Enhancing Cloud Security and Integrity byUsing multiple Encryption Algorithms and Stripping

Shelna Valsan K.P[1],Varshap[2]

[1]PG Scholar, Department of Computer Science & Engineering, Malabar Institute of Technology, Anjarakandy, Kannur (Dt), Kerala,India

[2]Faculty, Department of Computer Science & Engineering, Malabar Institute of Technology, Anjarakandy, Kannur (Dt), Kerala, India

Abstract: ***Cloud computing is the delivery of computing as a service rather than a product or service, whereby shared computing resources, software, and infrastructures are provided to computers and other devices as a utility like the electricity grid over a network typically the Internet. A cloud is a combination of hardware, networks, storage, and services that helps in delivering computing as a service. In Cloud computing technology there are a set of important issues, which include issues of privacy, security, reliability. But the most important between them is security and how cloud provider assures it. Cloud computing has several customers such as ordinary users, and enterprises who have different motivation to move to cloud. For enterprises the most important problem is also security but with different vision. This paper discusses about the Cipher Cloud. Cipher Cloud lets users keep their data confidentially on public cloud. To achieve this, the Cipher Cloud uses a two-step encryption process, in which all the data sent from a client to a cloud server or vice versa is kept totally encrypted and confidential. The thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures. This paper suggests unique encryption techniques, and also provide stripping technique in which data is segmented and stored in different locations (buckets/storage directories) in the cloud. Thus gives more security which is competitive and economical to private cloud models.***

Keywords: Cloud computing, Encryption algorithms, Data segmentation, Data stripping, Data security enhancement

1. Introduction

Cloud computing proposes new model for computing in information technology space. It provides allocation and reallocation of computing resources as and when necessary with click of a button, along with storage and networking capacity. It can satisfy the on demand needs of the user without any hassle and the process can be completely automated. It facilitates the sharable resources “as-a-service” model. For the business organization, the cloud offers flexible data centers to move their data globally. Cloud service models are categorized as Software as a Service better known as SaaS, Platform as a Service better-known as PaaS, Infrastructure as a Service better-known as IaaS. Thus we can use cloud application without necessarily installing it on the server/system. Cloud computing users work with data and applications that are often located on different servers located in securely distributed environment across geographic regions. However, many organizations are uncomfortable with the idea of having their data and applications on systems they do not have primary control. There is a lack of knowledge or understanding and legal regulations on how cloud computing impacts the confidentiality of data stored, processed and transmitted cross cloud servers. Cloud computing can be mainly split into three segments: "application" "storage" and "connectivity." Each part serves a different purpose and offers different products for organization. The services themselves together at high level have been referred to as Software as a Service (SaaS). There is an increasingly perceived vision that computing will one day be the 5th utility (mean necessity after water, electricity, gas and telephony). In order to accelerate the trend of ubiquitous computing, the web application frameworks are architected in public and hybrid cloud. The predominant problem associated with Cloud Computing are the information security challenges and the appropriate implementation of cloud over the communication networks.

2. Related Works

Cloud services make easier for users to access their personal information from databases or storage media which are globally accessible from any internet aware device. The high-availability and durability of such information in the cloud is crucial to provide better services to users and to authenticate users in case of services sensitive with respect to privacy and security. Users may have to typically establish their identity each time they use a new cloud service, we have to provide highly confidential information in order to secure their data. If it is not properly protected, there can be high probability of threat on the misuse of user identity information and data stored. Therefore, the development of a digital identity management (IdM for short) systems suitable for cloud computing is crucial. An important requirement is that users of cloud services must have control on which personal information is disclosed and how this information is used in order to minimize the risk of identity theft and fraud.

2.1 Preliminary Concept

Our approach, as many other approaches, assumes an IdM system that include several entities: namely Identity provider(IdP s), Cloud Service Provider (CSPs), users and registers. The CSPs provide access to data and software that reside on the Internet. IdPs can issue certified identity attributes to users and control the sharing of such information. Registrars are additional components that store and manage information related to identity attributes used in our multi-factor identity attribute verification approach. Note that, unlike the IdPs, the information stored at the Registrars does not include the values of the identity attributes in clear text form. Instead, the information only contains the cryptographic semantically secure commitments 1of the identity attributes which are then used by the clients to construct zero knowledge proofs of knowledge (ZKPK) 2of those attributes. The Registrar stores for each user an Identity Record (IdR) containing an identity tuple for each user's identity attribute m. And each identity tuple consists of a tag, with an attribute name, the Pedersen commitment of m, denoted asMi, the signature of the registrar on M, denoted by using σi.

