Advances in Computer Science and its Applications
Vol. 1, No. 1, March 2012

www.worldsciencepublisher.org

Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography

M.Sudha[1] , M.Monica[2]

[1] Assistant Professor Senior, School of Information Technology & Engineering, VIT University, India
[2] Assistant Professor, School of Computing Sciences &Engineering, VIT University, India

Email: msudha@vit.ac.in , monica.m@vit.ac.in

Abstract – Increasing demand for cloud applications has led to an ever growing need for security mechanisms. Cloud computing is a technique to leverage on distributed computing resources one do not own using internet facility in pay per use strategy on demand. A user can access cloud services as a utility service and begin to use them almost instantly. These features that make cloud computing so flexible with the fact that services are accessible any where any time lead to several potential risks. The most serious concerns are the possibility of lack of confidentiality, integrity and authentication among the cloud users and service providers. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication. In our model symmetric and asymmetric cryptographic algorithms are adopted for the optimization of data security in cloud computing.

Keywords – Symmetric Encryption; Public key Cryptosystem; Cloud computing; Data security.

1. Introduction

Cloud computing is an innovative technology that facilitates the networked nodes to share the pooled resources on demand in pay per use model. Resources could be a simple software application, a platform needed for project development or the infrastructure itself using Internet as the backbone. Cloud computing is highly scalable, dynamic and easily configurable more over it can handle multitenant request simultaneously. Any user who has a PC, Laptop with Internet facility can acquire the cloud source according to the service provider's policies and norms at any time without any prerequisites , this nature of computing opens several security breaches and vulnerabilities to the cloud environment. The flexibility that allows many users to make use of the cloud leads to various network and information security risks, in cloud environment mostly client data's are moved on to the data centers that are distributed across the network that is data resides in the physical storage of the service providers therefore an enterprisers or user data's are under the service providers concern which paves for unexpected security attacks and vulnerabilities when it is uploaded and offloaded to and from the cloud data centers. However some of the basic requirements for the cloud users need broadband internet connectivity. Cloud users vary broadly it could be an IT enterprise that request for "Super Computing facility" therefore its requirement includes several high performance servers, a cloud client could be an application developer or a user who need to access Amazon's EC2 facility for e-billing etc. cloud service provider facilitates different types of service and deployment models. Some of the widely adopted service models are software as service, platform as service, infrastructure as service, database as service, storage as service and testing as Service. The basic cloud usage models are Private cloud, Public cloud, Hybrid cloud and Commodity cloud. Cloud technology is very dynamic, adaptable, scalable and easily accessible this flexible nature of cloud paves some severe drawbacks in terms of data security and it challenging to deduce a mechanism enabling secure data sharing. One of the suitable solutions for this problem is to follow an authenticated data centric approach rather than using communication centric approach.

Security is broadly categorized as two types protecting the asset and protecting the data in our research the main focus is on data protection the research paper is organized as follows. Problem stated in section 2, existing related works are described in section 3. Section 3 gives a simplified problem statement. Section 4 introduces some important characteristics and building blocks of cloud computing systems. Section 5 presents our system model based on cryptographic techniques in detail. Section 6 describes the implementation steps, simulation results and the evaluation. Section 7 summarises our conclusions and points out future work.

2. Problem Analysis

Information security is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in any data centre across the network geographically distributed. So the nature of cloud computing raises serious issues regarding user authentication, information integrity and confidentiality. Hence it is proposed to implement a enhanced novel secure security algorithm in order optimize the information security ensuring CIA – Confidentiality, Integrity and Authentication while storing and accessing the data from and to data centers and also in peer interactions.

3. Related Works

In [4] they have addressed the security issues associated in cloud data storage and have explored many security issues, whenever a data vulnerability is perceived during the storage process a precision verification across the distributed servers are ensured by simultaneous identification of the misbehaving nodes through analysis in term of security malfunctioning, it is proved that their scheme is effective to handle certain failures, malicious data modification attack, and even server colluding attacks. This new technology opens up a lot of new security issues leading to unexpected challenges which is of dominant importance as security is still in its infancy now many research problems are yet to be solved and identified.

