International Journal of Theoretical & Applied Sciences, 9(2): 283-287(2017)

ISSN No. (Print): 0975-1718
ISSN No. (Online): 2249-3247

Hybrid Encryption Technique for Security of Cloud Data

Akanksha Pandey* and Dr. Sanjeev Sharma**
**Department of School of Information Technology,*
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, (Madhya Pradesh), India
***Head, Department of School of Information Technology,*
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, (Madhya Pradesh), India

(Corresponding author: Akanksha Pandey)
(Received 12 November, 2017 accepted 12 December, 2017)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cloud security is one of the major issue in field of computer science. As cloud is not just responsible for not just storing of data but it provides facilities like IaaS, PaaS which signify it can provide services which can have platform and entire infrastructure as well. Cloud services also allows user to have in organization and out organization facilities also with the help of private, public and hybrid cloud. All the large enterprises are funding in this field some of the well-known examples are Google Drive, Amazon AWS, Windows Azure, Hadoop and many such. All this cloud providers are the market achiever from the fact that they designed the well mannered layered protocol before providing any of the services. Thus in order to make everyone more cloud friendly cloud security is must.

Keywords: Iaas, Paas, Saas, ECC, RSA, HE

I. INTRODUCTION

As the world of digitization grows it result in proportionally increasing the data rate as well. The main player of data generator where the applications once but as the social media world comes into role play the user replaces the applications as a player. The social networking blogs, Emails, blogs, tweets and many such are the examples of it. Whenever there occur change in trends, the complete procedure needs refinement. Of all such changes, the key issue is storage of data. There comes the new technology then which is called as cloud computing.

Cloud computing is the technology which provides all the resources which are desired in any cloud based applications. The combination of technology like Virtualization, parallel computing and distributed computing. Any resource can be accessed on demand in effective and reliable way. There are so many cloud models which can be used. Cloud is capable of providing so many services, any services can be access using browser. The architecture design is performed in such a way that it should have cloud based services. The technology can access any hardware or software, the best part of using cloud services is that high cost devices can be used efficiently.

In cloud based environment, user demand services and the outside service provider carries the data. In order to access data, virtual operating system can be use which means one operating system can access another operating system. Data centers are established all around the globe. One of the widely known cloud services are Amazon EC2, Amazon S3, Google Drive, Hadoop and many others. Large enterprises are investing huge amount in accessing such services.

Cloud computing is beneficial as single computing can provide services to so many people. All servers and data center are internally connected in order to provide services. The extremity to which cloud services can be provided is not yet achieved, it is highly hopeful that cloud services can have it at very high level in near future. Virtualization schemes are widely adopt in order to have cloud based environment.

Cloud based services are not very new to the computer science arena, the cloud is having variety of categorization at different level. If complete infrastructure is provided then it is called as utility computing. The platform can also be accessed as service, platform term is used for operating system at virtual or real level, it is term as Middle-ware. Cloud can also provides software as well, it is called as software as a service in order to make everything available to individual.

In cloud based environment the cost calculation is must, the cost calculation is done in terms of computation time, overhead, memory and many such. The vendor want that cost should be user effective in order to attract more user. Cloud vendor is solely responsible to provide as much service as possible.

Cloud based environment know the significance of data sharing and thus maintain the partition in order to achieve it with more feasibility. Cloud are mainly classified in three very well-defined form called as public, private and hybrid. The complete details of all the cloud is described in further sections. The applications which are accessed depend on need and cost based requirement.

The services are classified in three categories which are given as:

SaaS- Software which are need of the system need not any downloading and can be easily accessed. This will result in accessing software multiple times in fruitful and beneficial. Software-as-a-Service can be used as a service. With the help of browser, any software can be accessed.

The example of it can be any software which can be access in our day to day life, like paint, photo-shop etc. SaaS can cover any software which one can need in day to day life.

PaaS covers any platform level accessing which contains languages, libraries, services, tools needed by the individual who developed all such softwares. Any virtual machine and operating system comes under the category of PaaS.

All the devices which perform storage, computing and capable of providing network connectivity, administrative services if comes under the categorization of utility computing. IaaS is referred as Infrastructure-as-a-Service which is establish at top of cloud computing model provides all the desired services in development and deployment.

Software and hardware anything can be demanded using cloud in order to access anything conveniently. Cloud services can be provided in three ways which are public, private and protected and is refer as cloud deployment model. The cloud have traces of services in all possible direction, which can be given as:

Private Cloud - If the services in cloud are carried by single organization then it is referred as private cloud. Any services can be access in private cloud like SaaS, PaaS and IaaS. The resource are shared with the organization only. It is not always necessary that the dependency is provided by internal management, it can be provided by third party owner as well. The organization must have the clear vision of Virtualization with the significant level. When the things are done properly it will lead to less use of resources as well as fast retrieval without issues.

