Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.1086 – 1091

RESEARCH ARTICLE

A Layered Signcryption Model for Secure Cloud System Communication

Shilpa Kukreja[1]

Student, M.Tech, Dept. Of Computer Science & Engineering.,VCE, Rohtak, Haryana[1]

Shilpakukreja1@gmail.com

Sunil Maggu[2]

Professor, Computer Science & Engineering, VCE, Rohtak, Haryana[2]

sunilmaggu04@gmail.com

Abstract— Cloud system provides the public and private services in distributed environment with inclusive system repository. This model requires the reliable and secure authentication model under signcryption technique. The presented model is here divided in three stages. In first stage, user authentication key is generated using signcryption technique. This technique is based on symmetric key and hash key map. Once the key is generated, the secure key exchange model is defined for public environment using certificate verification. In final stage, the session based key block encoding is defined for secure communication in cloud environment.

Keywords— Signcryption, Security, Encryption, Message Digest, Server

I. INTRODUCTION

Signcryption is having the significance to reduce the encoding weight applied on large information set. In this method, instead of applying the encryption on all information, signature adaptive mapping is performed. Signcryption is adaptive to provide the information encoding in various online and offline application. In this work, cloud system security is provided under signcryption standard. Signcryption itself is able to provide complete security solution that will provide the information encoding and authentication in an integrated form. It is able to provide the communication against under active and passive attacks on cloud system. As the cloud system provides the public and private communication. Most of the security problems in cloud system environment are during the transmission of information as well as while verifying the communicating users. In this work, secure cloud system architecture is provided under signcryption model to provide secure communication in public and shared environment. Signcryption model is able to change the information form so that the privacy and the authenticity of secure system will be improved. The electronic communication via cloud environment includes various sensitive and dedicated information contents such as emails, ecommerce data, FTP information contents, passwords, money transactions etc. It also involves various social activities that require to keep large information contents as the shared system. Today each user wants a separate web space, secure information area or digital locker to keep the secure information in it. These social activities under shared phenomenon is provided by cloud server. This signcryption model is shown in figure 1.

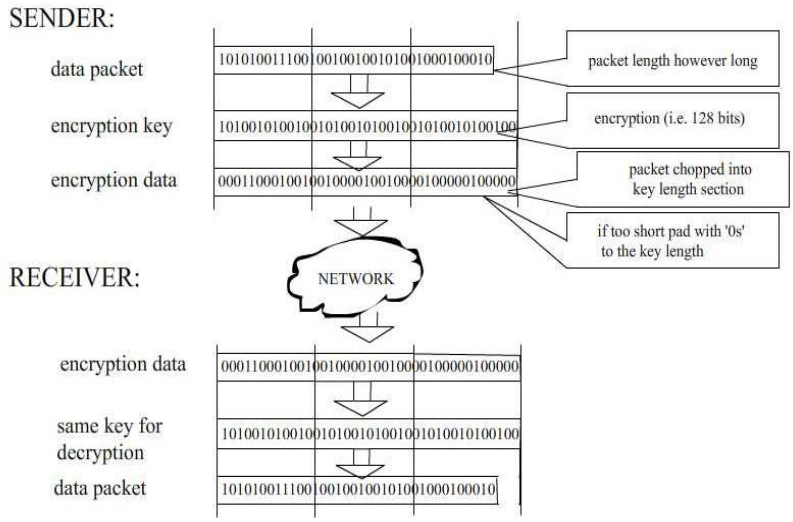

Fig 1 : Signcryption Model

The signcryption based authenticated cloud server also resolved the challenges including eavesdropping and impersonation. The communication is provided in cloud system in electronic form and the secure information transition is performed. Electronic means are here provided for secure information transmission at lower cost. The cost is here adaptive to the time and money. There are number of integrated applications that require the secure remote communication via email so that offline and online communication will be held. Telnet is the provided used to corporate the secure communication license under session generation so that the information security for cloud system will be achieved. Author also provided the session integrated communication so that protected information transmission is available. Author provided the application level integration to present the communication behavior. There is linked layered integration so that communication and authentication level secure information management will be achieved.

Another problem associated with cloud system is the authorization level provided to different user types. In this signcryption model, the user type analysis is also done to identify the user type and based on this type, the actual information encoding and information content retrieval can be obtained. The model is defined under authentication process so that the relative information content access can be obtained from the work. The cryptographic security model is provided to integrate the secure system behavior so that the information management and secure password under user type will be achieved. The cryptographic model provides the safe communication. The presented paper has provided the public and private security solution for this integrated cloud system environment.

