A Proposed Way to Secure Cloud Storage :A Review

Kanika Garg
School of Computer Science
Chitkara University
Ambala, India

Jaiteg Singh
School of Computer Science
Chitkara University
Patiala, India

***Abstract*—— Being constantly connected with the internet, internet of things enabled devices are vulnerable to attacks. The large amount of information traversing the Internet of things (IoT) environment could be interfered, altered, or caught while in transit. So, when sensitive data travels through the IoT environment, it should be encrypted to prevent these types of attacks. Algorithm used for encryption should take less time to encrypt the data. So evaluating the best cryptographic method that takes least time to encrypt the data is essential. As IoT enabled devices creates a large amount of data. So there is a need to store that data on the cloud. But as cloud itself has various security issues like improper key management etc. So it is also necessary to secure the data on the cloud. In this work, hardware and software implementation of symmetric cryptographic algorithms is proposed to firstly encrypt the data generated form IoT enabled devices. Then a security technique is proposed to secure the IoT enabled data that is stored on the cloud using the concept of fog computing. The security technique is named as Encoded Data Flow Technique (EDFT).**

Keywords- Cryptography; Encryption; Internet of Things; Fog Computing; Cloud Computing;

I. INTRODUCTION

The Internet of Things (IoT) refers to network of physical objects [3]. The internet of things is an information technology which comes third right after Internet and mobile communication network. But, being constantly associated with the web, IoT enabled devices are vulnerable to attacks [5]. These attacks can be classified based on the techniques used by the attackers and also on the domain of the attackers. Attacks can be active or passive. Some examples of attacks are spying, release of message contents, denial of service attacks, masquerading and message replay etc. End-to-end encryption can only provide the security necessary to prevent any kind of attack as these attacks cannot be prevented by firewalls alone.

With the accessibility of abundant networking options, IoT enabled gadgets are making utilization of cloud enabled administrations and platform because of the generation of huge amount of information by these gadgets. Cloud Computing refers to the act of utilizing a system of remote servers facilitated on the Internet to store, manage, and process information, instead of a personal computer or a local server. Cloud platforms offer a large number of different varieties of web services to its clients. Cloud storage provides the advantages of easier accessibility, reliability, easy deployment, and recovery from any kind of disaster and the expenditure is also very less on the whole [8]. IoT involves the production of huge amount of information by the information sources. This data is having characteristics like large volume, different varieties and is very difficult to manage. When this information is situated on the cloud server it can then be dealt with in a homogeneous methodology through standard APIs that can be shielded by applying top level security and attainment, so it can be called pervasive type of information.

Since the clients are as of now acquainted with working and capacity of cloud, they are expected to utilize their own cloud storage for individual information. Thus user's data is more vulnerable to illegal access by attackers [8]. Cloud based data security is individual to the sort of cloud organization required in regulating, securing and limit of data [7]. Most of the time data stored over a cloud based data center became vulnerable to attacks, when transmitted/communicated over a network as shown in Figure1.

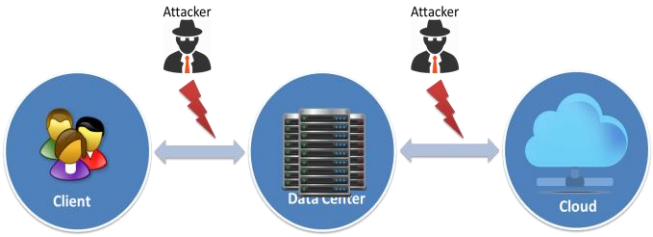

Fig1: An attack to steal cloud data during transit.

There are various cloud storage issues like Data Leakage, improper key management and improper way to handle cloud credentials. Privacy is important for everyone most importantly when individual's personal or sensitive information is being stored. Thus, there is a need to secure data stored in cloud [9].

In this paper an attempt has been made to increase the security of cloud storage by proposing a security technique. The successor of cloud computing is considered to be Fog Network. We assume fog networks as local network where all needful and common data is stored in servers of Fog network (Local data centers). Fog Computing is not a replacement of cloud. It just extends the cloud computing by providing security in the cloud environment. Fog services are able to increase the security of the cloud server by putting the information near the end client as indicated by the necessities. In this manner time to transmit the information is decreased and speed of the general framework is likewise increased [8].

