Enhancement of Cloud Security Using Enhance Multiplicative Inverse

Renu[1]* Priyanka Singla[2]

[1] Research Scholar, Department of Computer Science and Application, CRSU, Jind

[2] Assistant Professor, Department of Computer Science and Application, CRSU, Jind

Abstract – In this research paper the discussion has been regarding cloud computing and services offered by it. This chapter focuses on the threats to cloud environment from external attacks. In order to make comparative analysis several existing researches have been discussed. The loop holes of those researches are considered. Then a proposed model with integration of MD5 and multiplicative inverse has been developed. This work has introduced more security to the cloud environment. More over the size of packet got reduced that result in high performance of system. The system is more secure and reliable due to integration of two cryptographic mechanisms.

Keywords: Cloud computing, security, MD5, Multiplicative inverse, Matlab

- X -

[1]   CLOUD COMPUTING

Cloud computing provides service over networks, which may be public or private. Cloud is available at a remote location. There are a lot of applications like email and web dependent applications where cloud computing is used. Cloud computing (Jensen, et. al., 2009) has offered Platform independency. Thus, there is no need to setup particular software on the computer. The services offered by cloud computing are shown in Figure 1.
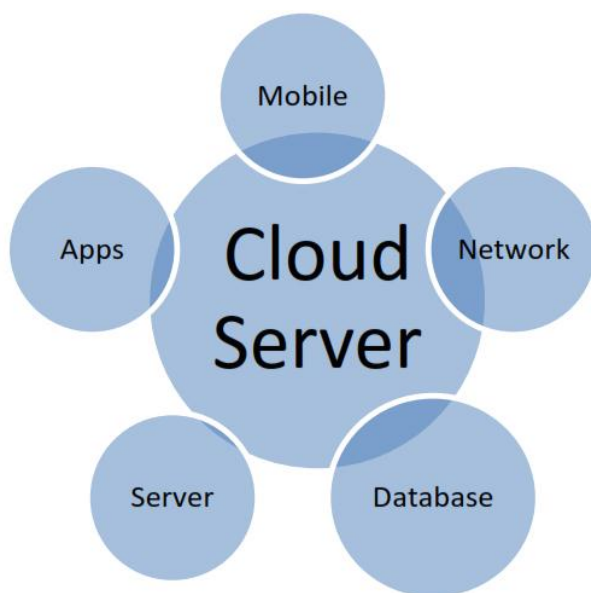

Figure 1 Cloud Computing Services

Some more benefits of cloud computing (Partheeban and Kavitha, 2015) which have been listed below: -

(i)   Cost: - It includes the racks of server, electricity for power and cooling. It adds up fast.

(ii)   Global Scale: -. It includes features like more and less computing power, bandwidth etc.

(iii)   Speed: - Mostly cloud computing services offers self-services. It also offers some other services to clients as on-demand. The quantity of computing resource may be provisioned in minutes.

(iv)   Productivity: - In IT sector, team can spend time to get more important business goals. So, there are facing many problems. These problems are software patching, hardware set up and other IT management chores. Can handle easily these problems by using cloud. Thus, it makes the productivity high.

(v)   Reliability: - The reliability of cloud computing is so high. And it is reliable in nature.

(vi)   Performance: - the performance of cloud computing is good. It is compared to another network connections and services.

Deployment model

There are three different types of (Deshmukh, 2012) cloud computing deployment.

(a)   Private Cloud: - A single business or a single organization is included in that type of cloud. It is physically placed on the organization's on-site datacenter. The maintenance of cloud services and infrastructure is done on a private network.

(b)   Public Cloud: - Cloud service provider maintains the public cloud who is a third party. It delivers their computing resources such as storage and servers over the internet.