2.2 Interoperable Multifactor authentication

Our multi-factor authentication protocol takes place between a client and a CSP and consists of two phases. In the first phase, the CSP matches the identity attributes in the client's vocabulary with its own attributes to help the client understand its identity verification policy. An identity verification policy consists of the set of identity attributes that the user must prove to know; if the values of these identity attributes are only needed for verification purposes but not for the execution of the service required by the client, the CSP has no reason to have to see these values in clear. In the second phase, the client executes the AgZKPK protocol to prove the CSP the knowledge of the matched identity attributes. Thus use of this protocol allows the client to convince the CSP and confirm that the client knows the values of the identity attributes without having to reveal to the CSP the values in clear.

2.3 The Protocol for identity Attribute Matching

Our attribute name matching technique uses a combination of look-up tables, dictionaries, and ontology mapping in order to address the different variations in identity attribute names. Syntactic variations refer to the use of different character combinations to denote the same term. An example is the use of ecommerce and e-commerce or e-com. Terminological variation from the linguistic perspective is the use of different terms to denote the same concept. An example of terminological variation is the use of the synonyms like Credit Card and Charge Card. The semantic variations are related to the use of two different concepts in different knowledge domains to denote the same term. Syntactic variations can be identified by using look up tables. A look up table enumerates the possible ways in which the same term can be written by using different character combinations. Terminological variations can be determined by the use of dictionaries or thesaurus such as Word Net. And, the semantic discrepancies can be solved by ontology matching technique. An ontology is a formal representation of a domain in terms of concepts and properties relating those concepts. Ontologies can be used to specify a domain of interest and reason about its concepts and properties. Ontology mapping is the process whereby the concepts of an ontology - the source ontology - are mapped onto the concepts of another ontology - the target ontology - according to those semantic relations

One of the most important issues related to the identity matching protocol is that which party has to execute the matching. In the recommended approach the matching is being performed by the CSP using server-side logic. Performing the matching on the client-side has the obvious drawback that the client may lie and asserts that an identity attribute referred to in the CSP policy matches one of its attribute, whereas this is not the case. The use of ZKPK protocols preserves the privacy of the user identity attributes by assuring that the CSP do not learn the values of these attributes; thus the CSP has no incentive to lie about the mapping. A second issue is how to take advantage of previous interactions that the client has performed with other CSPs. Addressing these kind of issues are crucial in order to make the interactions between clients and CSPs fast and convenient for the users. To address such issue, the matching protocol relies on the use of proof-of-identity certificates; these certificates encode the mapping between some of the user identity attributes and the identity attributes referred in the policies of CSPs with which the user has successfully carried out past interactionsencountered.

3. Proposed Model

In the proposed model, different encryption algorithms like RSA, AES, DES and Blowfish are used to ensure the security of data in the cloud. For the perspective requirements from different users, these algorithms are proposed. On top of it, the files which have to be stored into the cloud are segmented and kept in different buckets/folders in order to enhance security. The segmented files can be kept into different storage locations/zones based on the adopted public cloud model. The proposed model is validated in amazon public cloud, but can be implemented in any public, private or hybrid cloud infrastructure environment. DES algorithm was in use from early 1970s; Blowfish was developed in 1993by Bruce Schneier. AES was developed in 2001 by NIST. All these three algorithms use symmetric key, in which a single key is used for both encryption and decryption purposes. RSA is and asymmetric key algorithm which was developed in 1978by a group of cryptography scientists named Ron Rivest, Adi Shamir and Lenard Adleman. The algorithms are mainly in use for public key cryptography nowadays. In this solution, two set of public/private keys are used for encryption/decryption. There is an option for the users to choose any algorithm according to his/her need and accordingly encrypt/decrypt the data on cloud.