Security Content Automation Protocol (SCAP) and the benefits it can provide to cloud and tools for system security such as patch management and vulnerability management software, use proprietary formats, nomenclatures; measurements, terminology and content. Mentioned that the lack of interoperability causes delays in security assessment was addressed in [6]

It has been described in [7] about the overview of privacy issues within cloud computing and a detailed analysis on privacy threat based on different type of cloud scenario was explained, the level of threat seem to vary according to the application area. Their work has stated the basic guidelines for software engineers when designing cloud services in particular to ensure that privacy are not mitigated. The major focus of their schemes rests on the privacy risks, analysis on privacy threats, privacy design patterns and accountability with in cloud computing scenario.

In [8] it clearly stated about the issues associated in choosing a security mechanisms or security frameworks in the Cloud computing context and given a brief outline on flooding attacks. Also they have given an idea about, the threats, their potential impact and relevance to real-world cloud environment. It is well understood from their investigation, a significant pace for improving data security in cloud is to initial intensification of the security competence of both web applications and frameworks.

4. Cloud Framework

Cloud computing deployment model is the one that enables the consumers to choose the applications, platforms and other services for their requirement and for provisioning smooth flow of business interactions. According to the above mentioned business scenarios cloud service providers provide the cloud in following deployment models as in Figure1.

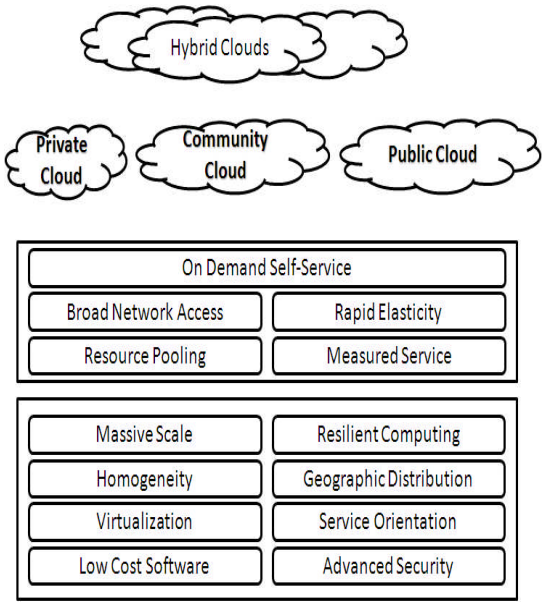

Figure 1. Cloud Framework

Private Cloud: It is for the business where the infrastructure requirement is more and therefore the enterprise need to own datacenter, servers to listen client request, to handle data storage and management. Therefore a private cloud model is for provisioning cloud service among the specific set of enterprises, business partner for their own employees or their clients.

Public Cloud: Is a cloud environment where a client or a user can acquire the cloud recourses using a web application like a web browser or a web API without any limitation, a user could be an independent client or an employee of an enterprise and so on. Some of the popular public cloud service providers are Amazon, Google etc.

Commodity Cloud: This deployment model is for specific set of users, group of agreed upon business enterprises sharing the agreed cloud facilities and infrastructure like sharing security policy regulations compliance with set of similar SLAs.

Hybrid Cloud- It is a combination of above mentioned deployment models, for example a private cloud user accessing a public cloud for addition requirements via a secured path.

5. Proposed System Model

Figure 2. Secure Hybrid Framework (SHF)

The proposed enhanced security framework is an efficient security framework that incorporates the various security preserving cryptographic techniques. In our model we have employed a two step authentication process one is the login password authentication mechanism which is an usually adopted scenario for user authentication at the server end for data access in a simple two or three tired client server architecture, with this in our authentication phase of this secure hybrid algorithm we have integrated an addition digital fingerprint mechanism to enhance the authentication process which is implemented using RSA for digital fingerprint generation and validation at the sender and receiver end and to overcome the following password vulnerabilities such as man in the middle attack, data hijacking, compromising of account attack , user password attack, password guessing against multitenant user, workstation hijacking, make use of user mistakes while registration, denial of service attacks.