(c)   Hybrid Cloud: - an arrangement of public cloud and private cloud has been called Hybrid cloud. This cloud offers great flexibility and more deployment option. These three deployments are defined in previous lines. As an output, cloud computing is more reliable. It comforts our network using many terms, concepts, methodology and methods.
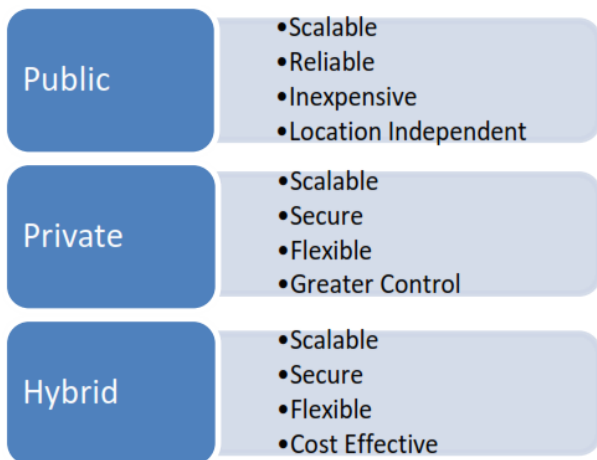
Figure 2Types of Cloud Computing

[2]   LITERATURE REVIEW

In this section numerous kinds of cloud security techniques has been provided..

In 2009, meikojensen and jorgschwenk [1] has proposed Technical aspect related to Security in Cloud Computing. They offered a major problem related to the protection of Cloud Computing.

In 2011, Flavio Lombardi a, Roberto dipietro[2] offered a secure imagination for cloud computing.

In 2015, S Subashini and V Kavitha [3] put forward a security outline by different methods provided with dynamism.

In 2010, Shushing Yu, Cong wang [4]published a paper with research objective to control fine grained data access in cloud computing.

In 2011 V. Krishna Reddy and Dr. L.S.S. Reddy [5] provide a review on cloud computing services to resolve security issues.

In 2011, Syam Kumar P and Subramanian R [6] described an effective and safe protocol with the help of ECC and Sobolseries.

In 2011, Rabi Prasad Padhy,et al[7] this paper projected on Security problem and   Research challenge.

In 2012 Punyada M. Deshmukh et. al. [8] this paper proposed a system which makes sure the data storage security with the help of a distributed scheme.

In 2012, S. Mathew [9], this paper described the Implementation of Cloud Computing in Education

In 2012, Santosh Kumar and R. H. Goudar [10] published a paper highlighting the designing along with well-known platforms of cloud computing.

In 2012, Kangchan Lee [11] wrote a paper in which Security Threats in Cloud Computing Environments security for Cloud Computing is developing sector for learning.

In 2013, Sajjad Hashemi [12] highlighted the challenges of security, mainly data storage security in a cloud infrastructure.

In 2014, Sudhansu Ranjan Lenkaet. Al. [13] implemented a permutation of RSA encryption and digital signature technique.

In 2014, swarnalatabollavarapu and   Bharat Gupta [14] wrote a paper in which data storage security system in cloud computing has been proposed.

In 2014, Salah H. Abbdal et. Al. [15] these paper, it has been concentrated on the issue of making sure the integrity of data.

In 2014, Gajender Pal [16] explained the introduction of Cloud computing.

In   2014,   S.   Venkata   Krishna   Kumar1, S.Padmapriya [17] this review has discussed the offered solution for.

In 2014 Monjur Ahmed and Mohammad Ashraf Hossain[18] it has been described the hurdle related to security challenges in Cloud computing.

In 2014 Suraj R. Pardeshi, Vikul J. Pawar [19] wrote a paper. In this paper it has been proposed the enhancing information security in cloud computing setting.

In 2014 E. Chandanapriya [20] this paper has been focused on Effective Data Sharing with the use of Advanced Ring Signature with the help of Forward Security.

In 2014 Ee-Chien Chang, Roland H.C. Yap, Chunwang Zhang [21] is has been explained reduction of Tagged-map.

In 2015, Goikar Vandana T et. Al. [22] this paper, it has been offered a security agenda for data access.