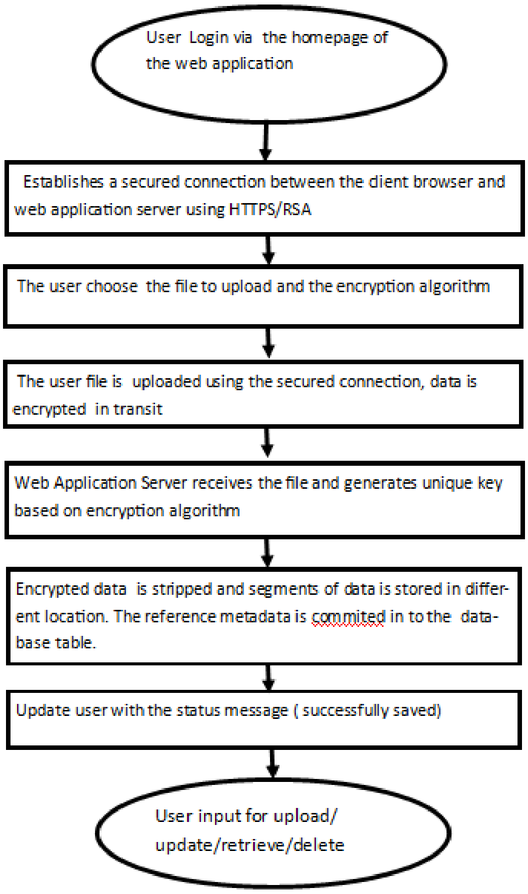
User Login via the homepage of the web application
Establishes a secured connection between the client browser and web application server using HTTPS/RSA
The user choose the file to upload and the encryption algorithm
The user file is uploaded using the secured connection, data is encrypted in transit
Web Application Server receives the file and generates unique key based on encryption algorithm
Encrypted data is stripped and segments of data is stored in different location. The reference metadata is commited in to the database table.
Update user with the status message (successfully saved)
User input for upload/ update/retrieve/delete

Figure 1: Proposed steps

Security Algorithms are
1. RSA Algorithm
2. DES Algorithm
3. AES Algorithm
4. Blowfish Algorithm

RSA Algorithm

Select two prime numbers.
Calculate n = p*q.
Calculate f (n) = (p-1) (q-1)
Select e such that e is relatively prime to f (n) and less than f (n).
Determine d so that decongruent modulo 1 (mod f (n)) and d<f (n).
Public key = {e, n}, Private Key = {d, n}
Cipher text c = message e mod n
Plain text p = cipher text d mod n

DES Algorithm

Triple DES uses a "key bundle" which comprises three DES keys, Key1, Key2 and Key3, each of 56 bits (exclude parity bits). The encryption algorithm is as below
Cipher text = EKey3 (DKey2 (EKey1 (plaintext)))
i.e., DES Encrypt with Key1, DES Decrypt with the Key2, then DES Encrypt with the Key3.
Decryption is the reverse:
Plain text = DK1 (EKey2(DKey3 (cipher text)))
Encryptor.
Each triple encryption encrypts one block 64 bits of data.

AES Algorithm

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule
2. Initial Round
2.1Add Round Key—each byte of the state is combined with the round key using bitwise xor
3. Rounds
3.1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
3.2. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
3.3. Mix Columns—a mixing operation which operates on the columns of the state, combine four bytes in each column.
3.4. Add Round Key
4. Final Round (no Mix Columns)
4.1. Sub Bytes
4.2. Shift Rows
4.3. Add Round Key

BLOWFISH Algorithm

Blowfish is a symmetric block cipher that can be effectively used for encryption. It will take variable length key, from 32 bitsup to 448 bits, making it ideal for securing data.Blowfish Algorithm uses Feistel Network, iterates a simple encryption function 16 times. Blowfish is a variable-length key block cipher . The block size is of 64 bits, and the key can be of any length up to 448 bit in size.. It is suitable for applications where the key does not change frequently, like a network communications link or an automatic file.
Blowfish has 16 rounds.
The input is a 64-bit data elementx.
Divide x into two 32-bit halves - xL and xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18.
Finally, recombine both xL and xR to create the ciphertext.