We have considered data access as well data sharing between the client and data center in cloud as a simplified Client-Server interaction in cloud and also the interaction between the peers. In case of peer interaction it is advocated to use simple two stage authentication instead of the login verification mechanism as in cloud service provider and cloud client interaction. Essential criteria to be considered in an encryption algorithm implementation is the computational speed of the algorithms and the tradeoffs between the performance and speed, public key algorithms are take more computationally time for its key generation process etc thereby the speed become comparatively low than symmetric key algorithms like AES, it is good practice to encrypt the actual message to be transmitted using a Symmetric key algorithm with better computational speed for cloud environment especially , therefore in our model AES is adopted e.g. if one wants to transmit the message "Hello World of Digital Signatures", then first encrypt this message using a symmetric key, say an 128 bit AES key like x7oFaHSPnWxEMiZE/0qYrg and then encrypt this key using an asymmetric key algorithm like RSA.

RSA a public key algorithm is used for both simple key distribution and to send data between the cloud users in encrypted message format without a separate exchange of secret keys for decryption at other end. A brief introduction for the RSA Algorithm is included to understand the basic implementation model. It complements itself with minimal network complexity.

5.1 RSA Algorithm

RSA algorithm was introduced by Rivest, Shamir & Adleman of MIT; RSA is an extensively used public key crypto mechanism it is based on exponentiation in a finite field over integers modulo a prime numbers. To encrypt a message M the sender has to obtain public key of recipient PU={e,n} to compute the cipher: $C = M^e \bmod n$, where $0 \leq M < n$ and similarly for decryption the recipient uses their private key PR={d,n} and computes: $M = C^d \bmod n$ it is important that the message M must be smaller than the modulus n (block if needed).How it works , RSA uses Euler's Theorem: $a^{\phi(n)} \bmod n = 1$ where gcd(a,n)=1 in RSA we have to initially calculate n=p.q such that ø(n)=(p-1)(q-1) one has to carefully chose e & d to be inverses mod ø(n) . **Key Generation**-RSA must determine two primes at random - p, q next is to select either e or d and compute the other primes p,q must not be easily derived from modulus n=p.q means must be sufficiently large and use probabilistic test exponents e, d are inverses, so use Inverse algorithm to compute at the other end.

5.2 AES Algorithm

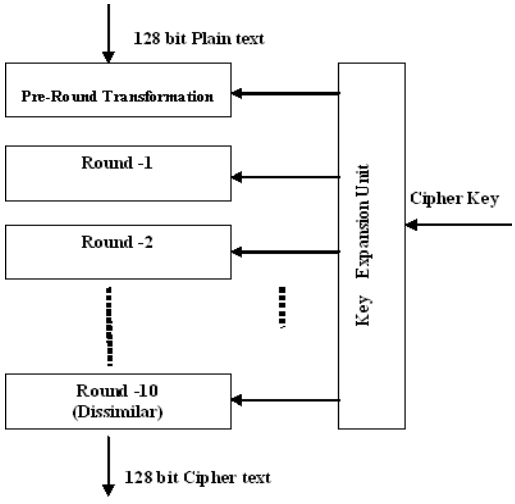

Figure 3. AES (Rijndael) Algorithm

a) Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule

b) Initial Round
AddRoundKey - each byte of the state is combined with the round key using bitwise xor

c) Rounds
1. SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. ShiftRows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
3. MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

d) Final Round (no MixColumns)
1. SubBytes
2. ShiftRows
3. AddRoundKey

e) Key generation
This module handles key generation by the server side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. [1] this key is then transferred to the cloud client via the LAN Wi-Fi connection which receives and stores a copy for it for decrypting purpose. The key is a 16 byte or a 128 bit key. An Example of a
key generated is: 8xRER4LyFiU3Hs9a40xExQ==
After the key generation and encryption, the cipher text is sent to the client, the client uses the reverse process of the AES encryption. Decryption to obtain the original plaintext that was transferred by the server.Hence the client receives the intended file in a secure manner over the LAN.

