International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-5, June 2017

An Implementation of Security Model using Homomorphic ECC Algorithm for Cloud Environment

Nilesh Kumar Sen, Navdeep Kaur Saluja

Abstract: ***Cloud computing is the process of providing services to user in according to their need. All the large enterprises are investing in very large amount in order to provide cloud services. Amazon, Google, Windows are having their own services which is available to all users in order to have efficient retrieval. In our survey it is find that homomorphic encryption is one of the finer encryption technique but the finest of all encryption technique is elliptic curve encryption. In this work, the comparison of both computation is performed and result are depicted in order to prove the elliptic curve cryptography as better encryption technique.***

Keywords: Security; Homomorphic Encryption; Elliptic curve cryptography;

I. INTRODUCTION

With increase in digitization in individual life the increase in data occurs at very rapid rate. The data generator where once the individual which are called as applications but with increase in importance of computer science in our day to day life user become the most crucial entity for data generation. The large generation of data is due to social networking sites, blogs and Emails. The storage of this large amount of data is major issue in today scenario, hence cloud is used for this. Cloud computing is solution of having large amount of storage. Cloud computing is the one of the well-known field, which is one of the key resource in web-based applications. Cloud computing is the technology which include Virtualization, parallel computing and distributed computing. Cloud computing is way to provide resources on demand, any resource can be use efficiently. Each cloud model consist of certain model, characteristics and deployment models. The cloud is not just technology which provides not just one service but package of so many services. Cloud computing is having one key component which is Internet, any service can be access with the help of browser. Service oriented architecture [2] is formed for having the cloud based services. The technology is not just confined to software but also to hardware, any hardware can be accessed. The benefit associated with cloud services is that high cost devices can be easily accessed. In cloud based environment the data is send to outside service provider from which user demand services. The data accessing is performed with the help of machine known as Virtual operating system.

Manuscript published on 30 June 2017.
* Correspondence Author (s)
Mr. Nilesh Kumar Sen, M. Tech., Research Scholar, Department of Computer Science & Engineering, Infinity Management and Engineering College, Sagar (M.P), India.
Mrs. Navdeep Kaur Saluja, M. Tech., HOD, Department of Computer Science & Engineering, Infinity Management and Engineering College, Sagar (M.P), India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

For accessing any data the data centers are established which is present all around the globe. One of the widely known cloud services are Amazon EC2, Amazon S3, Google Drive, Hadoop and many others. All the large enterprises are providing all such services.

Cloud computing is taking the advantage of low-cost computing as the single computing provides services to lots of people. All the servers and data centers of one cloud service provider is connected together. Virtualization is one of the major factor which helps in cloud computing, yet today the cloud computing is not fully implemented but can be adopted at very high level in near future.

Cloud computing is not new field in field of computer science, the cloud is classified into various fields which provides services at different level. The infrastructure is completely provided with the help of the cloud which is called as utility computing, having entire infrastructure as server, storage. The platform is also available in cloud services, it ensure facility of operating system and any Middleware. Cloud is not responsible for providing services on such higher it also provides software on demand to end user in order to make it available to each individual.

When there is need of environment with need of having cloud based services then the cost computation is always performed, here cost is compared in term of computation time, memory and processing speed. The cloud vendors thus try to lessen it as much as possible. Cloud vendor is having responsibility of providing the desired facilities to the user.

Cloud computing realizes the importance of data sharing and thus creates the partition in order to have more feasibility. Cloud is partitioned as public, private and hybrid cloud. Organizations which wants the private access which means the storage within the surroundings are private cloud whereas if the storage and services are allowed in and out of the surrounding then it is called as public cloud. There are certain business areas where there is need of services in both environment which are in and out, hence for them hybrid cloud is used.

These Cloud services can be further comes under the three categories.

1. SaaS- Software which are needed are provided on demand basis instead of the need of downloading it hence makes resource more fruitful and beneficial. The service is known as Software-as-a-Service in general and can be accessed using any we b browser.
2. PaaS- Any platform is accessed for using languages, libraries, services and tool usually platform is built by developers. Any operating system can be accessed using cloud services.