Another point of preference of Fog system over cloud system is high level of secured data communication. To provide such high level of security there are certain techniques and one of among these techniques is to set a secured data center in between the Fog network and the outer world. Therefore, No device is connected to cloud data center directly .All the devices in Fog network are connected to secured data center having predefined rules to enhance security Accordingly the risks can be made less by taking different measures or executing different security procedures. In this research one of the techniques is proposed to secure cloud storage and the name given to it is Encoded Data Flow Technique (EDFT).

Hence, the communication taking place between internet connected devices and Fog data center should be encrypted to ensure privacy and security of data.

II. TECHNIQUE TO FIND THE BEST CRPTOGRAPHIC ALGORITHM IN TERMS OF ENCRYPTION TIME

Cryptographic technique to be chosen to encode the data should be suitable in light of the fact that it should confirm to the quality of security framework. But the cryptographic method while simulation or implementation uses some amount of computer resources [4]. Cryptographic methods are categorized as symmetric cryptography and asymmetric cryptography. In Symmetric ciphers same key is used for encoding and decoding a document. In asymmetric ciphers different keys are used for encoding and decoding a document. Symmetric key cryptography is considered to be more appropriate than asymmetric cryptography in terms of data size, speed and low energy cost. Thus, symmetric key cryptography is considered better for wireless networks [6]. The chosen cryptographic algorithm should take less time to encrypt the data as it determines the speed. Encryption time is the time taken to encode the simple, actual and readable text into encoded text [2]. For choosing the best symmetric key algorithm in terms of encryption time, a comparison is required to be made between different algorithms like DES, AES and Blowfish and to find out the algorithm that will take least time to encode the data generated from IoT enabled devices. These three symmetric key algorithms are well known.

To find out the best cryptographic algorithm that takes the least time for encrypting the data produced by IoT enabled devices, both the hardware and software implementation can be done. The symmetric cryptographic algorithms that can be used are Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Blowfish [4].

It is not economically feasible to purchase hardware so as to analyze their performance. Thus for hardware implementation, a tool called XILINX ISE can be used to simulate the performance of these three algorithms on chosen hardware (Type of Field Programmable Gate Array) [3].

Xilinx ISE (Integrated Synthesis Environment) is a product device delivered by Xilinx. It is utilized for blend and investigation of HDL plans, and empowers the engineer to assemble their outlines, perform timing examination, look at RTL charts, recreate a configuration's response and design the objective gadget with the developer [3].

Artix-7 can be used as FPGA because it has lowest power consumption [3].

The time taken by these three algorithms can be calculated by using timing analyzer in XILINX ISE. Finally the results can be compared to find out the best algorithm among the three that will take least time to encode the data.

Equipment usage is costlier and harder to actualize in contrast with programming execution [1]. So in this research, software implementation of DES, AES and Blowfish can also be done. For doing server programming execution of this mechanism PHP can be utilized as a center programming language having MySQL connectivity to store log of requests. To show these requests logs client interface utilizing HTML, JavaScript and falling templates (CSS) can be developed. This software implementation will test all the three algorithms with respect to the following parameters: mode of encryption and time taken to encrypt the data.

The client entry form can be made which is used to create client ids. These ids are allocated to devices. These ids are used to identify client's device. Requests sent to server by the devices will be identified by their respective client ids.

A request form can be created which incorporates customer id, message that customer needs to scramble and mode which portrays algorithm which customer needs to use for encryption reason.

After doing hardware and software implementation, results can be compared to identify the implementation that will take least time to encode. Furthermore, results can be compared to analyze the symmetric key algorithm that will take least time for encrypting the data.

III. TECHNIQUE PROPOSED TO SECURE CLOUD DATA CENTER

The approach to implement security technique for secure access to cloud data center using Fog Computing is explained below and the name given to it is Encoded Data Flow Technique (EDFT). The mechanism is explained as follows:

1. The client will send the request to the proxy server by supposing it to be an actual cloud server.
2. The proxy server will further forward the requests to the fog server after applying some rules and authentication.
3. The fog server will receive the requests and after authentication of the client will send the request in encrypted form further to the cloud server.
4. Cloud server will receive the requests in encrypted form, will further decrypt it, do authentication and authorization and after that only will process the request. The cloud will send the reply back to the fog server which it will redirect to the client via proxy server.

