Competent multi-level encryption methods for implementing cloud security

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

\textsuperscript{1}Department of Computer Science & Engineering, SR University, Warangal, Telangana, India
\textsuperscript{2}Dept, of CS, Kakatiya University, Warangal, Telangana, India.

Email: tsk0707@gmail.com

Abstract. Cloud space to yourself is 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. 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.

Keywords: Encryption, Cloud, Security, multilevel security, file

1. Introduction

In the modern era Cloud computing is an evolutionary medium for performing predominant computation [4]. The cloud infrastructure vulnerabilities are one of the major challenging issues while performing cloud computing because cloud is often managed by unreliable third parties [3]. 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” [2].

Cloud infrastructure is an new technology with fairly reduced storage cost and enhanced processing capabilities [9]. The key objectives of the cloud data are: “exchange of cryptographic algorithms to maintain security, honesty, protection, authorization, access control, and non-repudiation” [12]. The data security and audit ability 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 [1].

Another issue that is emerging is that the “cloud data values” are replicated in “cipher code”, or in a separate language called as patterns [15]. 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 [14].
2. Cloud service overview

[28] 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 [13]. A Cloud should be built on the standard’s of NIST which contains CSP(Cloud Service Provider) and CA(Cloud Administrator) [14].

| Reference | Method                        | Description                                                                 |
|-----------|-------------------------------|-----------------------------------------------------------------------------|
| [15]      | Resources Pooling            | It is a collections of physical and virtual resources which can be utilized by the users of their need. |
| [16]      | On-Demand Self-Service       | We can choose a service for their need which is monitored.                  |
| [17]      | Easy Maintenance             | Cloud Administrators take care of new versions of the software’s and are maintained by them which gives a better comfort for the cloud users. |
| [18]      | Large Network Access         | Bandwidth of the cloud is sufficient for the client who can upload and download the data 24/7. |
| [19]      | Availability                 | The resources of the cloud can be modified according to the need of the Cloud user. |
| [20]      | (a) 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. |
| [21]      | (b) Economical               | Cost of the H/W and S/W is very less because we use them only when we need them. |
| [22]      | (c) Security                 | Data stored over cloud is very secured because cloud has its own cloud security standards. |
| [23]      | (d) Pay as you go            | We use the services as you pay and there will be no hidden cost.           |
| [24]      | (e) Measured Service         | Every service we use on the cloud is measured and accountable.            |

[29] The cloud service model is classified at a wider extent into specifically into categories such as: “delivery model and deployment model” [1]. 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 [2], PaaS is abbreviated as infrastructure as a service MBaaS abbreviated as mobile backend as a service [3], Serverless Computing and FaaS abbreviated as Function as a Service” [4].

[27] The “deployment model is classified into Public, Private, Community and under Others we have Community Cloud, Distributed Cloud, Multi Cloud, Poly Cloud, Big Data Cloud and HPC Cloud [9]. 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” [7]. And the overall aspects of “cloud infrastructure model are illustrated in Figure 1” [8].
3. 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” [12]
- “Shared Cloud Computing Services” [1]
- “Employee Negligence” [2]
- “Data Loss and Inadequate Data Backups” [5]
- “Phishing and Social Engineering Attacks” [3]
- “System Vulnerabilities” [4]

In the proposed system the cloud continues more and more heavily it is adopted and this is very vial 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 figure 2.
4. 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 [13]. 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)”.

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.
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”[26].

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.
5. Frame work of the algorithm

![Proposed frame work of the system](image)

**Figure 7.** Proposed frame work of the system

6. Proposed algorithm

In our proposed algorithm we use AES and TDES as an 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[30-32].

