 and 14 rounds for 128, 192 and 256-bit keys. Each round uses another 128 bit key that is calculated from original key [11]. In our work, we have randomly generated keys for each book. Those keys are encrypted using AES and stored in DB when a user requests a resource. When the resource is approved by the admin it is decrypted and the user is allowed to store in his local system.

E. *Cloud hosting:*

This digital library management system is hosted on to the Microsoft's Azure Cloud where it is available for the users. It is one of the most popular and widely used cloud hosting tools.

VI. PSEUDO CODE

Book Encryption Pseudo code

Step 1: Generate random key (bkey1) for each book.
Step 2: Encrypt each book with its corresponding bkey1.
Step 3: Encrypt the bkey2 again for each user request and store it in the database
Step 4: if (BookStatus==approved)
Decrypt the bkey2

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

```
        else
            Wait for admin to approve
        end
Step 5:  Match the bkey2 with bkey1
Step 6: if (bkey1==bkey2)
            Decrypt the book
      else
            Cannot download book
Step 7: End.
```

VII. CONCLUSION AND FUTURE WORK

In this paper, we have witnessed a new privacy issue during the access of data in the cloud which could be overcome by shared authority based privacy preserving protocol. The basic criteria for security are achieved using various concepts. Authentication is enforced in order to achieve data integrity and confidentiality. Privacy is enhanced by anonymous request matching mechanism that informs the cloud server regarding the access desires of the users. Forward security is witnessed by session identifiers in order to prevent correlation. Therefore, the proposed work implies that it can be used to enhance privacy in any applications on the cloud. The deployment of Trusted Third Party for enhanced security can be the future enhancement. Also, the performance could be monitored in order to ensure it is improved by efficient calculations and observations.

REFERENCES

[1] Mr. Ar. Arunachalam, Deepak Kumar and Atul Ranjan, 'Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing', COMPUSOFT, An international journal of advanced computer technology, Vol. 4, Issue 4, 2015.
[2] Security & Resilience in Governmental Clouds, 'www.enisa.europa.eu/act/rm/emerging-and-future risk/deliverables/security-and-resilience-ingovernmental-clouds', Accessed on: 14/02/2016.
[3] Madrid Resolution International Standards on the Protection of Personal Data and Privacy, 'www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/209_Madrid/estandares_resolucion_madrid_en.pdf', Accessed on: 02/04/2016
[4] Miranda M and S. Pearson, 'A Client-Based Privacy Manger for Cloud Computing', Proceedings of the 4th International ICST Conference on Communication and middleware, 2009.
[5] L. A. Dunning and R. Kresman, 'Privacy Preserving Data Sharing With Anonymous ID Assignment', IEEE Transactions on Information Forensics and Security, Vol. 8, Issue 2, pp. 402-413, 2013.
[6] Jia-Lun Tsai and Nai-Wei Lo, 'A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services', IEEE Systems Journal, Vol. 9, Issue 3, 2015.
[7] Gurpreet Singh and Supriya, 'A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security', International Journal of Computer Applications (0975 – 8887), Vol. 67, Issue 19, 2013.
[8] Abha Sachdev and Mohit Bhansali, 'Enhancing Cloud Computing Security using AES Algorithm', International Journal of Computer Applications (0975 – 8887), Vol. 67, Issue 9, 2013.
[9] Sanchez-Avila, and R. Sanchez-Reillol, 'The Rijndael block cipher (AES proposal): a comparison with DES', 35th International Carnahan Conference on IEEE, 2001.
[10] Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud, 'Performance Evaluation of Symmetric Encryption Algorithms', IJCSNS International Journal of Computer Science and Network Security, Vol.8, Issue 12, 2008.
[11] Advanced Encryption Algorithm, 'www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm' Accessed on: 12/02/2016

BIOGRAPHY

Judith Nita M is a Master degree student in the School of Information Technology and Engineering Department, VIT University, Vellore, TamilNadu, India. She received Bachelor of Computer Application (BCA) degree in 2010 from VIT University, Vellore, TamilNadu,, India. Her research interests are Data mining, Cloud computing and Web designing.

Rajaprabha M N is a Faculty in the School of Information Technology and Engineering Department, VIT University, Vellore, TamilNadu, India. She received her M.Tech(CSE), B.E(CSE) from Amrita Inst. of Tech & Sci. Her research interests are Cloud Computing and Data Mining.