ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

Centralized Database Security in Cloud

Leena, Miss A.Kakoli rao

Department of Computer Science, Galgotia college of Engineering, Greater Noida , India

ABSTRACT: Data Security and Access Control is an exigent work in the environment of Cloud Computing. The users upload the personal and classified data over the cloud. Security is mandatory for such type of outsourced data, so that users are confident while processing their private and confidential data. Modern technology suffers from computational problem of keys and there exchange. This paper emphasizes the different problems and issues that arise while using cloud services such as key generation, data security and authentication. The paper addresses these problems using access control technique which ensures that only the valid users can access there data. It proposes a RSA Key Exchange Protocol between cloud service provider and the user for secretly sharing a symmetric key for the secure data access that solves the problem of key distribution and management. The Authentication will be done using Two Factor Authentication Technique with the help of key generated using TORDES algorithm. The proposed work done using Cloud is highly efficient and secure in the existing security models.

Keywords: Cloud computing, Data security, public key cryptosystem, Symmetric encryption

I. INTRODUCTION

1.1Cloud computing

Cloud computing is defined by the National Institute of Standards and Technology (NIST)2 as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management e ffort or service provider interaction. Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for agencies which are migrating applications to a cloud environment. cloud deployment models as follows:

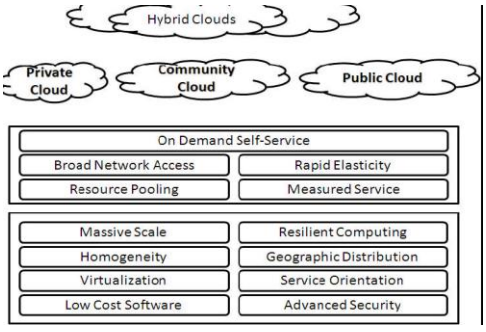

Figure1: cloud model

• *Private cloud.* The cloud infrastructure is operated exclusively for an organization. It may be managed by the organization itself or by third party which can be executed in the premise or off premise.

•*Community cloud.* The cloud infrastructure is managed by several organizations. It may be managed by the organization itself or by third party which can be executed in the premise or off premise.

•*Public cloud.* The cloud infrastructure is open for general public or a large industry group and can be owned by an organization by acquiring cloud services.

•*Hybrid cloud*. The cloud infrastructure is a combination of more than one clouds (i.e. private, community, or public) which always remain single entities but are bound together by standardized technology that enables data and application portability (eg, cloud bursting for load-balancing between clouds).

Cloud computing can also categorized into service models.

•*Software as a Service (SaaS).* User can only access the applications running on the cloud. This application can be accessible through various client interfaces like web browser. In the process user don't have the access of management console due to which as a user you cannot manage or control the base of infrastructure like network, server, operating systems, storage or other capabilities. Users have some limited

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

user specific configuration setting with respect to application.

•*Platform as a Service (PaaS)*. One of the facilities given to the user is to deploy any of the application on the infrastructure which will be created using programming language and the tool supported by the user. In this user cannot manage or control base of infrastructure like network, server, operating systems, storage but on same time has control over deployed application and possibly application hosting configurations.

•*Infrastructure as a Service (IaaS).* In this one functionality is provided to the user which is storage, networks and other fundamental computing resources where user can deploy and run random software which can be some application or operating system. In this user has control over operation system, application which is deployed, storage and limited control on networking components like firewall etc.

Cloud is vibrant, flexible and easily avaliable due to all this nature some severe drawback comes in picture in terms of data security which cause challenge in secure data sharing. To overcome from this issue we can follow an authenticated based approach rather than communication based approach. In broad manner security is categorized in two types - data protection and asset protection. In this research paper the main focus is on data protection. Section 2 of this paper state the issue and section 3 show related work. Section 3 gives a simplified problem 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 summaries our conclusions and points out future work.

II. 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 the world aur any data centre across the network geographically distributed. So the nature of cloud computing raises serious issues regarding user authentication, information integrity and data 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.

III. 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

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

security competence of both web applications and frameworks.

