Using L2TP Protocol in Cloud Infrastructure with IoT for Secure and Robust Communication

Muhammad Imran Majid[1], Safwan Ashraf, Haris Ghouri[2]
Institute of Business Management Karachi, Pakistan
[1]imran.majid@iobm.edu.pk, [2]safwan.ali.47@gmail.com

Abstract:

Security is the major issue in networking world and it is extremely critical for business continuity. In this paper, VPN is deployed between virtual Cloud and physical IoT devices to obtain faster communication with security allowing transferring of data proficiently and safely. L2TP technology is used to achieve VPN connectivity with two phase authentication and encryption of data, which results as a secure and fast tunnel for data transfer minimizing time from 240ms to 140ms. This will provide a new way to transmit data securely and in less time. Other VPN technologies such as IPsec and SSL can be incorporated with this technique, which can further enhance the data rate and make the connection more secure.

I. Introduction

Internet of Things and Cloud computing are new technologies that are growing rapidly in the field of telecommunications. As the world is advancing in technology, the risks of security breaches are becoming more common in the field of information technology [1]. In this paper we are discussing the method of securing the IoT data with the help of Cloud infrastructure and L2TP protocol. We focus on the privacy of data transferred by IoT to the servers through Cloud, the servers as well as the firewall are virtual machines deployed on Cloud infrastructure.

Data or information is the most important aspect for any human or any organization. Data security should be to the utmost level so to secure the unauthorized use of the data [2]. IoT is comprised of multiple devices, software's operating systems which can send out kilobytes of data a minute to complex things comprising of multiple sensors churning out gigabytes of data in a continuous data stream. As per RFC 4949, the security breaches by entity to evade established measures can be classified in terms of intent, origination and delivery method. Depending on the intent of attacker, as active (resources / operations) or passive (put information to use without affecting system resources). If referenced to the point of initiation, "inside attack" versus "outside attack" are the known types Using the method of delivery, direct and indirect attacks are well referenced. These includes "smurf attacks" as well "reflection attacks"(replay by intrusion). Use of IoT results in improved efficiency and reduced human error.

L2TP protocol will be used in this experiment to further secure the layer of data and find out the impacts of this protocol. The layer 2 tunneling protocol is utilized to help virtual private systems (VPNs), depending on an encryption protocol that it goes inside the passage to give security. L2TP does not give secrecy or solid validation independent of alternate sources. Other algorithms such as 3DES and AES128 (Figure 4 & 5) are described as they provide encryption.

Due to the universal appeal IoT is incorporated with Cloud computing, because of the amount of data IoTs could generate and their requirement to have the freedom of virtualization and storage capacity. Ability to create smart applications is balanced by security as it is the main concern in Cloud computing [1]. In this paper was present a novel solution paradigm for secure communication links between IoT devices and application servers in the cloud.

In Section II we present literature review of existing security techniques. In Section III we introduce the paradigm of IoT Security using L2TP as the initial protocol and we present the base architecture. In Section IV we present the results and analysis present a way of integrating components; Cloud platforms, Cloud infrastructure and IoT middleware. We identify the future work and finally conclude in the last two sections.

II. Literature Review

Users expect that their data is protected from external sources from malice. In [2] notion of Probabilistic Yoking Proofs (PYP) performance metrics of cost, security, and fairness are stressed. The proposal combines the message format with incremental sampling process dictated by Poisson where there is rate of change of metrics. Further in other work, IoT devices gathered data from different instruments and send the data to the controller in plain format. We hence prefer star topology as used in traditional ISP server. In [3], IoT and Cloud Computing is integrated using COTS to enable privacy preservation. Here proxying IoT using VPN is considered effective and we further extend the concept of simple cryptographic techniques using two authentication techniques and adapt L2TP parameters to enable a cost effective as well as time effective implementation.

The Cloud environment is based on virtual machines and virtual infrastructure, it can be provided by standard internet protocols. The communication leads data transfer and applications work between the users and Cloud. Communication with in VMs are also taking place on logical network which is places on physical network. Single physical machine is hosting multiple VMs and using different ports to distinguish traffic among them.

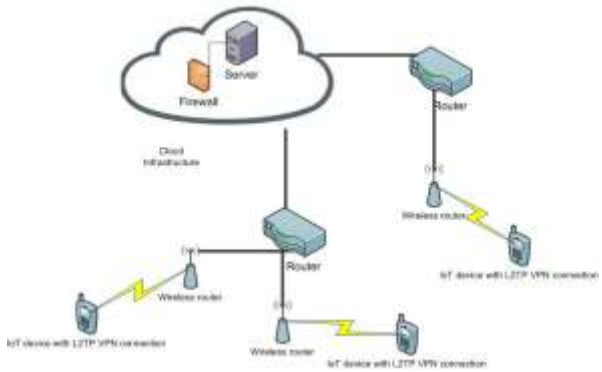

Figure 1 Cloud and TWO IoT Device based Framework to enable security protocols over VPN.