5.3 SHA Algorithm

Secure Hash Algorithm converts an arbitrary size message to fixed size message digest or a hash code by processing message in blocks through some compression function either custom or block cipher based mode. Hash function can be applied to any sized message M and it produces fixed-length output h .therefore it is easy to compute**.**

In our model for enhanced authentication the hash value of the message i.e. a message digest is generated using secure hash algorithm which is of constant size for any arbitrary length of data is concatenated with the digital signature and the encrypted actual data as a string and the entire concatenated string is encrypted using the public key of the receiver and sent to that intended requesting recipient in the cloud therefore the deciphered message later used to generate the message digest (hash value) in turn by the secure hash algorithm for data integrity verification and digital finger print validated using RSA algorithm as conformance for the sender's authentication.

h= H (M) for any message M,
Given h is infeasible to find x s.t.
H(x) =h one-way property
Given x is infeasible to find y s.t. H(y) = H(x) , Also it is infeasible to find any x, y s.t. H(y) = H(x)

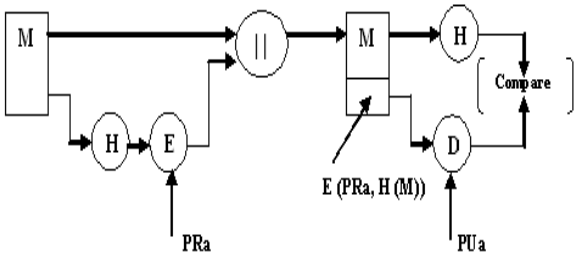

Figure 2. Digital signature using RSA approach

6. Proposed security framework

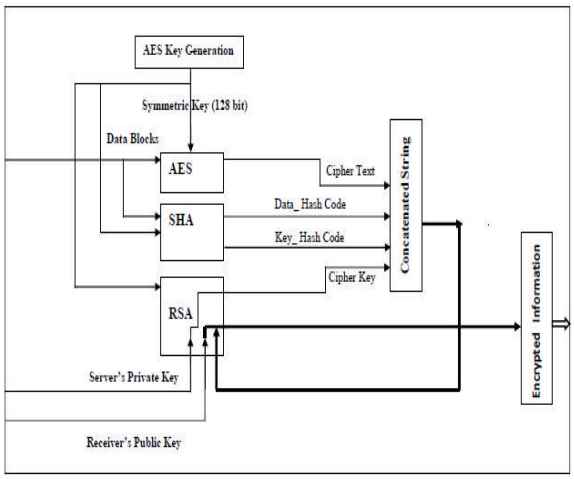

Figure 3. Proposed Secure Hybrid Framework

In this scenario we have consider cloud client and the cloud servers interaction as initial step the user has to be an registered cloud client, if he is a registered user the login password verification will be performed if not the client has to first register with the service provider and the Certificate Authority is an agent software that generates the certificate for the cloud client. After user login authentication the next level is a simple random string is generated by the server for the intended client and the digital signature is generated by signing the random string using the client private key which will be exchanged with the peer client during the interaction and by the server for enhanced authentication.

Following the two step authentication when the user requests for data from the cloud data center the following steps are executed according to the proposed secure hybrid framework which could ensure information security with minimal infrastructural requirements using symmetric key for efficient confidentiality and simplicity, as well public key cryptosystems for ease of key exchange, the hybrid construct of symmetric and asymmetric crypto have enhanced the framework as a robust mechanism.

Step 1: Upon successful server authentication process, the data is encrypted using the symmetric (AES) algorithm to generate the cipher text.