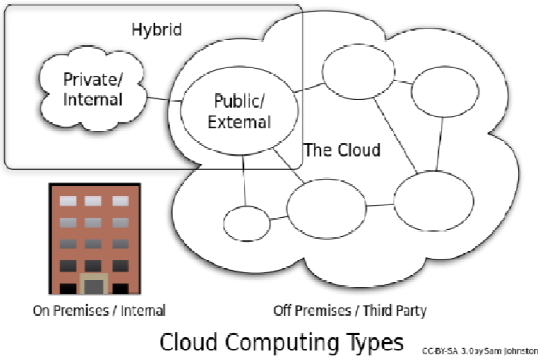
It is quite possible that data centers for it can be created but it will lead to high cost consumption. The classification should be done in proper way as the asset will change with time. The security is also important need as the cloud is the environment with multiple variants. The private cloud is not very much preferred due to the reason that it lead to high purchasing cost. The management and other such factors are also included some estimates found that the cloud is not having more than 20% users.

Public Cloud – The inside and outside access of cloud is referred as public cloud. Everyone can retrieve the services which they want on the basis of pay per use module. If the cloud service provider is new in the market then they provide service at free of cost whereas the business tycoons of the same field demand high cost. The more services you will demand the more will be the charge needed. Hence cloud is commonly known as pay-per-use model.

The difference between both the cloud is services provide in terms of security and access. The security is given so much attention due to the fact that cloud is having all possible crowd of Internet, hence it can have non-trusted users. Some well-known cloud providers are AWS Amazon, Azure and Drop-box. User need services at all level like database, programming, software and many such. The user must have nice Internet connectivity which must be done at private and customized level.

Community Cloud – If the cloud services provided are used internally as well as externally, then it is termed as community cloud. The cost-effective feature of it lead to attract more users in comparison of community cloud.

Hybrid Cloud - If any cloud service are combined in order to form the cloud which allow to have the best results and services in terms of any possible way then it is called as hybrid cloud. Hybrid cloud combines the public and private utilities in order to have the best possible services. The suitable architecture design is being form in order to have the effortless consumption of all possible services.



Gartner, Inc. precise “a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers”.

As we know that, all the cloud services are isolated whether it is private, public or community. Cloud provides all the desired features by using so many processes like aggregation, integration and customization. There are so many drawbacks associated in isolated cloud services, this drawbacks are in network, database and security needs. Also it desires strong authentication mechanism which is resolved in hybrid cloud till some point.

Types of Cloud

There are several characteristics associated with the cloud:

Of all the researchers performed in computer science, cloud computing gain the market due to the fact that it is having the features which resolves so many in-line issues. Cloud is having variety of features which can be mentioned as: The description of this attribute is given as under:

Shared resources: Resources if consumed by one entity of entire architecture can result in so many issues, as the other entity will have had to wait until first one will not use the resource. Cloud architecture provide the facility of having the resource sharing which allows multiple user to access the same resource at same time.

Scalability: Cloud is consider as scalable model due to the fact that with increase in number of user it doesn't degrade its performance. The scalability feature is provided due to the bandwidth availability within the entire architecture.

Elasticity: The demand of user can vary and the resource consumption will be performed in same way, the user if demand more resources than required then it is not mandatory to use them all.

Pay as you used: There always exist the cost of using the resources provided in cloud, hence user will not be ask to purchase the entire service architecture instead it need to pay for the services it use.

Self-provisioning of resources: Cloud is complete in its own way due to the fact that it is having entire Infrastructure like network, storage and services.

II. LITERATURE REVIEW

Homomorphic encryption is suggested by Rivest, Adleman and Dertouzos using the RSA algorithm. In this work, the proposed mechanism was unable to get the desired output. All the algorithm designer propose the scheme of homomorphic encryption, but none of them succeed. Partial homomorphism scheme is also contributed by Goldwasser and Micali [13], ElGamal [14] and Paillier [15]. Fontaine & Galand [16] has conferred a survey of homomorphic encryption whereas Gentry gives the concept of fully homomorphic encryption in his work [17]. Gentry's model is modified, by various researchers. Smart and Vercauteren research the homomorphic encryption with smaller cipher-text. Some other researchers gives the method of arithmetic operation over integers Dijk, Gentry, Halevi, and Vaikuntanathan [19]. Stehle and Steinfield [20] gives further modification in Gentry's model. Y Govinda Ramaiah finds that "Efficient Public Key Homomorphic Encryption over Integer Plain-texts" [4].