In 2015 Karun Handaet. Al. [23] this paper, it has been expressed that Cloud Computing has been considered a methodology that voluntarily provide available properties.

In 2015 Manpreetkaur and Hardeep Singh [24] a review of cloud computing security issues has been explained.

In 2015 Amol C. Adamuthe [25] wrote on Cloud Computing, a market approach and of Directions Research

In 2015 Raj Kumar [26] wrote a paper in which they have classified the fact that security has formed the biggest obstacle in widely accepted cloud computing.

In 2015 burhanul Islam Khan, [27] wrote a paper in which they have classified the secure, split, merge data sharing in cloud structure.

In 2015 Jianghong Wei, Wenfen Liu, Xuexian Hu [28]wrote a paper in which they have classify the secure Data Sharing in Cloud Computing which provides a changeable and suitable method for data sharing.

In 2016 AL-museelemwaleed, Li Chunlin [29] assesses the security and secrecy problem transpire in cloud computing.

In 2016 Nidal Hassan Hussein et. Al. [30] presented a complete study of present literature for cloud computing security, challenges along with its solution.

In 2016, Santosh Bulusu et. Al. [31] addresses the several data security and confidentiality security challenges in a cloud computing technology.

In 2016, sakshichhabra, Ashutosh Kumar Singh [32] wrote a paper in which they described the dynamic data leakage detection model dependent point of view for map reduce computational security in cloud

In 2016, Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, jianshen, huanguozhang [33]wrote a paper.

In 2016, Dr.G.M.Nasira, Thangama[34] discussed the Securing Cloud Database By Data combine Technique with the use of Cloud Storage Controller.

In 2016, Aaron Zimba, Chen Hongsong, Wang Zhaoshun concentrated on Integrated State Transition-Boolean Logic Model for the purpose of protection eveluation in Cloud Computing

In 2017, Suraj R. Pardeshi et. Al. [35] it is explained that Cloud computing has been considered net-depended computing.

[3] OBJECTIVES

To fulfil this objective, cryptographic execution control is applied. That is chiefly based on cryptography.

(i) Data confidentiality and integrity are ensured with data encryption and fingerprint mechanisms.

(ii) To have a reading of present protection techniques for storage of cloud data along with integrity.

(iii) To make available a fresh blowfish symmetric cryptography mechanism.

(iv) In order to control the integration of clients, it is offered an image processing concept with the help of finger print mechanism.

(v) To execute all cryptographic tasks on the favor of user.

[4] TOOLS AND TECHNOLOGY

Hardware Requirement

1. CPU (Above 1 GHz)

2. RAM (Above 2 GB)

3. Monitor

4. Keyboard

5. Mouse

Renu[1]* Priyanka Singla[2]

Software Requirement

1.   Windows 7/8/10

2.   Mat lab \ java

JAVA SOCKET PROGRAMMING

The main use of Java Socket programming is the transmission among applications which are executing on a variety of JRE. It is possible that Java Socket programming involve the link-oriented as well as connection-less.

The Socket uses and Server Socket classes have their existence for link -oriented socket programming. In Datagram Socket and Datagram Packet classes, it can be applied. The classes are used for without link socket programming. In socket programming, the user should have the knowledge of the following points:

1.   The user should have the knowledge of IP Address of the Server

2.   The user should also have the knowledge of Port numbers.

Cryptography

Modern cryptography has been considered as deeply dependent on theory of mathematics along with practice of computer science. Cryptographic algorithms are formed along with tough supposition of computation. It makes algorithms tuff to crack by an opposition. Although it is feasible to creak such a structure but it is impossible to occur so by a recognized sensible medium. So these schemes are described as computationally safe theoretical advances for example increment in integer factorization algorithms. Quicker computing methodology demands these solutions to be frequently modified.

