EFFICIENT MULTI-LEVEL ENCRYPTION PROCEDURE FOR CLOUD SECURITY

Sampath Kumar Tallapally\textsuperscript{1}, B. Manjula\textsuperscript{2}

\textsuperscript{1}Assistant Professor, Dept. of CSE, S R Engineering College, Warangal, India.

\textsuperscript{2}Assistant Professor, Dept. of CS, Kakatiya University, Warangal, Telangana, India.

\textsuperscript{1}tsk0707@gmail.com, \textsuperscript{2}manjulabairam@kakatiya.ac.in

https://doi.org/10.26782/jmcms.2020.06.00031

Abstract

Cloud space to yourself is a one of the most considerable tentative issue in cloud computing as some of the clients are satisfied with existing policies or protocols where as rest of them are quite concerned with the aspects of corresponding security [IV]. In order to enhance the security levels in this paper we have proposed a multilevel security scheme that provides more security than that of any type of the existing single level encryption based process. In particular the proposed technique ensures that only pre authorized users can only access the cloud data and the other advantage of our algorithm is faster and safer in multiple directions such as while performing uploading and downloading a specific file [X].

Keywords: Cloud security, single level encryption, multilevel security scheme, cloud data.

I. Introduction

In the modern era Cloud computing is an evolutionary medium for performing predominant computation [IV]. The cloud infrastructure vulnerabilities are one of the major challenging issues while performing cloud computing because cloud is often managed by unreliable third parties [III]. The cloud computing is a collection of proven technology and strategies that bundled in a modern network model providing “increased scalability, elasticity, enterprise agility, quicker deployment time, reduced operating expenses and assets flexibility just-in-time” [II].

Cloud infrastructure is a new technology with fairly reduced storage cost and enhanced processing capabilities [IX]. The key objectives of the cloud data are: “exchange of cryptographic algorithms to maintain security, honesty, protection, authorization, access control, and non-repudiation” [XII]. The data security and auditability was listed as the top ten hurdles in cloud storage according to the Berkeley study. There have been a number of cryptographic algorithms implemented in the
modern past and most of them are worth noting whereas some of them such as RSA or DES that are deemed very healthy for a stable cloud world [I].

Another issue that is emerging is that the cloud data values are replicated in cipher code, or in a separate language, called patterns. After deep research generalization of the coding method, any intelligent attacker will quickly identify such patterns. We suggested a strategy for multilevel encryption in which cloud storage will obtain a high degree of confidentiality.

II. Cloud Service–Overview

Cloud is built over internet which combines both software and hardware resources it is mainly used to store a huge amount of data in a secured manner where the responsibility is taken care by the administrators of the cloud and it contains different CPU’s and GPU’s of different configurations with additional capacity of primary memory which increases the speed of execution [XIII-XV]. A Cloud should be built on the standard’s of NIST which contains CSP (Cloud Service Provider) and CA(Cloud Administrator).

| Table 1: Essential features of the cloud:– |
|------------------------------------------|
| **Resources Pooling**  | It is a collections of physical and virtual resources which can be utilized by the users of their need. |
| **On-Demand Self-Service**  | We can choose a service for their need which is monitored. |
| **Easy Maintenance**  | Cloud Administrators take care of new versions of the software and are maintained by them which gives a better comfort for the cloud users. |
| **Large Network Access**  | Bandwidth of the cloud is sufficient for the client who can upload and download the data 24/7. |
| **Availability**  | The resources of the cloud can be modified according to the need of the Cloud user. |
| **Automatic System**  | Cloud automatically analyzes the data needed and supports a metering capability at some level of services. We can monitor, control, and report the usage. |
| **Economical**  | Cost of the H/W and S/W is very less because we use them only when we need them. |
| **Security**  | Data stored over cloud is very secured because cloud has its own cloud security standards. |
| **Pay as you go**  | We use the services as you pay and there will be no hidden cost. |
| **Measured Service**  | Every service we use on the cloud is measured and accountable. |

The cloud service model is classified at a wider extent into specifically two categories such as: “delivery model and deployment model [I]. Where delivery model is subcategorized into six types such as SaaS is abbreviated as software as service, IaaS is abbreviated as infrastructure as a service [II], PaaS is abbreviated as infrastructure as a service MBaaS abbreviated as mobile backend as a service [III], Serverless Computing and FaaS abbreviated as Function as a Service” [IV].

