IMPLEMENTATION OF AES CODE AND SPLITTER TO SECURE THE FOG BASED CLOUD ENVIRONMENT

[1]Manesh; [2]Renu Malik

[1]M.Tech Scholar, Computer Science and Engineering Department, OM Institute of Technology and Management, Juglan (Hisar)-125001

[2]Assistant Professor, Computer Science and Engineering Department, OM Institute of Technology and Management, Juglan (Hisar)-125001

[1] mjangra9717@gmail.com; [2] malikrenu188@gmail.com

Abstract: As the uses of fog based cloud service are increasing therefore such services must be secure. For this, the AES code has been proposed in the research work. The main objective of the research work is to provide a secure system for secure data transmission of fog based cloud system. To ensure the data protection the splitting and encryption of data has been made using AES code. This paper is describing the method to reduce the probability of packet dropping and congestion. It designs and implements more secure algorithm to protect data from active and passive type of attack at application layer. Here the security would be applied on application layer as well as session layer. It also makes comparative analysis of proposed model with existing security model. The research work also provided the comparative analysis of packet dropping in traditional and proposed work.

Keywords: Cloud Computing, Fog Computing, Port no., AES code, Session layer security, Application layer, Splitter

[1] INTRODUCTION

Cloud may be internet or network [1] that is providing services over the network which may be public or private. Cloud is available at the remote location and may be used in wide area network as well as in local area network. It is needed in virtual private network too because there are lots of application like email and web dependent services. Cloud computing [2] has offered Platform independency. Thus, there is no need to set particular software on the computer.

Effortlessly availability of system and services to the organization is made possible by the public cloud. To compare the public cloud with private cloud, the private cloud provides more security due to the private nature of it. Two concepts are there for private cloud. These are hosted by one user's own data centre. Effortlessly availability of system and services to the general public is made possible by the public cloud. It is not more

secure due to its availability for public. The Public clouds may be owned or may be and operated by third person. The composition of two or more clouds is known as Hybrid cloud. These included clouds in Hybrid clouds have their different entities. These are bounded together. This group of cloud computing is offering the advantages of several deployment models. In Hybrid cloud the several clouds are managed within cloud resources. The community cloud allows a group of organizations to access the systems and services. A community cloud in computing has been determined as a collaborative effort. In community cloud an infrastructure has been distributed in multiple organisations.

[2] FOG COMPUTING

Fog computing [3] is known an architecture. In this architecture one or more collaborative end-user clients have been used. Such end user are applied to carry out a significant size of storage, communication rather than routed over internet backbone, control, configuration etc. Fog computing is a decentralized computing system. In this system the data and the fog applications are shared in logical, capable place among the data source and cloud. Fog computing is capable to extend the cloud computing and its services. It provides the services to edge of network. It offers the advantages of cloud. The basic objective of fog computing is to enhance the efficiency. It also decrease the size of data transported to cloud. Such data is send to process, evaluate and for storage. Fog computing has been used because it is capable to improve the efficiency. As well as it also used to secure the data.

Table 1 Difference between Cloud & Fog

Requirement	Cloud computing	Fog computing
Latency	high	low
Delay jitter	High	Very low
Location of server nodes	With in internet	At the edge of local n/w
Distance between the client and server	Multiple hops	One hop
Security	Undefined	Can be defined
Attack on data enrouter	High probability	Very Less probability
Location awareness	No	Yes

[3] OBJECTIVE

This paper carries several objectives which have been listed below:

1. To ensure the data protection by splitting and encrypting data using advanced cryptographic mechanism.
2. To reduce the probability of packet dropping and congestion.
3. To study active and passive attack
4. To provide security to network at different layer
5. To design and implement more secure algorithm to protect data from active and passive type of attack at application layer
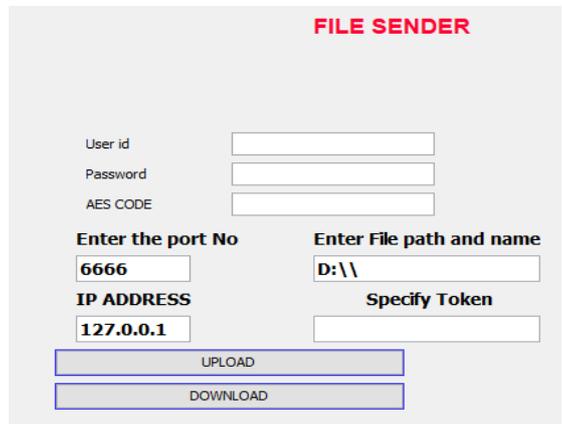6. To make comparative analysis of proposed model with existing security model

[4] PROBLEM FORMULATION

The proposed work would be more secure as to traditional approach. Here the security would be applied on application layer as well as session layer. More over the information would be transmitted from multiple paths using user defined port. It has not used predefined port such as 21 for ftp, 80 for http for data transmission. Proposed encryption mechanisms have been capable to secure data from being destroyed. Proposed system provided security not only on application layer it is also providing security at session. The whole data is not transmitted in single cycle. Data has been split in fog and cloud. If split data is decrypted unauthentic ally it is completely unusable for cryptanalysts
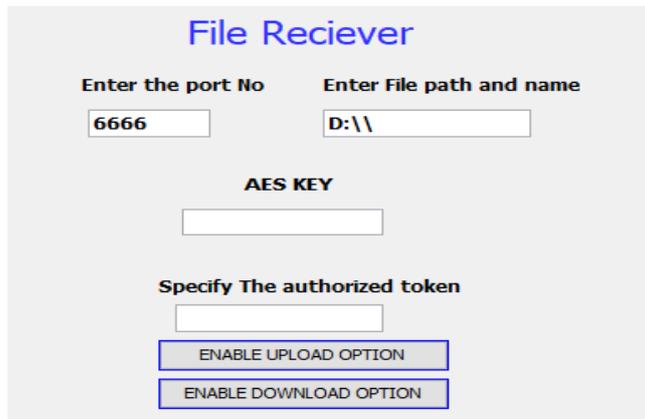
[5] RESULT AND DISCUSSION

5.1 DESIGN GUI INTERFACE FOR CLIENT

This is the file sender interface that would send data to the server. Here the user id, password, port number, ip address, path of file to be send along with security token and AES CODE.

FILE SENDER

User id	
Password	
AES CODE	

Enter the port No   **Enter File path and name**
6666   D:\\
IP ADDRESS   **Specify Token**
127.0.0.1

UPLOAD

DOWNLOAD

Fig 1 Sender Side Application

This is the file sender interface that would send data to the server. Here the port number, AES CODE, path of file to be received along with security token.