Pre-requisites

1. Plain text/Original text
2. Cloud Storage - Authentication
3. AES algorithm
4. TDES algorithm
5. ECC algorithm for generating the key
6. Hessian algorithm for generating the key
7. Internet

The function/methods we used are

1. blockFunc() which return’s a with fixed size block every time.
2. send(cipher_block) which transfer the cipher text to Cloud Storage.
3. receive(plain_block) which appends the block in to a File.
4. AES(block_data,key1) which call AES algorithm with block of data and a key
5. TDES(block_data,key2) which call TDES algorithm with block of data and a key
6. ECC() which return
7. HCC() which returns key2

Algorithm - File Upload

1. EncryptFile(F)
2. {
3. declare plain_block,cipher_block;
4. declare key_1,key_2;
5. key_1=ECC();//Generate K1public, K1private
6. key_2=HCC();//Generate K2public, K2private
7. Open Connection with Cloud-Storage.
8. foreach(plain_block in blockFunc(F))
9. {
10. cipher_block=AES(plain_block,key_1);
11. cipher_block=TDES(cipher_block,key_2);
12. send(cipher_block);
13. }
14. Close Connection with Cloud-Storage.
15. }
Algorithm-File Download
1. DecryptFile()
2. {
3. declare plain_block,cipher_block;
4. declare key_1,key_2;
5. key_1=ECC(); //Generate K1_public, K1_private
6. key_2=HCC(); //Generate K2_public, K2_private
7. Open Connection with Cloud-Storage.
8. foreach(cipher_block in blockFunc(Cloud-File))
9. {
10. plain_block=AES(cipher_block,key_1);
11. plain_block =TDES(plain_block,key_2);
12. receive(plain_block);
13. }
14. Close Connection with Cloud-Storage.
15. }

7. 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.