IV PROPOSED SYSTEM MODEL

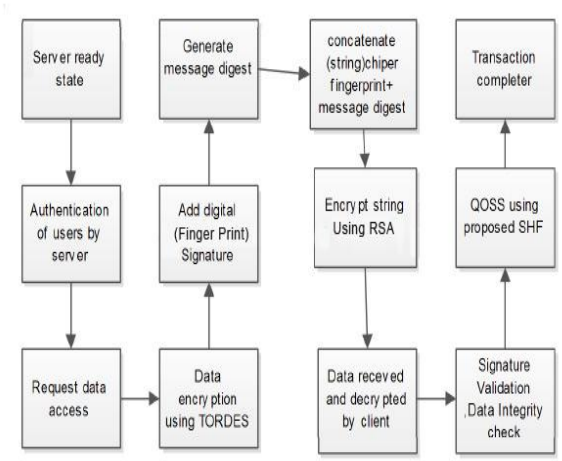

Figure 2. Secure Hybrid Framework (SHF)

In cloud computing the data and applications exist on a"cloud" of Web servers. When talking about a cloud computing system, it's helpful to divide it into two sections: the front end and the back end. The front end is the side the computer user, or client, sees. The backend of the system is the various computers, servers and data storage systems that create the "cloud" of computing services. They connect to each other through a network, usually the internet. All cloud computing systems don't have the same user interface. All servers are run with its own independent operating system. In theory; a cloud computing system could include practically any computer program, from data processing to E mail. Usually, each application will have its own server. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly .A cloud computing system must make a copy of all its clients' information and store it on other devices. These copies are enabling to the central server to access backup machines to retrieve data. The applications of cloud computing are practically limitless. Clients would be able to access their applications and data from anywhere at any time. The client access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network. The biggest concerns about cloud computing are security and privacy. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing will need to find ways to protect client privacy. One way is to use authentication techniques such as user names and passwords. Another is to employ an authorization format -- each user can access only the data and applications relevant to his or her job. Cloud has centralized server administration system Centralized server administers the system, balances client supply, adjusts demands, monitors traffic Here, all the data are backed up at multiple locations. In cloud computing, it is very common to store data of multiple customers at one common location. Over proposed security frame work should have provide proper techniques for data security and confidentiality. 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

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

become comparatively low than symmetric key algorithms like TORDES, 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 TORDES is adopted. 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.

V. TORDES ALGORITHM

TORDES is a block cipher algorithm (Bhushan et al., 2012) and unique independent approach which uses several computational steps along with string of operators and randomized delimiter selections by using some suitable mathematical logic. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message with limited size. It also protects the cipher text from attacks like Brute-force like attack because it is fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys

VI. 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 = Me mod n, where 0≤M<n and similarly for decryption the recipient uses their private key PR={d,n} and computes: M = Cd mod 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: aø(n)mod 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.

VII. PROPOSED SECURITY FRAMEWORK

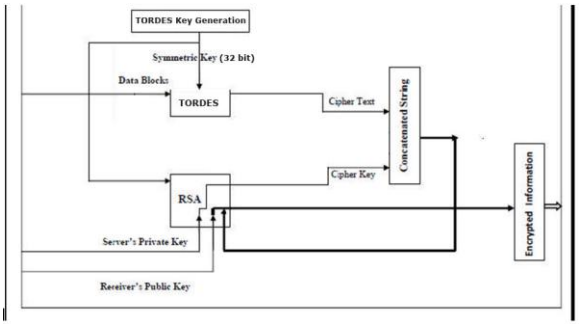

Figure 3.security framework

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.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

Step 1: Upon successful server authentication process, the data is encrypted using the symmetric TORDES 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 (TORDES) 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: 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
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.

VIII. 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 TORDES, RSA 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] **W**. Stallings "Cryptography and network security principles and practice," Fourth edition, Prentice hall, 2007
[2] Gope, P., Ghosh, D., Chelluri, A.R.K. and Chattopadhyay,P., 2009. Multi Operator Delimiter based Data Encryption Standard (MODDES). ICCNT. Chennai,India, June 27 – 29. 2009.
[3] Gope, P., Kaushik, A., Arora, K. and Kumar, N.,2010. XMODDES (Extended Multi Operator Delimiter Based Data Encryption Standard, Proceedings of the 2nd International Conference on future Networks (ICFN) 2010, China, March, 2010, pp 399-403.
[4] NIST, "Advanced Encryption Standard Call", NIST, 1997.
[5] Bhushan , A., 2012. Transform Operator Random Generator Delimiter based Encryption Standard (TORDES). CCIT2012, Iraq.
[6] National Bureau of standards-Data encryption Standard.
[7] FIPS Publications, 46. 1997.
[8] Tanenbaum, A. S., 2004. *Computer Networks*. New Delhi, Prentice Hall Inc.
[9] Charles, P.P. and Shari, P.L., 2008. *Security in Computing*: [10]4th edition,Prentice-Hall, lnc.
[11] Jing, F. and Xian Z., 2009. Data Encryption by Two Keys. [12]NIST data for DES
[12] Bhushan , A., 2012. TORDES a new symmetry key algorithm IJRS ,2012.
[13] 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.
[14] 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.
[15] 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.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

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

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

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

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