In this paper, a signcryption based cloud system security model is provided. This model has integrated all the security policy at one form. These policies include the authentication, authorization and secure communication. The signcryption itself integrates the secure authentication integrated communication so that safer communication in the public environment will be achieved. In this section, a brief introduction to signcryption model is presented and the requirement of this model in cloud system environment is presented. The section also explored the strengths and limitations of secure cloud system environment along with security requirements. In section II, the work defined by earlier researchers for secure cloud system is presented. In section III, the proposed research model is shown. In section IV, the conclusion obtained from the work is presented.

II. RELATED WORK

Different researchers provided work to identify the cloud server risks and to improve the security at cloud system. Some of the contribution of earlier researchers is discussed in this section. SiFan Liu [1] has presented a work on cloud system environment to analyze the risk at lower level and identify the security requirements in cloud system respective to consumers. Author defined the cloud system security model that can cover the maximum number of associated threats. Author discussed the risk points and provided the risk analysis based resource management and allocation so that the integrated security at cloud server will be improved. Author defined the cloud server environment analysis under secure stack based approach. This stack has prioritized the users under the security threats. A work on cloud system assessment under security constraints is provided by Hong Ling Zie [2]. Author has provided the integrated service assessment model to identify the associated uncertainty and certainties. Author analyzed all these parameters and quantizes them so that the cloud service selection will be performed. Author assigned the weight age to different security levels provided by cloud server. These security levels includes authentication, authorization, communication security, session integrated security etc. Saripalli [3] has provided a work on risk analysis framework to identify the risk points under attack model. Author defined the attack categorization and security under different vectors. Author defined

the defensive scheme to improve the reliability over the cloud server. Author defined the attack generation and security issue analysis so that the system integrity will be improved.

Yugang Tian [4] presented a security system model under risk assessment so that the improved secure communication will be performed. The analysis is here defined under communication frequency and entropy weight analysis. Author also presented a case study to identify the flooding communication analysis so that the disaster situation will be identified and the security over the system will be reduced. Author defined the security weights under uncertain conditions analysis. Author defined the study under weighting vector to generate the risk modeling so that the system security and reliability will be improved. Xuan Zhang [5] has presented a work on cloud service model under security constraints. Author defined the risk modeling under service delivery so that the secure system will be obtained. Author defined the service model and its integration under risk analysis. Author defined a framework to improve the security under maturity model. R.PalsonKennedy Author [6] has provided the identity analysis approach under signcryption model to reduce the security risk under efficiency vector. Author defined the security stack to improve the system reliability and the cloud system reliability is improved.

Xin Jing [7] has provided a work on server side infection under different criticalities including the physical hazard, communication security, authentication etc. These all security parameters are analyzed under fuzzy set and generated a probabilistic measure under uncertain conditions and vectors so that the security strengths of the system will be improved. Author defined a qualitative and quantitative model for reducing the system complexities under different assessment model so that system performance and security measures. Author defined the decision assessment model so that the system faults will be identified at earlier stage and the system reliability will be improved. Mariam Kiran [8] has presented a cloud service model under security vector. Author defined the system under secure modeling so that the risk reduction for cloud system will be obtained. Author has presented an infrastructure based service delivery model with integration of IT services so that the system performance and the reliability will be improved. Murat Kantarcioglu[9] has presented a secure system modeling under multiple analysis vectors including availability, scalability, resource integration etc. Author also analyzed the fault and failure integrated in the system so that the system performance will be improved. Author defined the model to provide the optimal system solution under uncertainty parameter. Author defined the adoption rule to improve the system reliability with specification of threshold value. Ashish Bhardwaj [10] has provided a work on demand driven secure service architecture to provide data management and storage on cloud server. Author also handled various security challenges to identify the attack reasons and the security alliances. Author provided the associated model to discover the risks in heterogeneous network environment. Adil M. Hammadi [11] has provided an assure communication mechanism to improve the real time security in cloud environment. Author defined the monitoring framework to provide the reputation assessment in cloud environment. Author reduced the transactional risk under SLA analysis. Author provided a layered architecture for risk assessment and reduction so that the security will be improved over the server. Charles Lim [12] has provided the risk integrated control mechanism to reduce the security threats in cloud system.