File Reciever

Enter the port No   **Enter File path and name**
6666   D:\\

AES KEY

Specify The authorized token

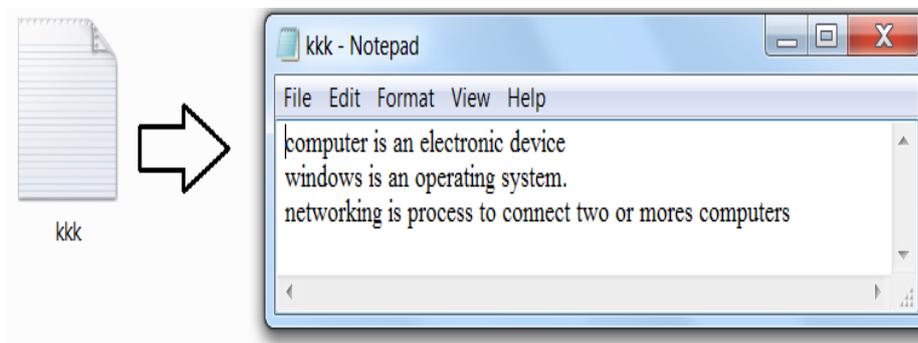ENABLE UPLOAD OPTION

ENABLE DOWNLOAD OPTION

Fig 2 Receiver side Application

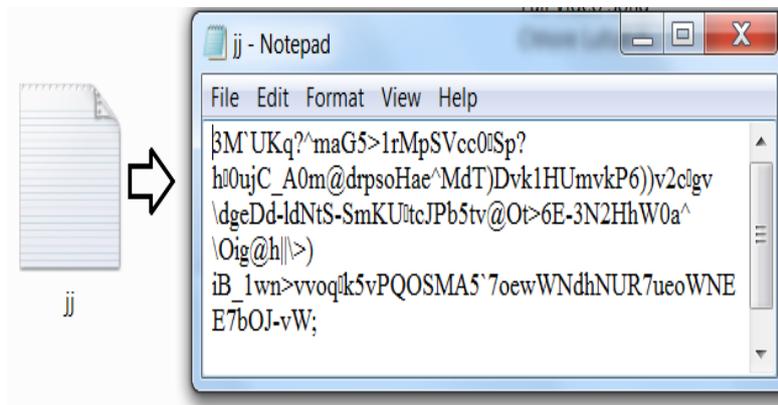Following file would be transferred to the receiver from sender end. It may be notepad file.
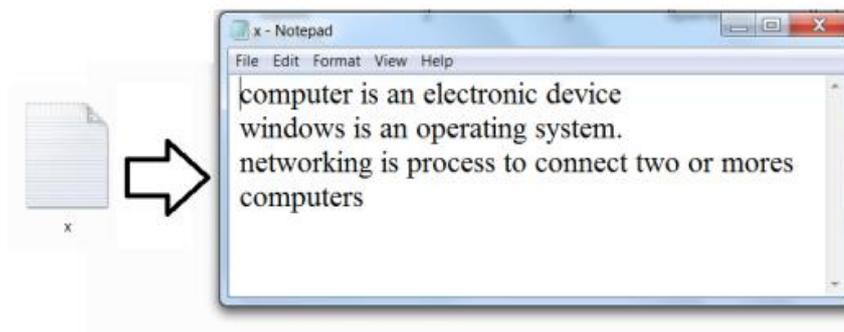
Fig 3 Transfer for file

Following file would be received at the receiver end. The content of that file would be same as file sent from sender end.

Fig 4 File Received

The contents after encryption will be as it has been shown in figure
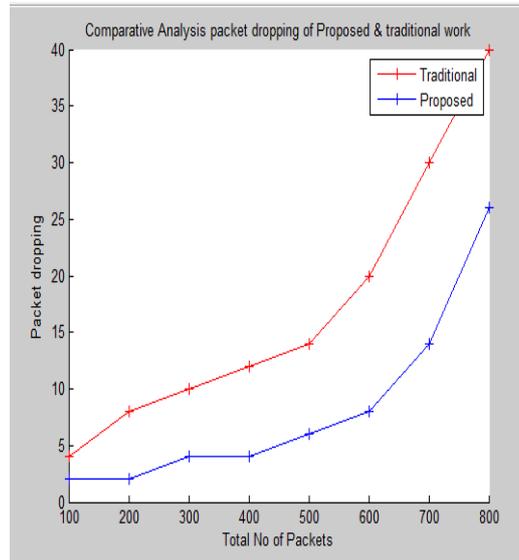