Overall purpose of this implementation is to secure all locations where data is being exchanged. So here is brief information about all units as discussed above to enhance security:

A. Proxy Server

In computer networks, a proxy server is a server that acts as an intermediary for requests from clients seeking resources

from other servers. Proxy servers are categorized as per the direction of communication as: Forward proxy and Reverse proxy. In our EDFT mechanism we will be using Reverse proxy as it will keep Cloud server behind the wall. In fact proxy will redirect requests to the fog data center also named as broker server.

B. Fog server also named as Broker Server

The Broker Server(s) are intermediary independent unit(s) working between Proxy server and the Cloud Server. Role of these Broker units is to authenticate the identity of the client devices and the request validity. Another thing that is being checked by these servers is request structure. So if these servers found that the request is in valid format only then it will be forwarded to the Cloud server.

After authenticating the client device and request format, Broker will encrypt the request sent by the client and forward it to cloud data center. The requests is in encrypted form, hence it will be difficult for the attacker to decode those requests and to decode the identity of the clients as well.

Another advantage of using these Broker servers is that they avoid the bottle neck situation at Cloud servers end. So if any unauthorized device is trying to keep server busy by flooding requests. Then these requests will be filtered out by the Broker Server. The data exchange will be encrypted so it's Broker Server's responsibility to encrypt the request before forwarding it. This encryption mechanism is critical and it follows well known public-private key encryption mechanism. Broker Server encrypts data using its Private Key and then forwards the encrypted request packet to the Cloud server [8].

C. Cloud Data Center

To avoid misuse of its resources Cloud will receive the requests in encrypted form. The request received will be decrypted using private key of broker as cloud will be having private keys of all the broker servers. Cloud server will verify the identity of Broker server. If it founds that the request is being forwarded by the valid Broker then only the request is processed.

D. Devices As authenticated clients

Client devices will be registered using the simple device authentication mechanism. This mechanism can be developed to uniquely identify these devices. It can be any network enabled device. These all devices are in fog network and are allocated a uniquely identified client ID. Request received by server using these client IDs will be processed. If request to the server comes from any other client without having client ID or invalid client ID, then the request will be rejected by the server.

Once a client device is validated by the server only then it can avail the services of the cloud server.

E. Users Authentication

To enhance overall security of this system, users will be authenticated using username and password combination. To enhance security to a major level without having any effect on scalability , this username and password combination can be restricted to valid devices only.

IV. CONCLUSION

This research is intended to analyze performance of various cipher based security techniques and to analyze their efficiency in terms of encryption time. On the basis of performance analysis the best suited algorithm for secure data transmission from IoT enabled devices to local data center, would be chosen. And this research is also intended to increase security of cloud based data center using the concept of Fog computing.

REFERENCES

[1] J.Thakur, and N. Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering, pp: 6-12, 2011.

[2] Rimpi D., Priyanka A., Geetanjali V.," DES,AES and TRIPLE DES: Symmetric key cryptographic algorithm" International Journal of Science, Engineering and Technology Research (IJSETR) 3.3, 2014.

[3] K. Kaur, B. Pandey, J. Kumar, A. Jain, and P. Kaur, "Internet of Things Enabled Energy Efficient Green Communication on FPGA", IEEE 6th International Conference on Computational Intelligence and Communication Networks (CICN), Udaipur, 14-16 November, 2014

[4] N.Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." IEEE Information and communication technologies(ICICT),2005.

[5] A.Ukil, J.Sen and S. Koilakonda "Embedded security for Internet of Things." Emerging Trends and Applications in Computer Science (NCETACS), 2nd National Conference on. IEEE,pp-1-6, 2011.

[6] Q.Shanxin, S.Guochu., H.Yihong.," High throughput, pipelined implementation of AES on FPGA", Information Engineering and ElectronicCommerce,IEEC,pp:542-545,2009.

[7] R.Raut , M.Waje , S.Kulkarni and A. Gupta , "Security for Cloud using Fog Computing." IJRIT International Journal of Research in Information Technology, Volume 2, 2014, pp: 98- 101

[8] Aazam M, Huh EN. Fog computing and smart gateway based communication for cloud of things. InFuture Internet of Things and Cloud (FiCloud), 2014 International Conference on 2014 Aug 27 (pp. 464- 470).IEEE.

[9] 1.Medaglia CM, Serbanati A (2010) An overview of privacy and security issues in the internet of things. InThe Internet of Things Springer New York, 389-395.