© Copyright: All rights reserved.

3. IaaS- Processing and storage capacity, networking and computing resources where the user has control over operating system and deployed application; sometimes referred to as utility computing.

There are three kinds of cloud private, public, protected and hybrid which are commonly called as cloud deployment models.

Private Cloud - If the cloud services is owned by single organization and no user apart from internal ones can use it then it is referred as private cloud. All the services whether a platform, infrastructure or software can be accessed by user.

Public Cloud – If the services can be accessed inside and outside the organization then it is referred as public cloud. The services can be fetch giving appropriate amount.

Community Cloud –If the cloud is used by specific community which may be internal and external to environment then it is called as community cloud. The cost effectiveness of it attract many users instead of having private cloud.

Hybrid Cloud - Any combination of available cloud is referred as hybrid cloud.

Cloud computing is based on five attributes: multi-tenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources, it makes new advances in processors, Virtualization technology, disk storage, broadband Internet connection, and fast, inexpensive servers have combined to make the cloud a more compelling solution.

Cloud is associated with several attributes like scalability, reliability, elasticity, shared resources, pay per use and many such. Virtualization, Internet connectivity and high disk capacity make it even more profound.

The description of this attribute is given as under:

Shared resources: At each level of layered architecture the resources are shared, number of user can access the same services.

Scalability: With increase in number of user cloud user doesn't perform poor, it scalability feature makes it more profound with large bandwidth availability.

Elasticity: It is not required to use all the resources if users doesn't demand that.

Pay as you used: The payment associated with resources are as per the use hence user can efficiently deactivate services when it is not required.

Self-provisioning of resources: Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

Cloud computing can be managed with distributed system, grid computing, utility computing, service oriented architecture, web application, web 2.0, broadband network, the browser as a platform, Virtualization, and free/open software.

The dependency between user and provider is in such a way that is scared of allowing access to unwanted users whereas user is scared to have their sensitive data uploaded on cloud providers which leads to malicious use. In achieving dependency and secure architecture lot of work and analysis is performed. The generation of various dimensions occurs which result in heterogeneous security requirement which must be handled properly. The model present in existing system doesn't have enough security that matches with our requirements. Moreover, the cloud providers host services of users about which they are not aware of these security requirements to be enforced on such services. It leads to a loss of security control over these services and the cloud platforms. Multi-tenant model is formed in order to have better security by having certain security features:

1. Dynamic Scalability
2. Service abstraction
3. Location Transparency

Cloud is highly associated with security as user is always concerned about their data. Cloud provides the storage facility as a service, hence user is always worried where the data is store, and how it is stored. In current days, each organization is trying to provide as much security as possible. Cloud security is highly important as data is not of provider but user. Cloud security can be achieved with the help of multiple encryption techniques as well as multiple access control techniques.

Instead of platform it provides entire infrastructure, the commonly known name of it is utility computing, it conveys the infrastructure can comprises any software and hardware need of the user. It consist of everything platform, software and database services as well.

The architecture of it is given as under:

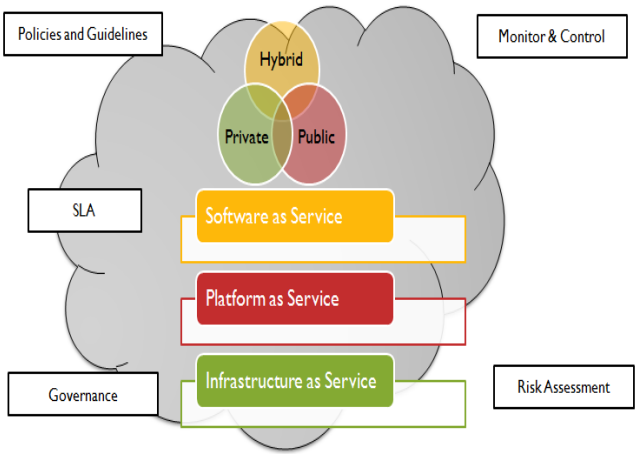


Figure 1.2: Cloud Services model

II. LITERATURE REVIEW

Deyan Chen et al. [1] gives the research on cloud security loopholes and also mention the application of it in wide variety of areas, discussed the importance of cloud computing in all the dimensions like business, organizations and other applications. The research finds that data are migrating but still the real market is not yet captured. Security issue is one of the most popular discussion in terms of cloud computing in researcher background. The work suggests the issue in cloud computing in respect to security in entire data processing in cloud architecture. In fields like data segregation, data security, privacy the role of cloud and its major advantages and drawbacks are discussed in this work.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Tumpe Moyo et al. [2] proposed the solution in field of cloud computing for this hurdles in entire cloud architecture for adoption occurs in respect of organization are discussed. The main issues which this work covers are regarding security obstacles in cloud.

Nasrin Khanazeai et al. [3] researches in field of cloud computing by realizing the issues in security. The AES and RSA are implemented to enhance the security. The system enhance the security to attackers. Vishwanath s Mahalle et al. [4] uses three keys instead of one, along with this encryption is performed at administrator level even in order to makes system more secure. Downloading is also performed is such a way that secure transaction occurs.

Mrudula Sarvabhatla et al. [5] focused on the storage facility provided by Hadoop Ecosystem using HDFS. In this work, entire study on HDFS is performed. The work is done in authentication feature of security model. Nivethitha work is extended as it is just to provide the mechanism of authentication.

III. PROBLEM DOMAIN

With increase in networking popularity the centralized server drawbacks are realized and distributed computing enhances to be popular. The innovation of new field known as cloud is formed and is called as virtual centralization. Cloud is that field of computer science in which user doesn't know where the data is stored where it comes from and how it is managed. When it comes to field of security the initial work was encryption later on algorithm for this are design in which keys are used. The well-known algorithm of cryptography are RSA, Elliptic curve cryptography, Diffie-Hellmen. The security is achieved from the fact that it is very tough to calculate factor of product of number obtained from two large prime number. Discrete logarithmic problem, Integer factorization problem are base of achieving security. So many encryption techniques are designed and observed. There exist no work in which comparison of elliptic curve with homomorphic encryption is performed.

IV. SOLUTION DOMAIN

The security in any environment is categorized as confidentiality, authentication, non-repudiation, access controls, and integrity. In all this security features each one is having its own significance, which one to apply is decided based on the need. Authentication can be defined as the process of getting an assurance whether the user which makes the request is authentic one or not, if it is found correct then user is authentic otherwise it is not. Non-repudiation is the process in which user cannot deny once the services are assigned. Integrity is no content modification in the communication. Access control is method of isolating access on the basis of access rights given, some commonly found access rights are RBAC and ABAC. The commonly find privileges are read, write and updates. Confidentiality is the mechanism of communicating data in which no eavesdropper can interrupt.

The security relies in top features of cloud architecture like Authentication, non-repudiation, access control, integrity and confidentiality. Of all the security features present everyone has its own significance. The one which we will apply is based on the need at the time.

Homomorphic encryption is the method of performing encryption in such a way that third party server will have encrypted data and all the operation will be performed on that encrypted data thus maintaining security. The homomorphic encryption is of two types, partial homomorphic encryption and fully homomorphic encryption. The partial homomorphic encryption allows operation to be performed on already implemented algorithm like unpadded RSA, Elgamal etc. Fully homomorphic encryption is the technique in which operation like addition, subtraction and any such can be perform arbitrarily on any data, the data in it should be in encrypted form.

Elliptic curve cryptography is the technique which performs public key cryptography by plotting the elliptic curves. The algorithm is not based on predefined technique of large prime number instead it uses equations of ellipse. The encryption scheme using in our technique is homomorphic encryption, whereas encryption technique used in our technique is performed using elliptic curve cryptography. The performance is analyzed in terms of processing speed, memory and many other parameters. The comparative analysis of both the techniques are given and concluded as the elliptic curve cryptography is better technique. The computation time of elliptic curve cryptography is much less than other algorithm and thus consider as efficient algorithm for achieving confidentiality. The comparison plot of elliptic curve cryptography and homomorphic encryption is shown below in order to prove the best of both technique:

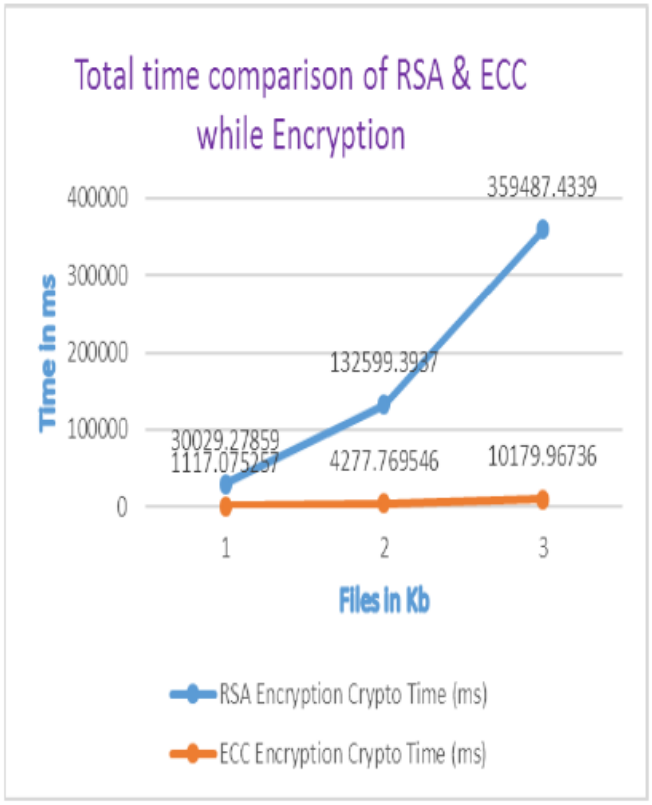
Total Crypto time comparison of RSA and ECC while encryption:

RSA Encryption Chunking Time (ms)	ECC Encryption Chunking Time (ms)
21.414143	259.909853
110.628577	844.429639
341.282809	1564.697042

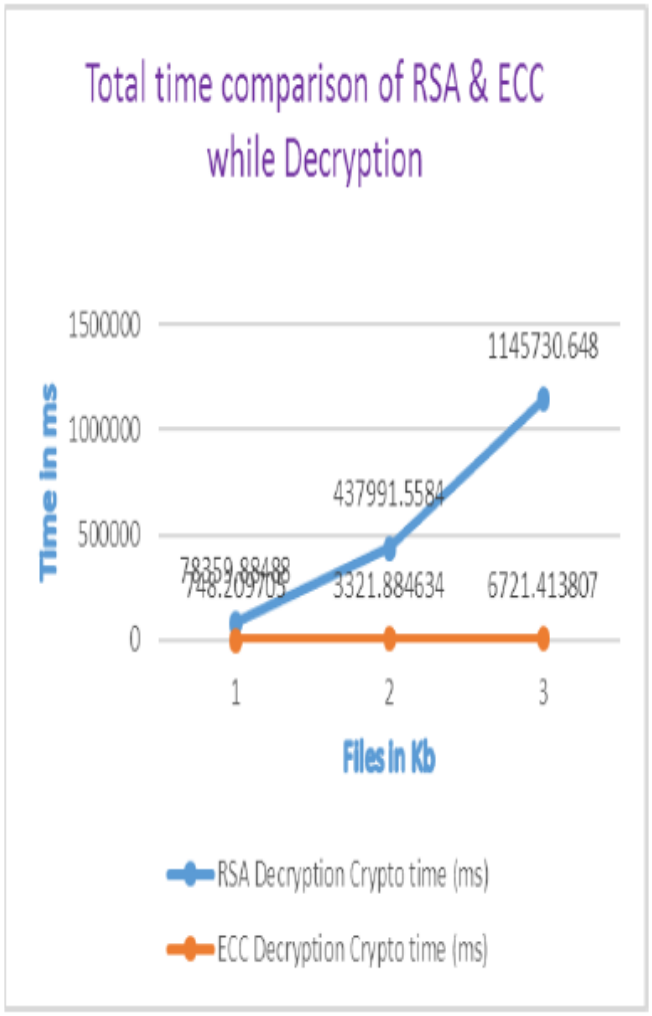
Total Crypto time comparison of RSA and ECC while Decryption

RSA Decryption Chunking Time (ms)	ECC Decryption Chunking Time (ms)
40.21707	681.358987
85.065231	3188.831189
173.338894	6291.386991

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.