Mat lab

MATLAB as a Simulation Tool

MATLAB has been considered a high-performance language for technical computing. It is a mix-up of computation, programming, and visualization in an accessible setting. It is occurred where issues and their solutions are described in familiar mathematical notation. Mat lab is a combination of computation and Math with typical uses of them.

[5]   RESULT AND DISCUSSION

In this research the chart is representing the comparative analysis of time taken to transfer packet. Here the proposed work is taking less time as compare to traditional work.
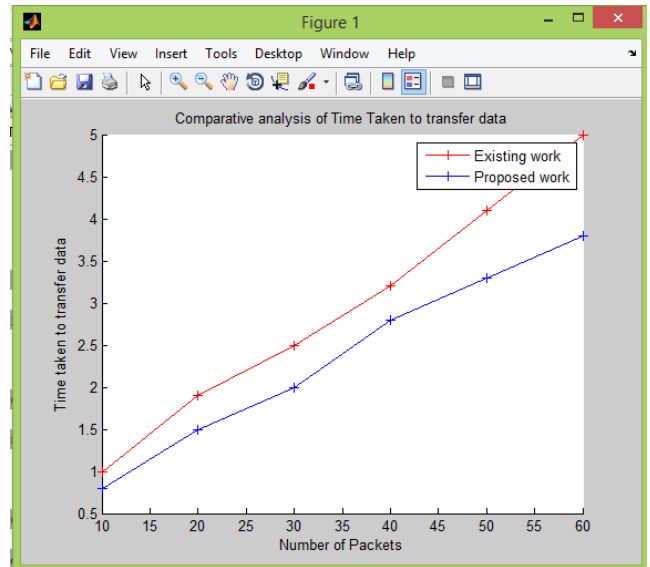

Fig 3 Comparative analysis of time taken to transfer packet

Following chart is representing the comparative analysis of error rates at time of transfer data. Here the proposed work has less error rates as compare to traditional work.
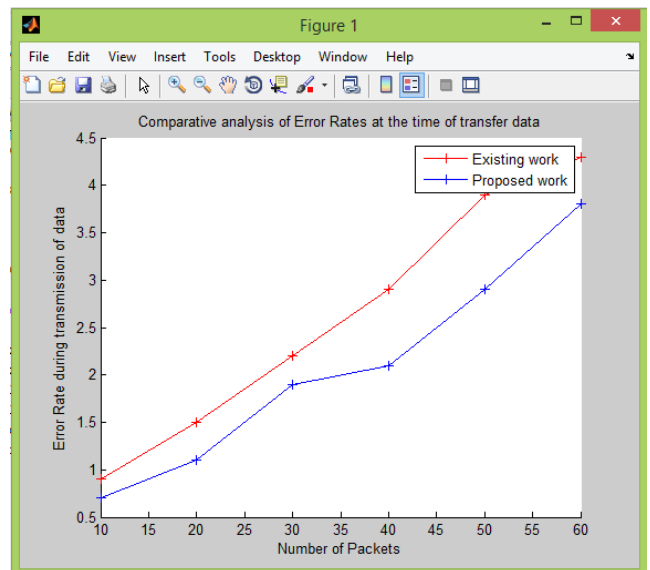

Fig 4 Comparative analysis of error rates at time of transfer data

Following chart is representing the comparative analysis of packet size. Here the proposed work has less packet size as compare to traditional work.

Renu[1]* Priyanka Singla[2]
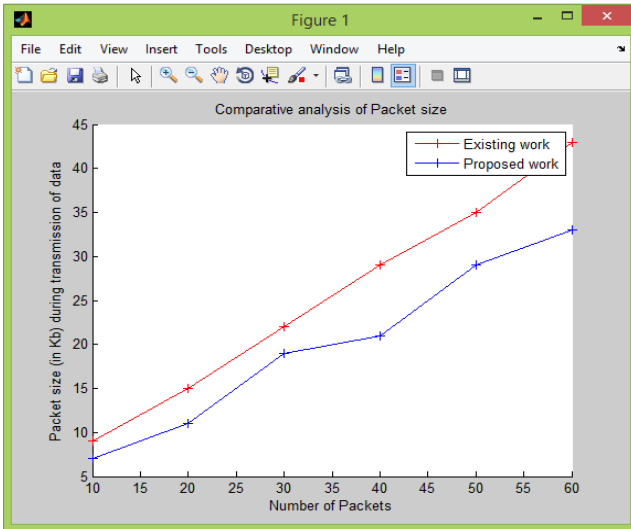
Fig 5 Comparative analysis of packet size