III. PROBLEM DOMAIN

With network popularity it has been find out that the centralized server if crashes then all the data will be lost and cannot be recover. To overcome the above mentioned drawback distributed computing comes into frame. The distributed computing can be termed as computing technique which is having data servers at multiple data centers. If any data loss occur then it can be recover from some other end. Cloud computing facilitate the way which it conveys how the data storage occur, along with all other accomplishment. The keys are used for designing algorithm, like RSA, Elliptic curve cryptography, Diffie-Hellmen. All this algorithm rely on the fact that, the product of two large prime number should be perform in such a way that factors shouldn't be easily obtained. Discrete logarithmic problem and integer factorization problem are the base of designing all such algorithm. But elliptic curve cryptography is not based on all such concepts, it is based on equation of ellipse. Our work observe that their exist no algorithm which perform combination of homomorphic encryption and elliptic curve cryptography.

IV. SOLUTION DOMAIN

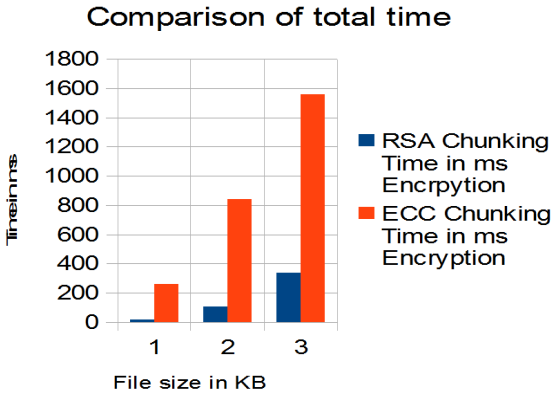
Cloud security is one of the major issue in field of computer science. As cloud is not just responsible for not just storing of data but it provides facilities like IaaS, PaaS which signify it can provide services which can have platform and entire infrastructure as well. Cloud services also allows user to have in organization and out organization facilities also with the help of private, public and hybrid cloud. All the large enterprises are funding in this field some of the well-known examples are Google Drive, Amazon AWS, Windows Azure, Hadoop and many such. All this cloud providers are the market achiever from the fact that they designed the well mannered layered protocol before providing any of the services. Thus in order to make everyone more cloud friendly cloud security is must.

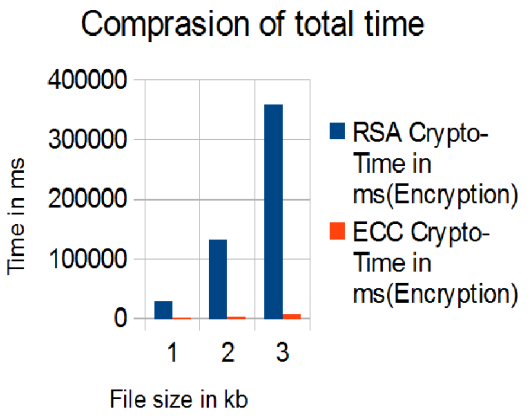
In our work, we are providing the algorithm for implementing Homomorphic encryption by implementation of it of Amazon web services. The aim is to have the processing which must be strong enough to ensure no data theft in process of transfer.

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.

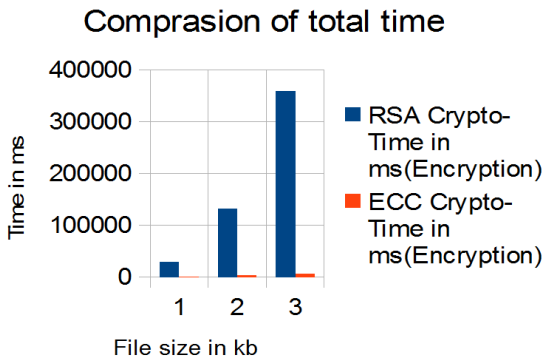
Total time comparison of RSA and ECC while encryption:

RSA CryptoTime in ms (Encryption)	ECC CryptoTime in ms (Encryption)
30029.27859	1117.075257
132599.393703	4277.769546
359487.433852999	10179.967358





RSA Crypto Time in ms (Decryption)	ECC Crypto Time in ms (Decryption)
78359.884876	748.209705
437991.558373	3321.884634
1145730.64811599	6721.413807



Chunking time comparison of RSA and ECC while encryption:

RSA Chunking Time in ms (Encryption)	ECC Chunking Time in ms(Encryption)
21.414143	259.909853
110.628577	844.429639
341.2828090001	1564.697042

V. CONCLUSION

As the security is the need in any environment of computer science, it should be thoroughly studied in order to get the in-depth detail of everything. In this work of all the security need the one which is observed and implemented is authentication. The encryption technique which they work for is Homomorphic encryption.