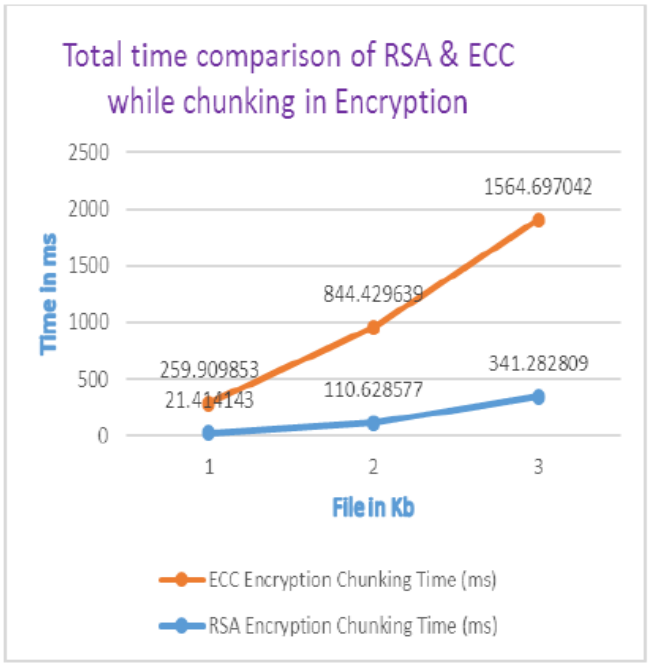
Overall Encryption Time comparison in between RSA & ECC



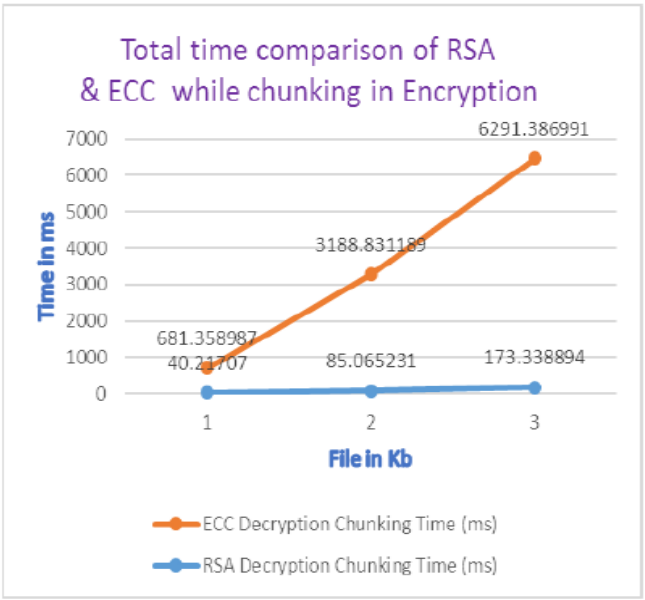
Overall Decryption Time comparison in between RSA & ECC

RSA Encryption Chunking Time (ms)	ECC Encryption Chunking Time (ms)
21.414143	259.909853
110.628577	844.429639
341.282809	1564.697042

RSA Decryption Chunking Time (ms)	ECC Decryption Chunking Time (ms)
40.21707	681.358987
85.065231	3188.831189
173.338894	6291.386991