Following chart is representing the comparative analysis of transmission time in case of secure and unsecure traditional and proposed work
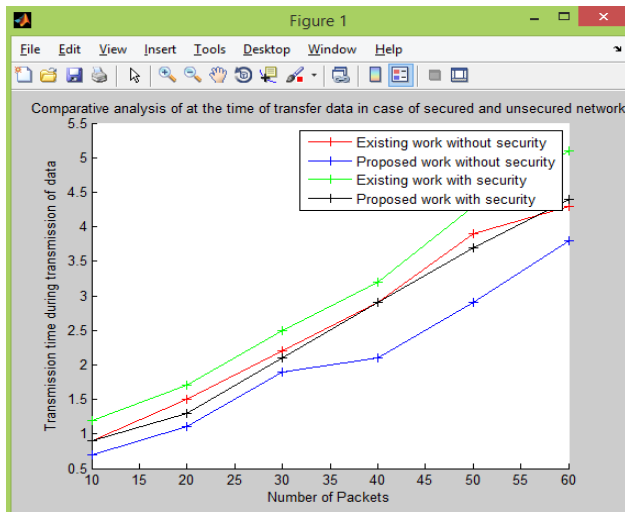
Fig 6 Comparative analysis of transmission time in case of secure and unsecured traditional and proposed work

Research conclusion is that if there is secure transmission then speed of data transfer gets degraded. But if packet size is reduced then speed of data transmission could be improved in contrast of secure traditional work.

[6]   CONCLUSION

Cloud is used to obtain flexible and measurable services. On the other hand, there are numerous threats of protection along with information sending from one cloud server storage into another. The present work would be proved a helper to decrease the threats to confidentiality and availability of data previous. It would be feasible by choosing a cloud vender or selecting cloud. The security a fear of cloud services has brought into focus in our work. In our work, it would offer the current security system. Integration of MD5 with multiplicative inverse has enhanced the security. This encrypted content would be too complex for cryptanalyst to decode. In this way presented scheme protects the information on cloud with the help of multiple level of protection.

[7]   FUTURE SCOPE

Protection to data from being damaged by the attacker has been considered in this research. In existing research, there was scarcity of strong security system to encrypt data. Thus, transmission of data faced delay because of less powerful security system. So, in order to overcome this hurdle, we have decrease of packet's size. In this way we can shrink the issue of transmission delay. Apart of this, we can also create more powerful security system.

Battle between moral or white hat hackers and non-moral or black hat hackers have many contradictions. That has no ending point. When ethical hacker supports the black hat hacker, he has the knowledge of an organisation. They help them to know the security needs of organisation. Thus, malicious hackers break in without any permission. After that they harm network for their own profit. On the other hand, Ethical and creative hacking plays an essential role in network security to make sure the protection of data of a company. Ethical hackers help the company to recognize the individuals, to take curative measures to remedy loophole.

REFERENCE

[1]   M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono (2009). "On technical security issues in cloud computing," CLOUD 2009 - 2009 IEEE Int. Conf. Cloud Comput., pp. 109–116.

[2]   F. Lombardi and R. Di Pietro (2011). "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122.

[3]   P. Partheeban and V. Kavitha (2015). "A study with security concerns in service delivery models of cloud computing," Int. J. Appl. Eng. Res., vol. 10, no. 21, pp. 42219–42230.