Homomorphic encryption provides the assurance of hiding the information in such a way that no exposure will be occur. The key idea behind the provided scheme is that third part cloud provider should not have any access to data. The work perform the computation time calculation and compares the parameters in order to ensure which scheme to be adopt at which instance. In the given work homomorphic encryption is applied with the help of two algorithm one is ECC and other is RSA.

The aim behind the given work is to have content unavailable and unreadable to any intruder which may tries to interrupt the communication. The size of cipher-text achieved is high, hence in future work it should be the target to have cipher-text of less size. The facility of querying and processing can also be given in near future.

The demand of security in cloud based architecture is always wanted and analysis is performed in our work also to achieve it. In this activity the security feature which is mainly centered is confidentiality. The confidentiality is performed with the help of two techniques homomorphic encryption and elliptic curve cryptography.

The analysis is done and key parameters are calculated and desired graph as well as comparison are plotted. The work will help to decide which security is to opted when and how.

REFERENCES

[1]. Deyan Chen, Hong Zhao, (2012). "Data Security and Privacy Protection Issues in Cloud Computing", "International Conference on Computer Science and Electronics Engineering", 2012.

[2]. Tumpe Moyo, and Jagdev Bhogal, (2014). Investigating Security Issues in Cloud Computing. IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems, 2014.

[3]. Nasrin Khanezaei, Zurina Mohd Hanapi, (2014). "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, (2014). "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm", "Power, Automation and communication (INAP)", 2014.

[5]. Mrudula Sarvabhatla, Chandra Mouli Reddy M, Chandra Sekhar Vorugunti, (2015). "A Secure and Light Weight Authentication Service in Hadoop using One Time Pad", "2*nd International Symposium on Big Data and Cloud Computing (ISBCC'15)", Procedia Computer Science* **50**: 81–86.

[6]. Tebaa, M., El Hajji, S. El Ghazi, A., (2012). "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of, pp. 86-89.

[7]. Mather, Tim, Subra Kumaraswamy, and Shahed Latif. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance. "O'Reilly Media, Inc.", 2009.

[8]. Samyak Shah, Yash Shah, Janika Kotak, (2014). "Somewhat Homomorphic Encryption Technique with its Key Management Protocol", *International Journal on Recent and Innovation Trends in Computing and Communication* (IJRITCC), Vol. **2** Issue 12, PP: 4180–4183.

[9]. Ramaiah, Y. Govinda, and G. Vijaya Kumari (2012). "Efficient public key homomorphic encryption over integer plaintexts." *Information Security and Intelligence Control (ISIC), 2012* International Conference on. IEEE, 2012.

[10]. Gentry, Craig (2010). "Computing arbitrary functions of encrypted data." *Communications of the ACM,* **53**(3): 97-105.

[11]. Atayero, Aderemi A., and Oluwaseyi Feyisetan (2011). "Security issues in cloud computing: The potentials of homomorphic encryption". *Journal of Emerging Trends in Computing and Information Sciences,* **2**(10): 546-552.

[12]. Catteddu, Daniele, and Giles Hogben. (2009). "Cloud computing" Benefits, Risks and Recommendations for Information Security/European Network and Information Security Agency, *ENISA* (November 2009).

[13]. Deyan Chen; Hong Zhao, "Data Security and (2012). Privacy Protection Issues in Cloud Computing," in *Computer Science and Electronics Engineering (ICCSEE),* 2012 International Conference on, vol. **1**, pp.647-651.

[14]. Pearson, Siani (2009). "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.

[15]. Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. (1978). "On data banks and privacy homomorphisms". *Foundations of secure computation* **4**(11): 169-180.

[16]. Rivest, Ronald L., Adi Shamir, and Len Adleman. (1978). "A method for obtaining digital signatures and public-key cryptosystems. "*Communications of the ACM*, **21**(2): 120-126.

[17]. A. C. Yao. (1982). Protocols for secure computations (extended abstract). *In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages* 160-164. IEEE, 1982.

[18]. Goldwasser, Shafi, and Silvio Micali. (1984). "Probabilistic encryption." *Journal of computer and system sciences* **28**(2): 270-299.

[19]. ElGamal, Taher (1985). "A public key cryptosystem and a signature scheme based on discrete logarithms." Advances in cryptology. Springer Berlin Heidelberg.

[20]. Paillier, Pascal (1999). "Public-key cryptosystems based on composite degree residuosity classes." *Advances in cryptology—EUROCRYPT'99.Springer Berlin Heidelberg*, 1999.

[21]. Fontaine, Caroline, and Fabien Galand (2007). "A survey of homomorphic encryption for nonspecialists." *EURASIP Journal on Information Security 2007* (2007): 15.