International Journal of Research (IJR) Vol-1, Issue-7, August 2014 **ISSN 2348-6848**

A Comparative Study on AES, DES and Hybrid Encryption Algorithm on VPN Network

S. Pradeepa[1] & **S. Kamalakkannan**[2]

[1]Research scholar, Dept of BCA & IT, VELS University, Chennai, India

[2]Asst professor, Dept of BCA & IT, VELS University, Chennai, India

Abstract

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy and security procedures. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. A well-designed VPN can provide great benefits for an organization. It can: Extend geographic connectivity, Improve security where data lines have not been ciphered, Reduce operational costs versus traditional WAN. In this Paper we proposed IMS (Institute System), using virtual private technology.

Keywords: VPN, Hybrid Encryption, AES, DES Algorithm

Introduction

The VPN market has changed significantly in the past ten years as the Internet has grown and as vastly more companies have come to rely on the Internet for communications. The landscape of VPN products and services offered by a wide variety of vendors continues to evolve. This has caused companies whose networks need protection to become confused about what is and is not a VPN, and the features of the different VPN systems that are being offered to them.

Before the Internet became nearly-universal, a virtual private network consisted of one or more circuits leased from a communications provider. Each leased circuit acted like a single wire in a network that was controlled by customer. The communications vendor would sometimes also help manage the customer's network, but the basic idea was that a customer could use these leased circuits in the same way that they used physical cables in their local network.

The privacy afforded by these legacy VPNs was only that the communications provider assured the customer that no one else would use the

same circuit. This allowed customers to have their own IP addressing and their own security policies. A leased circuit ran through one or more communications switches, any of which could be compromised by someone wanting to observe the network traffic. The VPN customer trusted the VPN provider to maintain the integrity of the circuits and to use the best available business practices to avoid snooping of the network traffic. Thus, these are called trusted VPNs.

As the Internet became more popular as a corporate communications medium, security became much more of a pressing issue for both customers and providers. Seeing that trusted VPNs offered no real security, vendors started to create protocols that would allow traffic to be encrypted at the edge of one network or at the originating computer, moved over the Internet like any other data, and then decrypted when it reached the corporate network or a receiving computer. This encrypted traffic acts like it is in a tunnel between the two networks: even if an attacker can see the traffic, they cannot read it, and they cannot change the traffic without the changes being seen by the receiving party and therefore rejected. Networks that are constructed using encryption are called secure VPNs.

More recently, service providers have begun to offer a new type of trusted VPNs, this time using the Internet instead of the raw telephone system as the substrate for communications. These new trusted VPNs still do not offer security, but they give customers a way to easily create network segments for wide area networks (WANs). In addition, trusted VPN segments can be controlled from a single place, and often come with guaranteed quality-of-service (QoS) from the provider.

A secure VPN can be run as part of a trusted VPN, creating a third type of VPN that is very new on the market: hybrid VPNs. The secure parts of a hybrid VPN might be controlled by the customer (such as by using secure VPN equipment on their sites) or by the same provider that provides the trusted part of the hybrid VPN. Sometimes an entire hybrid VPN is secured with the secure VPN, but more commonly, only a part of a hybrid VPN is secure.

Review on Existing System

The existing institute system is based on paper work. And the documentation of current system is traditional documentation and management (File type). The data of more than 1500 faculty, client is very difficult to maintain. And every year the

number of students is increases. There are many drawbacks of current system. The existing system contains Source enrolment module which is actually paper base and it has several downsides like misplacement of authentication sheet, time consuming etc. The current system has not any facility like intranet. Because of this disadvantage, students cannot get any information about attendance and assignment notification, user control and security, event notification, data and material sharing and many more option. In the institute, all the library work is done by manually. As describe above, all the drawbacks of the existing institute management system should convert in advantages. And because of these several disadvantages, there is a robust requirement of new computerized system.

In this Existing system we have to use Encryption and Decryption Only. It is less security for Password and Uses Data. Manual Paper Work is High, Maintenance Cost High.

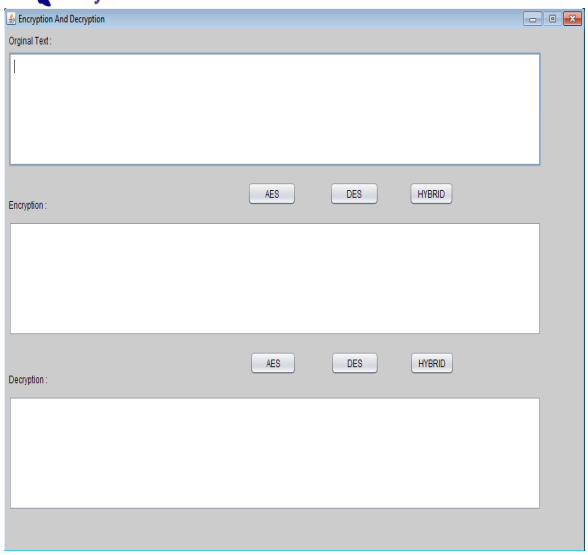
Proposed System

In this Proposed System we have to use hybrid technology it is Combination of the Encryption and Decryption. It is give more secure to Password for hybrid encryption and Decryption and we have to use SOAP Protocol for Email Sending. This proposed system Contains File System Model .It Controls all Department Resources and it is Reduced Manual paper work. It is effectively less cost maintenance.