The physical layer cannot determine the threats present in the virtual network, thus it becomes extremely challenging to inspect and detect abnormal activities of the virtual machines. Firewalls and antiviruses deployed on virtual networks help overcome such situations and observe traffic patterns to find anomalies in the system. Traffic flooding and Denial of Service (DoS), spoofing and sniffing of virtual network. The traffic rates are monitored for the detection of malicious content [4].

a. Security in IoT via Cloud service

The records within the Cloud is a good deal extra liable to danger in terms of confidentiality, integrity, and accessibility in comparison to the conventional computing version [5]. The growing numbers and users are indication towards greater risk and security breaches. To secure data for IoT and Cloud, VPN technology is becoming more and more popular as it isolates the infrastructure that is already in Cloud from unknown attackers.

To protect the correspondence and system, the CSA (Cloud Security Alliance) rules prescribe the utilization of mixture of virtual LANs, IDS, IPS, and firewalls to ensure the information in travel. The rules additionally center around spillage of client's information because of a virtual system and the utilization of same fundamental foundation. The CSA suggests the utilization of previously mentioned devices with strict access administration approaches. The CSA has permitted utilization of virtual gadgets and traditional physical gadgets with snug coordination with the hypervisor to guarantee perceivability and checking of movement over the virtual system [6].

III. System Model

The star topology system architecture is shown in Figure 1. Here the services rendered are as described in RFC 2661. Specifically we use authentication and encryption without the use of IPSec. Connection oriented architecture assume a remote smart phone which established a PPP connection across the PSTN Cloud to an LAC. The LAC then tunnels the PPP connection across the Cloud server to an Node Server which provides authentication, and access as well as accounting by home smart phone's Management Domain.

We configure the Cloud firewall, and configure L2TP VPN, to measure our success using various time instances as our metric. In today's world, three of the most important things in networking are security, time and business continuity; we looked at three of those metrics to implement this experiment.

a. Configuring Devices:

In this experiment following devices/machines are used.

i. Firewall:

A firewall is deployed on the Cloud, with three interfaces. We used two of them.

One is LAN interface Port A, which we would be able to ping

Other is port B for WAN IP masking.

With interface Port A, we have connected a virtual machine that is communicating with the IoT devices for testing purpose.

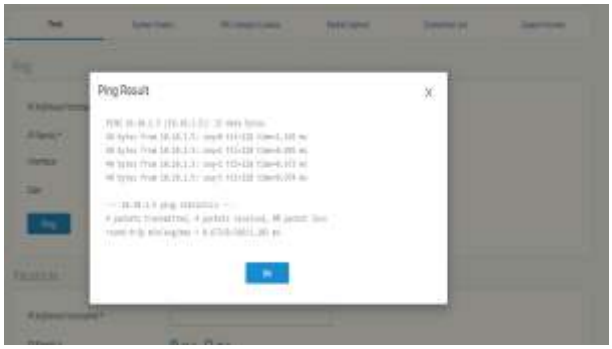

Figure2 Ping response from firewall to machine (cloud)

The ping response is shown in Figure 2. The simple technique is sufficient to quantify the effect of the slow L2TP implementation.

b. Encryption Techniques:

During the authentication, there are two phases and in both phases encryption and authentication takes place with given algorithms:

Table 1 Configurating Authentication - Phase I

Phase 1 configuration parameters		
DH Group	***Encryption***	***Authentication***
DH1024	3DES	SHA1
DH1024	3DES	MD5
DH1024	AES128	MD5

Table 2 Configurating Authentic ation - Phase II

Phase II configuration parameters		
DH Group	***Encryption***	***Authentication***
DH1024	3DES	SHA1
Dh1024	3DES	MD5
DH1024	AES128	MD5

3DES:

Triple information encryption algorithm turned into DES make it tougher to decrypt, 3DES increases the important thing length of DES i.e fifty six-bit by using algorithm 3 times with 3 exclusive keys. The combined key size now emerged as 168-bit.

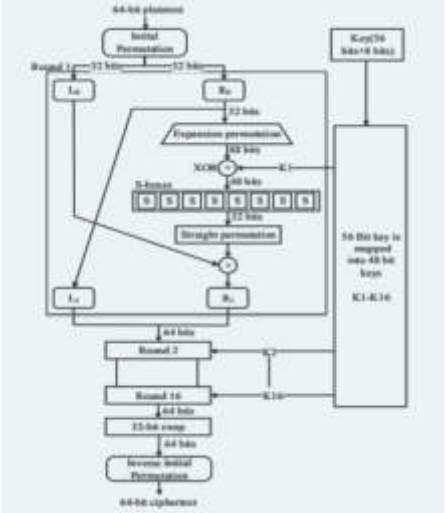

Figure 3 The working of 3DES logical [7]

AES128:

Any combination of data (128 bits) will be supported by AES algorithm. Key length of 128, 192, and 256 bits used. This is referred to as AES-128, AES-192, or AES-256 (depending on the key length). During the process of encryption decryption, AES system goes through 10 rounds for 128-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys to deliver final cipher-text or to retrieve the original plain-text [8].