III. PROPOSED MODEL

The complete cloud system security model is here inclusively defined with cryptography specific signature verification. The method is here defined under public key concept. In this method, the verification key is generated by the user in which the signature key is stored on cloud server in secure way. This encrypted secure authentication is here applied using registration key protocol. The user email id is considered as the authentication id and the key part is considered as the authentication password. Once the authentication key is obtained, the next requirement is to exchange this key information among the users. For this stage, the exchange protocol is applied. The partial key derivation and signature verification is here defined under hash function integration. The key derivation based voucher will be defined to initiate the distribution. The basic model integration applied in this work are given here in figure 2

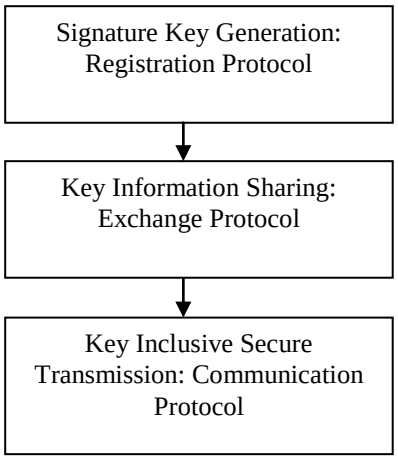

Fig 2 : Proposed Model

A) Registration Protocol

The registration phase is here defined under the token generation that will be defined itself as the complete key or the partial key and able to perform the sign encryption on input registration key. The registration key based signcryption process is here defined as under

1. Generate the certificate mapping for user level validity. This signature validation is here described by
    a. Verify the authenticity and integrity of certificate generated under CA.
    b. Verify the validity of certificate.
    c. Verify the certificate is not revoked till now.
2. Generate the random integer r between 1 and n for key generation.
3. Compute the key R=rG where R is based on the public key and private key verification
   Here, r is the random key generated for public key cryptography.
   G is the hash key signature combined with signature for authentication map.
4. Estimate the Key K based on the random secure vector given by
   K=(r+XrW)Wa
   Where
   r is the prime key vector for public key
   Xr is the signature hash word obtained from the key encryption.
   W is the window block size adapted as the key part.
   Wa is the common authentication window block key for sharing the key as signature value.
   The session key is also derived for encryption. The key is here generated using Hash function based deployment. The symmetric key generation and concatenation is formed.
5. Generate encrypted cipher sign using
   C=Encrypt (Sign).
   Here Encrypt is the secure symmetric encryption model defined using some session adaptive key.
6. Obtain the digital signature from signcryption given by
   s=twA-r (mod n)
   Here t is the hash function adaptive value used as the authentication key.
   wA is the window adaptive shared key for key distribution.
   Here t is obtained using hash function
   t= H(C || Xr || ID |Yr)
   C is the cryptographic function
   Xr is the horizontal matrix
   Yr is the vertical matrix content
   ID is key vector for encryption
7. Generate the token as key for server level authentication given by (R,C,S)

B) Exchange Protocol

To build the contract between the cloud server and client, it is required to sign a common contract by both of these under TTP and cloud integration. The signature exchange protocol is defined for the analysis and to provide the hash integrated secure communication. The steps followed by this protocol are given here:

1. The partial sign will be considered as the client part and pass under hash key. The hash key will identify the requirement of block form and the block generation is here done under padding inclusion. The triple is defined to represent the responder cloud given by
   $$PartialSign = h(m)^{d1} \bmod n$$
   Here h is the hash function,,m is the authentication key generated by client side and n is length of message itself.D1 is the size of block on which hash map will be applied.
2. As the cloud server will receive the triple (Ca, V, PartialSign) it will use it as the cloud server verification key. Ca is here considered as the key generated by the authority. V is the client side voucher encoded by TTP. Based on these key, the

verification of client is done at cloud server. The message contract will be build using this information and the cross check is also performed. The knowledge driven protocol is defined to check this key triple and verification will be considered as the sign done by the server.

3. Cloud server will generate two random numbers between 0 and 1 and represent it a client side key as the computing challenge applied on two client partial keys given here under

$$CloudKey = PartialKey^{2i} * PartialKey^{i} \text{ Mod } N$$

4. Define the client side challenge to accept the response using the third party. This client based commitment is given by

$$R = c^{e} \text{ mod } n$$

This will generate the could based number and consider as the commitment algorithm.

5. Client will verify the correct information generation so that the commitment pair will be initiated with each communication and the communication will be performed under key pair (r,t). This key pair is defined specific for cloud and client.
6. Cloud Server will beck the valid partial key as the signature value considered under contract deadline so that the resolution dispute will be resolved. It will also derive the signature mapping so that the client side session mapping is done.
7. As the key received by the client, the cloud server signature verification is done using partial sub key. The computation of this key is given by

$$CloudKey = h(m)^{d2}$$

This mapping is done using public key mapping integrated under hash algorithm.