Step 2: symmetric key used for cipher generation, hash code of symmetric key, original message and the cipher are concatenated to form a string.

Step 3: Concatenated string is encrypted using the receivers (RSA) public key; this key can be accessed from an authenticated (CA) Certificate Authority for simplicity CA is implemented in server itself.

Step 4: Apply the reverse process; the received message is decrypted using recipient private key and the required symmetric key is generated at the next level of encryption process using server public key.

Step 5: Actual message is decrypted using symmetric encryption algorithm (AES) key, then the verification and validation of the sender is implemented.

Step 6: Compute hash value of data using Secure Hash Algorithm (SHA) for checking the integrity of the sent message.

Step 7: If the generated hash value of the message matches the hash code sent then data integrity is accepted, digital signature is also validated.

Step 8: Server on receipt of commit request from the intended recipient to commit its transaction the server commits and terminates the session. The following test cases were generated and evaluated

Test Case 1: *To verify status of nodes in the cloud*: we need to verify if it's running properly and ready to be used in the cloud infrastructure. We do this by checking its status using the ping command in console.

Test Case 2:*To Verify status of cloud Server Node and the Datacenter node*: After the registering of client nodes and we check the set-up of cloud for the desired interaction, we need to verify if it is working properly and all the nodes are validated to be registered in the cloud.

Test Case 3: On the successful set-up of cloud, client, server and the desired computer system, this client is required to be registered and verified properly by the cloud server using the two step authentication process and the status of the cloud client is updated on authentication data center access is granted to the client for successful execution of applications on cloud.

Network Support and Technology Specific Tools

This model can be used to run on both Wireless and LAN networks. It supports following network architectures. Local Area Network (using network cables, Wireless Network (Wi-Fi), Ad-Hoc Network, Dial-up or VPN network to a workplace. In this work we use following tools: Java Development Kit - jdk1.6.0_02, Java Runtime Environment - jre1.6.0_06.
Java.awt package for layout of the applet .we have utilized Java.net package for connection settings, message passing, Socket Options interface of methods to get or set socket options.

Authentication of Client

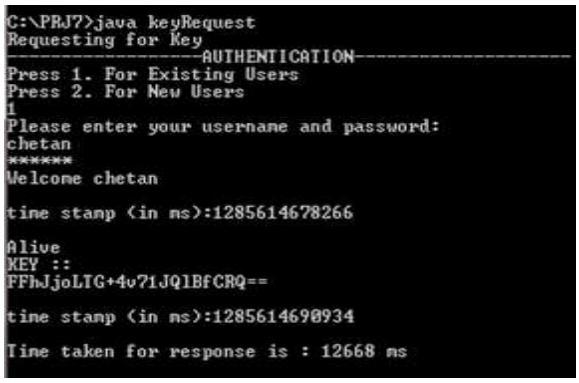

Figure 5. Client Authentication

After one step Authentication, the Key is requested for the next level authentication process to check the digital signature received.

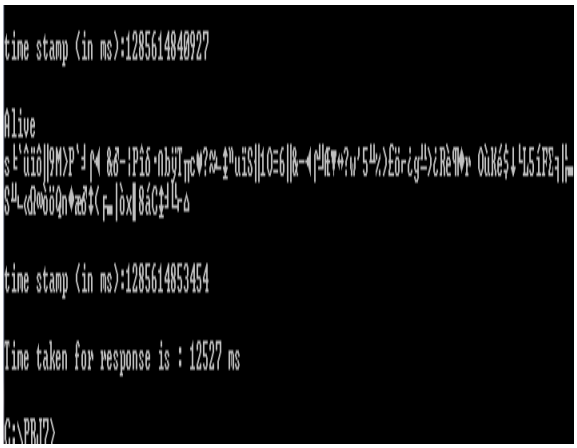

Figure 6. Authetication for Data Access

Data Confidentiality Check-Actually the data is encrypted before sending it to the network, therefore the recipient message confidentiality is preserved, now upon the receipt of the cipher the user now uses the key to decrypt the message as follows to get the readable message as shown below in the figure.