8. References
[1] Abhishek Mohta, Ravi Kant Sahu and LK Awasthi 2012 Robust Data Security for Cloud while using Third Party Auditor International Journal of Advanced Research in Computer Science and Software Engineering vol 2(2) pp 201-207
[2] Dr.Seena Naik 2016 An Effective use of Data Mining Techniques to Creation International Journal Of Advancement In Engineering vol 3(10) pp 157-163
[3] Ali Shaik, M. 2020 Time series forecasting using vector quantization International Journal of Advanced Science and Technology vol 29(4) pp 169-175
[4] Shaik, M.A. 2019 A survey on text classification methods through machine learning methods International Journal of Control and Automation vol 12(6) pp 390-396
[5] D.Ramesh, Syed Nawaz Pasha, G.Roopa 2017 A Comparative Analysis of Classification Algorithms on Weather Dataset Using Data Mining Tool Oriental Journal of Computer Science and Technology vol10(4) pp 1-5
[6] Aparjita Sidhu and Rajiv Mahajan 2014 Enhancing security in cloud computing structure hybrid encryption International Journal of Recent Scientific Research vol 5(1) pp 128-132
[7] P. Praveen, C. J. Babu and B. Rama 2016 Big data environment for geospatial data analysis International Conference on Communication and Electronics Systems (ICCES) pp 1-6
[8] Shaik, M.A., Sampath Kumar, T., Praveen, P., Vijayaprakash, R. 2019 Research on multi-agent experiment in clustering International Journal of Recent Technology and Engineering vol 8(4) pp 1126-1129
[9] Praveen P., Rama B 2020 An Optimized Clustering Method To Create Clusters Efficiently Journal Of Mechanics Of Continua And Mathematical Sciences Vol 15(1) pp 339-348
[10] Praveen P., Rama B. 2018 A Novel Approach to Improve the Performance of Divisive Clustering-BST.
[11] Satapathy S., Bhatjya V., Raju K., Janakiramaiah B. 2018 Data Engineering and Intelligent
Computing Advances in Intelligent Systems and Computing vol 542
[12] Shaik, M.A. 2018 Protecting Agents from Malicious Hosts using Trusted Platform Modules (TPM) Proceedings of the International Conference on Inventive Communication and Computational Technologies pp 559-564
[13] P. Praveen, C. J. Babu and B. Rama 2016 Big data environment for geospatial data analysis International Conference on Communication and Electronics Systems (ICCES) pp 1-6
[14] T. Sampath Kumar, B. Manjula, Mohammed Ali Shaik, Dr. P. Praveen 2019 A Comprehensive Study on Single Sign on Technique International Journal of Advanced Science and Technology (IJAST) vol-127
[15] Mohammed Ali Shaik, P.Praveen, Dr.R.Vijaya Prakash 2019 Novel Classification Scheme for Multi Agents Asian Journal of Computer Science and Technology Vol.8(S3) pp 54-58
[16] R. Ravi Kumar, M. Babu Reddy and P. Praveen 2017 A review of feature subset selection on unsupervised learning Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB) pp 163-167
[17] SanjoliSingla and Jasmeet Singh 2013 Cloud Data Security using Authentication and Encryption Technique by in IJARCET Vol 2(7) pp 2013-2019
[18] ParulMukhi and Bhawna Chauhan 2014 Survey on triple system security in cloud computing IJCSCMC Vol. 3(4) pp 201-209
[19] T. Sampath Kumar, B. Manjula, D. Srinivas 2017 A New Technique to Secure Data Over Cloud Jour of Adv Research in Dynamical & Control Systems vol 11 pp 125-131
[20] Sheshikala M, Kothandaraman D, Vijaya Prakash R, Roopa G 2019 Natural language processing and machine learning classifier used for detecting the author of the sentence Int J Recent Technol Eng vol 8(3) pp 936-939
[21] Pasha SN, Ramesh D, Kodhandaraman D, Salauddin MD 2019 An research to enhance the old manuscript resolution using deep learning mechanism Int J Innov Technol Explor Eng vol 8(6) pp 1597-1599
[22] Mothe R, Tharun Reddy S, Chythanya KR, Supraja Reddy Y 2019 Challenges, open research issues and tools in bigdata analytics Int J Recent Technol Eng vol 8(11) pp 2634-2641
[23] Dadi R, Salauddin, Pasha SN, Harshavardhan A, Kumarawamy P 2019 Adapting best path for mobile robot by predicting obstacle size Int J Innov Technol Explor Eng vol 8(9) pp 200-202
[24] Pramod Kumar P, Sandeep CH, Naresh Kumar S. 2018 An overview of the factors affecting handovers and effective highlights of handover techniques for next generation wireless networks Indian J Public Health Res Dev vol 9(11) pp 722-725
[25] Jamalpur Bhavana, Komuravelly Sudheer Kumar 2018 Implementation of Bovw Model Towards Obtaining Discriminative Features of the Images International Journal of Advanced Science and Technology vol 28 pp 17-25
[26] Harshavardhan A, Suresh Babu Dr and Venugopal T Dr 2017 “Brain tumor segmentation methods – A Survey” Jour of Adv Research in Dynamical & Control Systems 11 240-245
[27] Harshavardhan A, Suresh Babu Dr and Venugopal T Dr 2016 “3D Surface Measurement through Easy-snap Phase Shift Fringe Projection”, Springer conference International Conference on Advanced Computing and Intelligent Engineering Proceedings of ICACIE 1 179-186
[28] Mahender K, Kumar TA and Ramesh KS PAPR 2018 analysis of fifth generation multiple access waveforms for advanced wireless communication International Journal of Engineering and Technology(UAE) 7(3.34 Special Issue 34) 487-490 10.2147/NBHIV.S68956 old
[29] Harshavardhan A, Suresh Babu and Dr. Venugopal T Dr 2017 “An Improved Brain Tumor Segmentation Method from MRI Brain Images” 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT) IEEE 1–7. DOI.org (Crossref) doi:10.1109/ICECIT.2017.8453435.
[30] Rajasri I, Gupta AVSSKS and Rao YVD 2012 Structural aspect of symmetry and its effect on
generation of Planetary Gear Trains. Applied Mechanics and Materials 110-116 2619-2622
10.4028/www.scientific.net/AMM.110-116.2619

[31] A. Harshavardhan, Syed Nawaz Pasha, Sallauddin MD, D. Ramesh 2019 “Techniques used for clustering data and integrating cluster analysis within mathematical programming.” Journal of Mechanics of Continua and Mathematical Sciences 14(6) 546-57, DOI.org (Crossref) https://doi.org/10.26782/jmcms.2019.12.00038

[32] Seena Naik K and Sudarshan E 2019 Smart healthcare monitoring system using raspberry Pi on IoT platform. ARPN Journal of Engineering and Applied Sciences 14(4) 872-876.