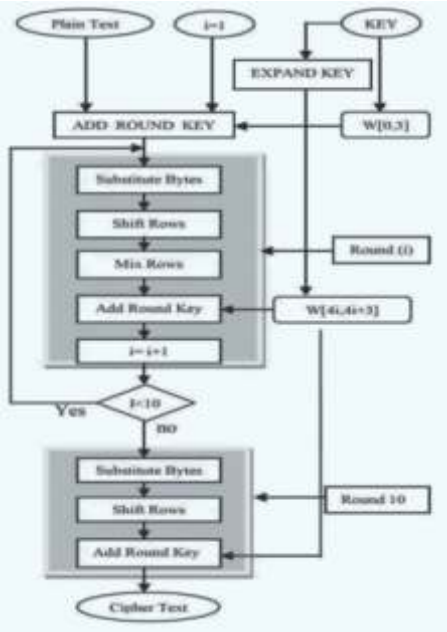

Figure 4 Working principle of AES logical flow

Figure 3 and Figure 4 show the key generation authentication is a flow based process which is fed back to the iterative loop encrypting and decrypting alternatively for asymmetric networks like those based on IoTs.

IV. Results and Analysis

To measure time in this experiment we used Packet internet groper (PING), verifying that no firewalls were implanted and by going directly to the server we were getting the mean time of PING 252 ms. But after the VPN configuration, the mean time reduced to 140 ms. So, by using VPN we are saving 112 ms or nearly 45% and the data is encrypted and secured with the help of L2TP protocols. This method helps the data to be secure as well as fast using known technique (3DES, VPN).

We also initiated the speed test and use trace route to detect that no external intrusions were traced during the time of deployment.

After deployment Figure 5 shows the logical diagram resulting from this experiment,

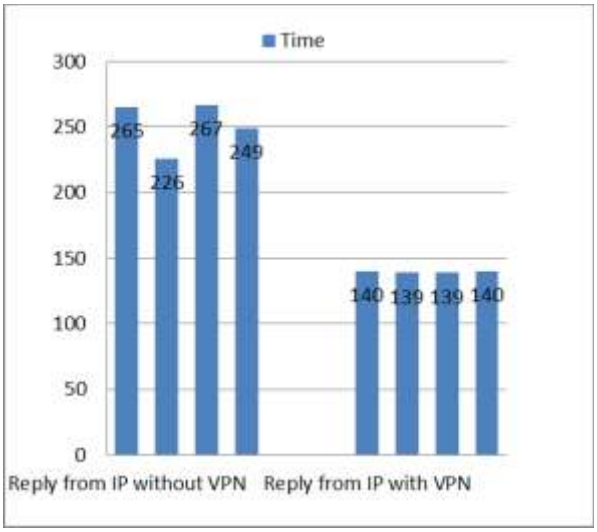

Figure 5 Comparison of the reply from IP with and without VPN, demonstrating the stability of VPN.

a. Analyses:

L2TP protocol is an open source connection oriented protocol which does not require third party application to implement. Additional algorithms are used with the implementation to make the connection secure such as 3DES. The old version protocols such as PPTP (Point to Point Tunneling protocol) were proprietary and now obsolete to work on. This method can be used in the service sector organization and business continuity is required such as the banking sector can use this method in its day to day services which can lower the time frame of data communication and enhance the security for their customers. The L2TP makes fewer nodes which results the packets to transfer towards the destination in less time than usual. This also makes the data transfer secure as the tunnel is single way process and no outer interference can occur.

b. Future Works

Apart from the L2TP protocol, the IPSec technology can also be used in the connectivity between the Cloud firewall and the devices, which may further enhance the results. The results however are not very different from the expected. We used Apple Iphone, which only supports L2TP for VPN technology. Other 3rd party applications can also be used in the process to perform the same experiment with different protocols.

V. Conclusion

The geographical spread of the Cloud technology has raised many security issues to all users individual or organizational. A novel method for authentication and accountability to prevent IDS (Intrusion Detection System) was presented which has enhanced the outcome to a greater extent. Irrespective of the fast data rate acceleration of each technology the security issue must be solved or decreased to a minimal to attain a better integration model. A model is proposed which saves time, and makes data secure by using the L2TP protocol via Cloud to serve IoT devices. The financial sector, commercial markets and other service industries can take advantage to this service. It is expected to see multiple L2TP and integration with IPSec as future work. With the proposed changes, belief between customer and the organization can again be enhanced.

References

[1] D. AB. Fernandes, Security issues in Cloud environments: a survey, Int. J. Inform. Sec. 13 (2) 2014, pp. 113–170.

[2] Christos Stergiou, Secure integration of IoT and Cloud Computing, Elsevier, 2016

[3] MR. Schurgot, “Experiments with security and privacy in IoT networks”, IEEE, 2015, pp. 4.

[4] N. Gonzalez, A quantitative analysis of current security concerns and solutionsfor Cloud computing, J. Cloud Comput.,2012, pp. 1–18.

[5] R. Latif, Cloud computing risk assessment: a systematic literature review, in: Future Information Technology, Springer, Berlin, Heidelberg, 2014, pp. 285–295.

[6] Cloud security alliance, security guidelines for critical areas of focus in Cloud computing v3.0, 2011

[7] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[8] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[9] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, “Performance Evaluation of Cryptographic Algorithms: DES and AES”, IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.