C) Key Inclusive Secure Communication

Secure socket integrated secure communication is provided to provide secure communication in the cloud server environment. The work has provided the public view and input modeling under secure socket modeling. The work has provided the privacy ensured communication so that security enabled communication will be performed. The work also applied the security inclusively to the high level protocol. This protocol integration is under symmetric encryption of authentication key and password. The key sharing is done using hash key based encoding mechanism. The secure session is here generated under client enable derivation so that SSL enable communication is performed. The secure transmission control protocol derivation is defined under reliability proved communication in secure way. The secure communication integrated model is shown in figure 3

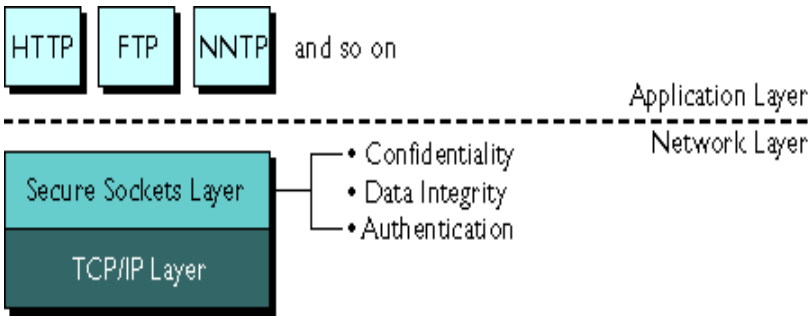

Fig 3: Secure Communication Model

The encoding mechanism followed for secure communication is shown here under:

1. Key integrated secure communication request is passed to build the session.

2. The certificate is verified for client verification.

3. The client adaptive trust is build to achieve the communication under connection derivation so that the trusted communication will be processed
4. The client side information communication is concerned under domain and key specification.
5. The encryption will be used to perform the block signature encoding
6. The cipher form information block will be generated under session key specification
7. Information encryption is done under session key specification and server specification
8. Encrypted session key will be used by client to perform decryption
9. Client will get the message and decrypt it using session key.
10. Secure message is delivered.

IV. CONCLUSION

The paper has presented the secure three stage model to achieve the secure information communication using signcryption technique. The paper has explored each stage of this model in detail along with algorithmic approach and the key generation model. The work also includes the exploration of signcryption model and its requirement in cloud system environment.

REFERENCES

[1] "SiFan Liu," VMRaS: A Novel Virtual Machine Risk Assessment Scheme in the Cloud Environment", 2013 IEEE 10th International Conference on Services Computing 978-0-7695-5026-8/13 © 2013 IEEE

[2] "Hong-Ling Xie," The Research of Power System Operation Risk Assessment modeling Based on Cloud Models", 978-1-4244-2487-0/09 ©2009 IEEE

[3] "Prasad Saripalli," QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", 2010 IEEE 3rd International Conference on Cloud Computing 978-0-7695-4130-3/10 © 2010 IEEE

[4] "Yugang Tian," Flood Risk Assessment Based on Entropy Weight and Cloud Model: A Case Study in Huaihe River Basin of China", 2010 2nd Conference on Environmental Science and Information Application Technology 978-1-4244-7388-5/10 ©201O IEEE

[5] "Xuan Zhang," Information Security Risk Management Framework for the Cloud Computing Environments", 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010) 978-0-7695-4108-2/10 © 2010 IEEE

[6] "R.PalsonKennedy," Assessing the Risks and Opportunities of Cloud Computing – Defining Identity Management Systems and Maturity Models", 978-1-4244-9008-0/10 ©2010 IEEE

[7] "Xin Jing," Risk Assessment for Vehicle Fires based on Cloud Model", 2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD) 978-1-61284-181-6/11©2011 IEEE

[8] "Mariam Kiran," Towards a Service Lifecycle based Methodology for Risk Assessment in Cloud Computing", 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing 978-0-7695-4612-4/11 © 2011 IEEE

[9] "Murat Kantarcioglu," Impact of Security Risks on Cloud Computing Adoption", Forty-Ninth Annual Allerton Conference Allerton House 978-1-4577-1818-2/11©2011 IEEE

[10] "Aashish Bhardwaj,'Cloud Security Assessment and Identity Management", 14th International Conference on Computer and Infonnation Technology (ICCIT 2011) 987-161284-908-9111 © 2011 IEEE

[11] "Adil M. Hammadi," A Framework for SLA Assurance in Cloud Computing", 2012 26th International Conference on Advanced Information Networking and Applications Workshops 978-0-7695-4652-0/12 © 2012 Ieee

[12] "Charles Lim," Risk Analysis And Comparative Study of the Different Cloud Computing Providers In Indonesia".