Results:

Cryptography

Cryptography is used to encrypt and Decrypt the data. In this Project we have to us hybrid encryption. This is new advantages of the project, it is not easy to encrypt with out internal keyword. In cryptography, public-key cryptosystems are convenient in that they not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties). However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem



Hybrid encryption

•Asymmetric encryption uses number theoretic operations and is slower than symmetric encryption that often uses block ciphers.

•Also we often want to encrypt long messages.

•In practice one usually

1.encrypts a randomly chosen symmetric key K using an asymmetric encryption algorithm and then

2. encrypts a message using a symmetric encryption algorithm and K.

•This is called hybrid encryption.

Data Encryption Standard (DES)

DES is a block cipher, with a 64-bit block size and a 56-bit key.DES consists of a16-round series of substitution and permutation. In each round, data and key bits are shifted, permutated, XORed, and sent through, 8s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse [3].

Advanced Encryption Standard (AES)

AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages. To provide security AES uses types of transformation. Substitution permutation, mixing and key adding each round of AES except the last uses the four transformations.

Future Work

I have implemented this VPN tool in IMS (students institute).we can also be proceeded the same VPN tools in some of the industries like healthcare, manufacturing, Retail, banking/Financial and General Businesses.

Conclusion

Virtual Private Network is Reduce the more complexity of the Data Load.A virtual private network (VPN) extends a private network across a public network, such as

the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.A virtual private network connection across the Internet is similar to a wide area network (WAN) link between sites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network.VPN allow employees to securely access their company's intranet while traveling outside the office. Similarly, VPN securely connect geographically separated offices of an organization, creating one cohesive network. VPN technology is also used by Internet users to connect to proxy servers for the purpose of protecting personal identity and location.

References

[1] Alan O.Freier, Philip Karlton, "The SSL Protocol Version 3.0 [EB/OL]". Oct.2008.

[2] Alcatel. Enabling Security in an Increasingly Networked World, Technical Report, May 2008. URL: http://cnscenter.future.co.kr/resource/rsc-center/vendor-wp/alcatel/pkitp.pdf

[3] Apostolopoulos, G.; Peris, V.; Saha, D.; "Virtual Private Network security: how much does it really cost?", Proceedings. IEEE 2008. Volume 2, pp.717 – 725

[4] Avolio, Fred. "Ipsec and VPNs: The Sad/Glad State of Affairs". Avolio Consulting Inc., February10, 2009. URL: ttp://www.avolio.com/columns/ipsec+vpns.html

[5] Blaze, Ioannidis, Keromytis. Trust Management for IPsec. NDSS 2008 paper. NEC Research Index. 2008. URL: http://citeseer.nj.nec.com/blaze01trust.html.

[6] Fontanna, John. "Top Web Services Worry:Security". Network World. URL: http://www.nwfusion.com/news/2008/0121webservices.html

[7] Gartner Company. http://www.gartner.com/.

[8] Hondo, M., Nagaratnam,N., Nadalin,A., "Securing Web Services." IBM Systems Journal 41 (2009): 228-241.

[9] IBM Firewall, Server and Client Solutions, A Comprehensive Guide to Virtual Private Networks, Volume Martin Murhammer, Tim Bourne, Tomas Gaidosch, Charles Kunzinger, Laura Rademacher, Andreas Weinfurter.

[10] IP Virtual Private Networking – Carrier Managed IP Virtual Private Networking http://www.nortelnetworks.com/solutions/ip_vpn/carrier.html

[11] Jingli Zhou, Hongtao Xia, Xiaofeng Wang, Jifeng Yu, "A New VPN Solution Based on Asymmetrical SSL Tunnels", IEEE Proceeding 2007

[12] Masica, Ken. "Understanding the IP Security Protocol: Encryption and Authentication for IP packets". Internet Security Advisor October 2008: 38-42.

[13] T.Dierks and C.Allen, "RFC2246: The TLS Protocol Version 1.0", http://www.ietf.org/rfc/rfc2246.txt, Jan. 2009.

[14] Tanenbaum, Andrew S. Computer Networks. 4th ed. Upper Saddle River, New Jersey: Prentice Hall PTR, 2003. 772-776.

[15] Virtual Private Networks - A Resource Guide for Service Providers, Lucent Technologies, Bell Labs.

[16] VPN Consortium, VPN Technologies: Definitions and Requirements. Jun 2008. URL: http://www.vpnc.org (select VPN technologies)

[17] Wilson,Tim. "VPNs Don't Fly Outside Firewalls. " Internet Week 28 May 2009.URL: http://www.internetwk.com/newslead01/lead052501.htm