Overall Encryption Time comparison in between RSA & ECC

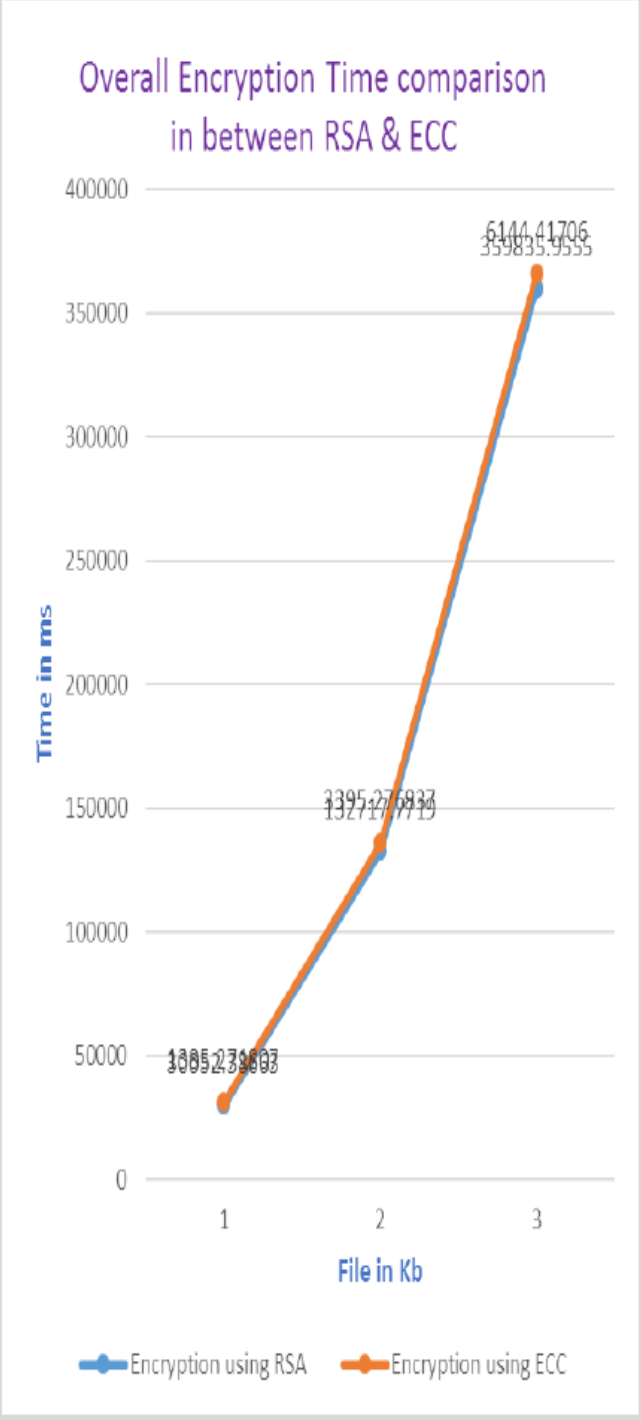


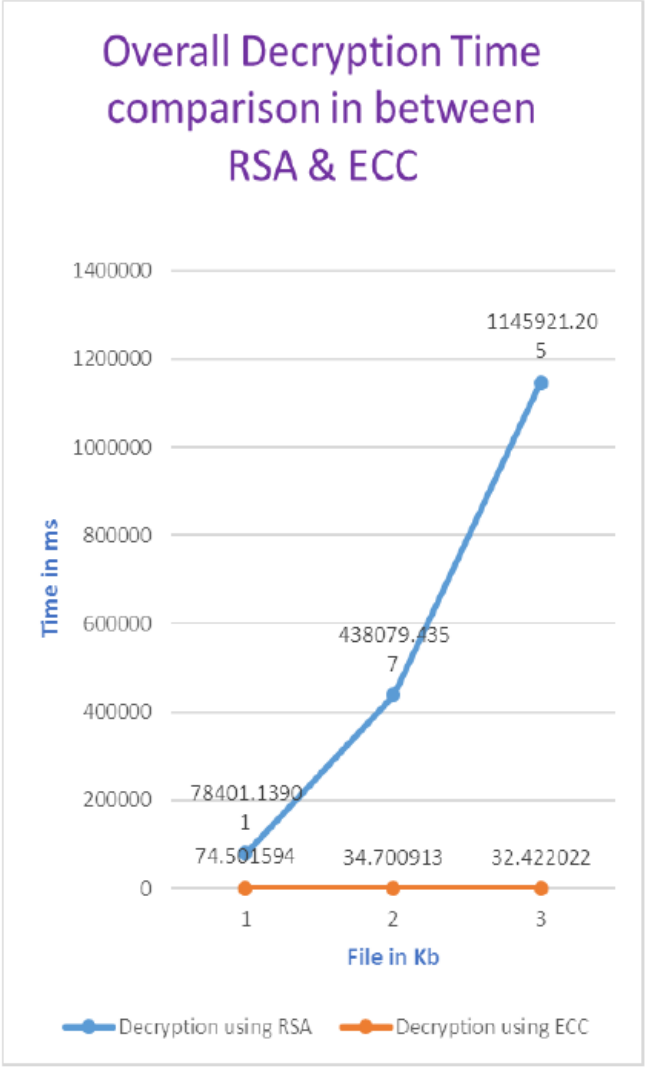
Overall Decryption Time comparison in between RSA & ECC