[4]   Shushing Yu, Cong Wang (2010). "control fine grained data access in cloud computing,".

[5]   V. K. Reddy and L. S. S. Reddy (2011). "Security Architecture of Cloud Computing," Int. J. Eng. Sci. Technol., vol. 3, no. 9, pp. 7149–7155.

Renu[1]* Priyanka Singla[2]

[6] Syam Kumar P. and Subramanian R. (2011). "an effective and safe protocol with the help of ECC and Sobolseries,".

[7] R. Prasad Padhy, M. Ranjan Patra, and S. Chandra Satapathy (2011). "Cloud Computing: Security Issues and Research Challenges," IRACST -International J. Comput. Sci. Inf. Technol. Secur., vol. 1, no. 2, pp. 136–146.

[8] Punyada M. Deshmukh (2012). A system which makes sure the data storage security with the help of a distributed scheme."

[9] S. Mathew (2012). "Implementation of Cloud Computing in Education - A Revolution," Int. J. Comput. Theory Eng., vol. 4, no. 3, pp. 473–475.

[10] Santosh Kumar and R. H. Goudar (2012). "The designing along with well-known platforms of cloud computing."

[11] Kangchan Lee (2012). "Security Threats in Cloud Computing Environments security for Cloud Computing."

[12] Sajjad Hashemi (2013). "The challenges of security, mainly data storage security in a cloud infrastructure."

[13] Sudhansu Ranjan Lenkaet (2014). "RSA encryption and digital signature technique."

[14] Swarnalatabollavarapu and Bharat Gupta (2014). "data storage security system in cloud computing."

[15] Salah H. Abbdal (2014). "Issue of making sure the integrity of data."

[16] Gajender Pal (2014). "The introduction of Cloud computing."

[17] S. Venkata Krishna Kumar1, S.Padmapriya (2014). The offered solution for Coercion has been considered as problem."

[18] M. Ahmed and M. Ashraf Hossain (2014). "Cloud Computing and Security Issues in the Cloud," Int. J. Netw. Secur. Its Appl., vol. 6, no. 1, pp. 25–36.

[19] Suraj R. Pardeshi, Vikul J. Pawar (2014). "The enhancing information security in cloud computing setting."

[20] E. Chandanapriya (2014). "Effective Data Sharing with the use of Advanced Ring Signature with the help of Forward Security."

[21] C. Zhang, E. C. Chang, and R. H. C. Yap (2014). "Tagged-mapreduce: A general framework for secure computing with mixed-sensitivity data on hybrid clouds," Proc. - 14th IEEE/ACM Int. Symp. Clust. Cloud, Grid Comput. CCGrid 2014, pp. 31–40.

[22] M. Computing, G. V. T, J. S. K, P. P. B, and P. S. D. (2015). "Improve Security of Data Access in," vol. 4, no. 2, pp. 331–340.

[23] Karun Handaet (2015). "Cloud Computing."

[24] M. Kaur and H. Singh (2015). "A Review of Cloud Computing Security Issues," Int. J. Education Management Eng., Vol. 5, No. 5, p. 32.

[25] A. C. Adamuthe, V. D. Salunkhe, S. H. Patil, and G. T. Thampi (2015). "Cloud Computing – A market Perspective and Research Directions," Int. J. Inf. Technol. Computer Science, Vol. 7, No. 10, pp. 42–53.

[26] Raj Kumar (2015). "Cloud Computing."

[27] Burhanul Islam Khan (2015). "The secure, split, merge data sharing in cloud structure."

[28] Jianghong Wei, Wenfen Liu, Xuexian Hu (2015). "The secure Data Sharing in Cloud Computing."

[29] AL-museelemwaleed, Li Chunlin (2016). "The security and secrecy problem transpire in cloud computing."

Corresponding Author

Renu*

Research Scholar, Department of Computer Science and Application, CRSU, Jind

renukajal17@gmail.com

Renu[1]* Priyanka Singla[2]