Copyright reserved © J. Mech. Cont. & Math. Sci.
Sampath Kumar Tallapally et al

403
The deployment model is classified into “Public, Private, Community and under Otherswe have Community Cloud, Distributed Cloud, Multi Cloud, Poly Cloud, Big Data Cloud and HPC Cloud [IX-XII]. If we store data in a private cloud the risk of securing the data will be taken by the CA but if we store data in Public Cloud the security should be taken care by the users/client who store the data over the cloud. Community Cloud stores the data of different communities, the combinations of Public and private is called as Hybrid cloud” [VII]. Overall of cloud infrastructure model is shown in Figure-I [VIII].

![Cloud Service Model](image)

Fig.1: Cloud Service Model

### III. Security Issues in Cloud

As we discussed Cloud Computing is an internet based technology where security includes network security and storage. Cloud security should provide CIA rules which stands for Confidentiality, Integrity and Authentication. We provide some of the major threats which are faced by Cloud

- Distributed-Denial-of-Service Attacks
- Shared Cloud Computing Services
- Employee Negligence
- Data Loss and Inadequate Data Backups
- Phishing and Social Engineering Attacks
- System Vulnerabilities
In the proposed system the cloud continues more and more heavily it is adopted and this is very vital or important to be aware of the challenges or various present organizations that are facing with the leveraging cloud computing environment that is summarized below in Fig II.

**Fig.2:** Security Challenges-Model

**IV. Overview on AES,TDES,ECC and Hessian Curve Cryptography**

AES: If we compare AES with other encrypting algorithms like DES and RSA with respective to the computational complexity it is proven that AES is efficient than others in terms of security [XIII]. AES takes less time when compared with others, this algorithm have different rounds depending upon the requirement and every round have a key which is the permutation of the original key. "AES is used for three different type block ciphers such as AES-128 (with 10 rounds), AES-192(with 12 rounds) and AES-256 (with 14 rounds)". The flow of the algorithm is shown below

**Fig. 3:** Schematic flow of AES security Model
Triple Data Encryption Standard:- TDES is a symmetric algorithm which uses the DES algorithm for three times which increases the security of the cipher text.

**Fig. 4:** Block Diagram of Triple DES Encrypting Algorithm

ECC (Elliptic-curve cryptography) is one of most secured and efficient way which can be used in public-key cryptography which is based on algebraic structure over finite fields it is used in key exchange between sender and receiver. “The key size of ECC 256bits is equal to 3072bits of RSA and ECC 384bits is equal to 7680bits of RSA this analysis shows how strong is the key generated by ECC, the security of the data lies of the key strength. ECC uses two key such as public key and private key. Public key is used for signature verification and encryption where as private key is used for decryption and signature generation”.

**Fig. 5:** ECC

ECC includes the following steps in key verification
- Key Generation
- Signature Generation
- Encryption
- Decryption
- Signature Verification.
Hessian curve is a plain curve which is an Elliptic Curve suggested for the applications used by ECC. Hessian curves are more efficient than ECC because it takes lesser memory and is faster because it does lesser arithmetic which is same to ECC in security.

Fig. 6: Hessian curve.

V. Frame Work of the Algorithm

VI. Proposed Algorithm

In our proposed algorithm we use AES and TDES as encrypting algorithms which is symmetric, for key generation we use ECC and Hessian Algorithms. Our proposed algorithm checks integrity and authentication twice, and we require the data to be stored on cloud.

Pre-Requisites

i. Plain text/Original text
ii. Cloud Storage-Authentication
iii. AES algorithm
iv. TDES algorithm
v. ECC algorithm for generating the key
vi. Hessian algorithm for generating the key
vii. Internet
The Function/Methods We Used

i. Block Func () which return’s a with fixed size block every time .

ii. Send (cipher_block) which transfer the cipher text to Cloud Storage.

iii. Receive (plain_block) which appends the block in to a File.

iv. AES(block_data,key1) which call AES algorithm with block of data and a key

v. TDES(block_data,key2) which call TDES algorithm with block of data and a key

vi. ECC() which return

vii. HCC() which returns key2

Algorithm-File Upload

i. EncryptFile(F)

ii. 