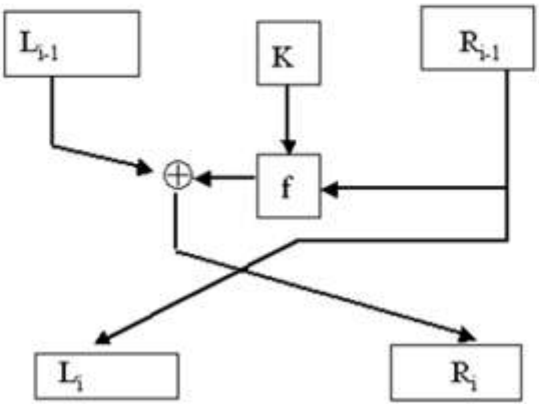

Figure 2: Fiestel network for blowfish algorithm

3.1Architectural Design

The registered user only can login to the system. After login users have many options like upload encrypted files, delete files, download files and update files. User can select the algorithm for encryption process. Once the user click on upload button, the file gets transferred to Cipher Cloud via an encrypted connection using HTTPS and then decrypted on the server side using private SSL key. Immediately after that it is again encrypted using a symmetric key algorithm selected by the user. Before storing into the media/secondary storage, data is segmented by using stripping algorithm and each segments of data is stored into separate bucket/folders to enhance security. Hence the Cloud Cipher framework is able to save the data in its encrypted form, and even retrieve it in its original form seamlessly and by using minimum possible CPU usage.

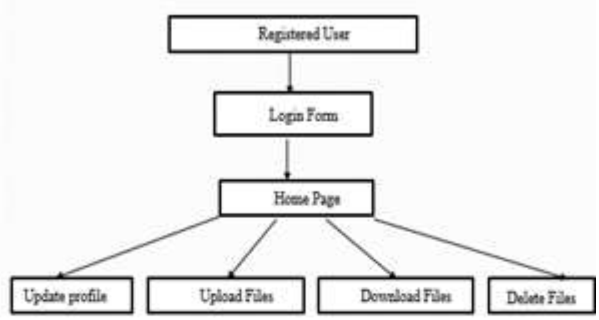

Figure 3: Architectural design for proposed system

4. Advantages of Proposed method

In the proposed system data is encrypted with user selected encryption method and the encrypted data is stripped and the segments are stored into different locations/buckets for enhanced security. Encryption is done with secured symmetric or asymmetric encryption algorithms. Compared with the existing systems this solution gives more security and flexibility on data for permission from the user to create a new account using the Google/Facebook account he/she had logged in the browser. Once the user is authenticated and login, user is presented with a landing page. It is on this page that the user has been offered with a choice of the algorithm that he/she wishes to use for this particular account. The algorithm once selected cannot be changed. There are four algorithms storage facility. Segmentation of data provides an enhanced level of security control over the encrypted data.

5. Conclusion

This will show the look and feel of Cipher Cloud and also show how implanting the encryption standards have increased the security of cloud storage. Here three concepts were distilled how data is issued, where data is located in relation to data owner and how data is protected. Cypher cloud encrypts data making ownership exclusives to its owner Then user login to the cloud with his or her id and password. After entering to the cloud user can see the contents of his or her account. In this user has following options: Download files, Uploading files, Delete files and update profile. Once the user click on the upload button, the file gets transferred to Cipher Cloud via an encrypted connection using HTTPS. It is encrypted by using the symmetric key algorithm selected by the user. Data is segmented into two parts and are stored into two different places. Time at which data is stored is taken as the key and the same key is used to retrieve the data. Once the file is uploaded and saved in encrypted form, it can then be downloaded by the user using the download button. The file retrieved by this method will be in its decrypted form. User will be shown a link to open his/her account. Then user can upload, update or retrieve the encrypted files in his/her account. In case the user is new, Cipher Cloud asks that are used for the security of the data. User would be able to select the algorithm according to his/her choice, means choose algorithm according to his/her data. If message is small then RSA algorithm is preferred and for large message AES algorithm is naturally preferred.

References

[1] Andrzejak. 2010, Exploiting Non-Dedicated Resources for Cloud Computing ,In Proceedings of 12th IEEE/IFIP Network Operations & Management Symposium(NOMS 2010),Osaka Japan)

[2] Bertino, R. Ferrini 2009, Privacy- Preserving Digital Identity Management for Cloud Computing vol.32-No.2, IEEE Data Eng. Bull I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[3] D L. Ponemon 2010, Security of Cloud Computing Users, vol. 34-No. 2, International Journal of Computer Theory and Engineering R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] Dawson 2002, Maximizing sharing of protected information,journal of computer and system science.

[5] Pieters, W. 2006, Acceptance of Voting Technology: Between Confidence and Trust. In K. Stolen (Eds.), I Trust., Computer science press.

[6] Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.