Fig 5 Encrypted File

Fig 6 Server side Implementation

Fig 7 Client Side Implementation

Table 2 Comparative Analysis of Packet Dropping In Traditional and Proposed Work

	Traditional	Proposed
100	5	3
200	9	3
300	10	4
400	12	4
500	14	7
600	18	8

700	30	12
800	40	23

Fig 8 Comparative Analysis of Packet Dropping In Traditional & Proposed Work

[6] CONCLUSION

The proposed work has divided data in multiple parts in order to provide reliable transmission mechanism. This mechanism would make security system immune to attacks made by hacker or crackers. In case of traditional work there was security of data at application layer only. Here in proposed work the security has been provided to the packet. In case of traditional work there was security of data at application layer only. Here in proposed work the security has been provided to the packet. There are several types of limitation of existing security mechanisms. Therefore it is very essential that they must be proposed new security architecture. It is necessary that the decentralized security must be implemented to stop the attacker. Advanced Encryption standard is also used with multilayer security. The proposed work has divided data in multiple parts in order to provide reliable transmission mechanism. This mechanism would make security system immune to attacks made by hacker or crackers.

7. FUTURE SCOPE

The research would provide protection against attack at application layer where user interacts with network directly. The common protocol at application layers are FTP, TELNET & HTTP. The proposed work would be proved helpful for secure transmission because it very efficient and less time consuming system at application layer. The research work would provide protection to data transmission by providing data splitting option on cloud. Some part of data would be stored on cloud while other part would be stored on fog side. This data would be transferred from two different locations and merged at receiving end and decoded after that.

REFERENCES

[1] Yunguo Guan, Jun Shao,GuiyiWei "Data Security & Privacy in Fog Computing" 0890 - 8044 /18/ $25.00 © 2018IEEE

[2] JiyuanZhou (2017) "AHierarchic Secure Cloud Storage Scheme based on Fog Computing" ,2017IEEE 15thIntl Confon Dependable, Autonomic & Secure Computing, 15thIntl Confon Pervasive Intelligence & Computing, 3rdIntl Confon Big Data Intelligence & Computing & Cyber Science & Technology Congress

[3] Bushra Zaheer Abbasi, Munam Ali Shah (2017)"*Fog Computing: Security Issues, Solutions & Robust Practices"*, Proceedings of 23rd International Conference on Automation & Computing, University of Hudders field,Hudders field, UK, 7-8September 2017

[4] Nabil Abubaker, Leonard Dervishi & Erman Ayday "Privacy-Preserving Fog Computing Paradigm" The 3rd IEEE Workshop on Security & Privacy in Cloud (SPC 2017)

[5] M.Verma, N.Bhardawaj, A.K.Yadav, "architecture for Load Balancing Techniques for Fog Computing Environment", I.J.Information Technology & Computer Science Volume 6 No.2, pp.269--274, April 2016, DOI:10.090592/IJCSC.2015.627

[6] K.Shenoy, P.Bhokare, U.Pai, "Fog Computing Future of Cloud Computing", International Journal of Science & Research(IJSR) Volume4 Issue6, pp.55-56, June2015.

[7] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan (2014) "Fog Computing: Will it be the Future of Cloud Computing?" ISBN: 978-1-941968-00-0 ©2014 SDIWC

[8] B.H.Bhavani and H.S.Guruprasad, "Resource provisioning techniques in cloud computing environment: A survey," International Journal of Research in Computer and Communication Technology, vol.3, no.3, pp.395--401, 2014.

[9] M.Georgescu and M.Matei, "The value of cloud computing in the business environment" The USV Annals of Economics and Public Administration, vol.13, no.1, pp. 222--228, 2013.

[10] P.Pazowski and Z.Pastuszak, [8]" Cloud computing–a case study for the new ideal of the IS/IT implementation," in International Conference on Management, Knowledge and Learning, Zadar, Croatia, 2013, pp.855--862.

[11] S.Malkowski, Y.Kanemasa, H.Chen, M.Yamamoto, Q.Wang, D.Jayasinghe, C.Pu, and M.Kawaba, "Challenges and opportunities in consolidation at high resource utilization: Non-monotonic response time variations in n-tier applications," in Fifth IEEE International Conference on Cloud Computing, Honolulu, HI, USA, 2012, pp. 162--169.