iii. declareplain_block,cipher_block;

iv. declare key_1,key_2;

v. key_1=ECC(); //Generate K1 public, K1 private

vi. key_2=HCC(); //Generate K2 public, K2 private

vii. Open Connection with Cloud-Storage.

viii. foreach(plain_block in blockFunc(F))

ix. 

x. cipher_block=AES(plain_block,key_1);

xi. cipher_block=TDES(cipher_block,key_2);

xii. send(cipher_block);

xiii. }

xiv. Close Connection with Cloud-Storage.

xv. }

Algorithm-File Download

i. DecryptFile()

ii. 

iii. declareplain_block,cipher_block;

iv. declare key_1,key_2;

v. key_1=ECC(); //Generate K1 public, K1 private

vi. key_2=HCC(); //Generate K2 public, K2 private

vii. Open Connection with Cloud-Storage.

viii. foreach(cipher_block in blockFunc(Cloud-File))

ix. 

x. plain_block=AES(cipher_block,key_1);

xi. plain_block =TDES(plain_block,key_2);

xii. receive(plain_block);

xiii. }

xiv. Close Connection with Cloud-Storage.

xv. }
VII. Conclusion

One encryption algorithm cannot provide absolute security for the sensitive data so we proposed an algorithm used gives better security to the data which is to be stored and transmitted over the communication line. It gives double authentication and confidentiality. Our algorithm will be fast when uploading and downloading the data from the cloud. In future we will focus on implementation and comparing the results with other techniques.

References

I. https://en.wikipedia.org/wiki/Cloud_computing
II. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
III. https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
IV. https://en.wikipedia.org/wiki/Hessian_form_of_an_elliptic_curve
V. R Ravi Kumar M Babu Reddy P Praveen, “An Evaluation Of Feature Selection Algorithms In Machine Learning” International Journal Of Scientific & Technology Research Volume 8, Issue 12, December 2019 ISSN 2277-8616,PP. 2071-2074.
VI. T. Sampath Kumar, B. Manjula “Perusing on Cloud Computing and its Security Issues”. International Journal of Engineering and Advanced Technology (IJET) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019
VII. T. Sampath Kumar, B. Manjula “Security Issue Analysis on Cloud Computing Based System” International Journal of Future Generation Communication and Networking Vol. 12, No. 5, (2019), pp. 143 - 150
VIII. T. Sampath Kumar, B. Manjula, “Asymmetric AES Algorithm for Cloud Security”, International Journal of Future Generation Communication and Networking Vol. 12, No. 5, (2019), pp. 301-305
IX. R. Ravi Kumar, M. Babu Reddy and P. Praveen, "A review of feature subset selection on unsupervised learning," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2017, pp. 163-167.doi: 10.1109/AEEICB.2017.7972404.
X. Sanjoli Singla and Jasmeet Singh ;“Cloud Data Security using Authentication and Encryption Technique” by in IJARCET Vol 2, Issue 7, July 2013.
XI. Survey on triple system security in cloud computing by ParulMukhi and Bhawna Chauhan in IJCSMC, Vol. 3, Issue. 4, April 2014.

XII. T. Sampath Kumar, B. Manjula, D. Srinivas,"A New Technique to Secure Data Over Cloud", Jour of Adv Research in Dynamical & Control Systems, 11-Special Issue, July 2017.

XIII. T. Sampath Kumar, B. Manjula, Mohammed Ali Shaik, Dr. P. Praveen, "A Comprehensive Study on Single Sign on Technique", International Journal of Advanced Science and Technology (IJAST), ISSN:2005-4238E-ISSN:2207-6360, Vol-127-June-2019.

XIV. Praveen P., Rama B (2020). “An Optimized Clustering Method To Create Clusters Efficiently” Journal Of Mechanics Of Continua And Mathematical Sciences, ISSN (Online): 2454-7190 Vol.-15, No.-1, January (2020) pp 339-348 ISSN (Print) 0973-8975 https://doi.org/10.26782/jmecs.2020.01.00027.

XV. Praveen., P and Ch. Jayanth Babu. “Big Data Clustering: Applying Conventional Data Mining Techniques in Big Data Environment.” (2019).Innovations in Computer Science and Engineering, Lecture Notes in Networks and Systems 74, ISSN 2367-3370, https://doi.org/10.1007/978-981-13-7082-3_58 Springer Singapore.