Random Message

Now the received deciphered message is used to genertae the message digest to verfiy the data integrity using the secure hash algorithm.

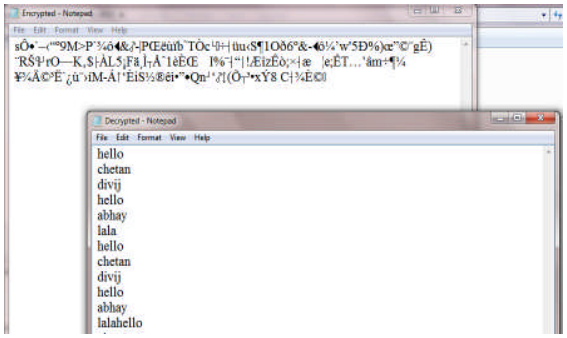

Figure 7. Sample_Encrypted Message

Thus in our hybrid model an user is gauranteed an expected level of *confidentiality, integrity and authentication (CIA)* properties as stated in Quality for Security Services model (QOSS) with minimal network overhead for handling these cryptographic techniques.

7. Conclusion

In this paper, a simple security framework using cryptographic algorithm the data protection is optimized by incorporating both public and private key cryptosystems for various cloud applications; we have examined the performance and have verified the test cases of our model in the a simple cloud setup. We have achieved enhanced data *security* using AES, RSA and SHA algorithm with the minimal cost and effort in; Simulation results on utilizing this strategy in both general (random) and specific application indicate that our strategy is efficient, scalable and cost-effective for simple data access/sharing application.

References

[1] M.Sudha and M.Monica "A Comprehensive Framework for Data Protection in Network Centric Cloud Applications", International Journal of Computer Applications (IJCA), Volume 12, Number.8 December 2010, Pages 19-23.

[2] M.sudha and M.Monica "A Simplified Network manager for Grid and Presenting the Grid as a Computation Providing Cloud",International Journal of Advanced Research in Computer Science (IJARCS), Volume 01, Number 03, October 2010, Pages 173-176.

[3] M.sudha and M.Monica "Investigation on Efficient Management of Workflows in Cloud Computing Environment", International Journal of Computer Science and Engineering (IJCSE), Volume 02, Number 05, August 2010, Pages 1841-1845.

[4] Cong Wang, Qian Wang and Kui Ren,"Ensuring Data Storage Security in Cloud computing" 978-1- 4244 -3876-1/2009 IEEE

[5] Lijun Mei, W.K.Chan, T.H.Tse, "A Tale of Clouds: Paradigm comparisons and some thoughts on research issues", 2008 IEEE Asia-Pacific Services Computing Conference

[6] John Harauz, Lori M. Kaufman, Bruce Potter, "Data security in the world of cloud computing", 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[7] Siani Pearson" Taking account of Privacy when Designing Cloud computing Services *CLOUD'09*, May 23, 2009, Vancouver, Canada ¸2009 IEEE

[8] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society

[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.Atanu Rakshit, "Cloud security Issues"2009, IEEE.

[9] Guy Bunker, Farnam Jahanian, Aad van Moorsel, Joseph Weinman," Dependability in the cloud: Challenges and opportunities", IEEE 2009

[10] Lizhe Wang, Jie Tao, Marcel Kunze , Alvaro Canales Castellanos, David Kramer, Wolfgang Karl "scientific Cloud computing: early Definition and Experience", 2008 IEEE

[11] Ivona Brandic" Towards Self manageable Cloud services" 0730-3157/09, 2009 IEEE

[12] www.cloudsecurity.org, accessed on April 10, 2009.

[13] Iuon-Chang Lin and Hsing-Lei Wang, "An Improved Digital Signature Scheme with Fault Tolerance in RSA" 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

[14] Book: "Cryptography and Network security" by William Stallings, 5e -Pearson education publications.