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Encryption using RSA	Encryption using ECC
30052.38663	1385.271807
132717.7719	3395.276837
359835.9555	6144.41706

Decryption using RSA	Decryption using ECC
78401.13901	74.501594
438079.4357	34.700913
1145921.205	32.422022





V. CONCLUSION

The need of security in cloud based architecture is always desired and analysis is performed. In this work the security feature which is focused is confidentiality. The confidentiality is performed using two techniques homomorphic encryption and elliptic curve cryptography. The analysis is performed and key parameters are calculated and desired graph as well as comparison are plotted. The work will help to decide which security is to opt when and how.

REFERENCES

1. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", "International Conference on Computer Science and Electronics Engineering", 2012.
2. Tumpe Moyo, and Jagdev Bhogal, Investigating Security Issues in Cloud Computing. IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems, 2014.
3. Nasrin Khanezaei, Zurina Mohd Hanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", "System, Process and Control (ICSPC), 2014.
4. Vishwanath s Mahalle, Aniket K Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm", "Power, Automation and communication (INAP)", 2014.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

5. Mrudula Sarvabhatla, Chandra Mouli Reddy M, Chandra Sekhar Vorugunti, “A Secure and Light Weight Authentication Service in Hadoop using One Time Pad”,
6. “2nd International Symposium on Big Data and Cloud Computing (ISBCC’15)”, Procedia Computer Science 50 (2015) 81 – 86.
7. Tebaa, M.; El Hajji, S.; El Ghazi, A., "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of , vol., no., pp.86-89, 20-21 April 2012
8. Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. "O'Reilly Media, Inc.", 2009
9. Samyak Shah, Yash Shah, Janika Kotak, “Somewhat Homomorphic Encryption Technique with its Key Management Protocol”, Dec 14
10. Volume 2 Issue 12 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169,PP: 4180 – 4183
11. Ramaiah, Y. Govinda, and G. Vijaya Kumari. "Efficient public key homomorphic encryption over integer plaintexts." Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.
12. Gentry, Craig. "Computing arbitrary functions of encrypted data." Communications of the ACM 53.3 (2010): 97-105.
13. Atayero, Aderemi A., and Oluwaseyi Feyisetan. "Security issues in cloud computing: The potentials of homomorphic encryption." Journal of Emerging Trends in Computing and Information Sciences 2.10 (2011): 546-552.
14. Catteddu, Daniele, and Giles Hogben. "Cloud computing." Benefits, Risks and Recommendations for Information Security/European Network and Information Security Agency, ENISA (November 2009) (2009).
15. Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647-651, 23-25 March 2012.
16. Pearson, Siani. "Taking account of privacy when designing cloud computing services." Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE Computer Society, 2009.
17. Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On data banks and privacy homomorphisms." Foundations of secure computation 4.11 (1978): 169-180.
18. Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems."Communications of the ACM 21.2 (1978): 120-126.
19. A. C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.
20. Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." Journal of computer and system sciences 28.2 (1984): 270-299.
21. ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." Advances in cryptology. Springer Berlin Heidelberg, 1985.
22. Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." Advances in cryptology—EUROCRYPT’99.Springer Berlin Heidelberg, 1999..
23. Fontaine, Caroline, and Fabien Galand. "A survey of homomorphic encryption for nonspecialists." EURASIP Journal on Information Security 2007 (2007): 15.

© Copyright: All rights reserved.