*International Journal of Engineering Trends and Applications (IJETA) – Volume 2 Issue 1, Jan-Feb 2015*

RESEARCH ARTICLE OPEN ACCESS

# An Open-SSL Based Algorithmic Approach for Secure Data Transfer in Virtual Private Network

Sourish Mitra[1], Debraj Roy[2], Bidyutmala Saha[3]

Shirsankar Basu[4], Pallabi Das[5]

Department of Computer Science and Engineering

Gurunanak Institute of Technology

Kolkata, 700114

West Bengal – India

## ABSTRACT

Through any enterprise internal network when any remote or mobile users want to perform secure data transmission among different computers we need establish VPN connection to provide better security. The transmitted data within VPN network must be encrypted to ensure the security to protect illegal access, therefore data security of VPN network depends entirely on the strength of the adopted encryption algorithm. *Open SSL* is a general purpose cryptography library that provides an open source implementation of the SSL and TLS protocols. In this paper we propose a secure data transmission algorithm based on Open SSL and VPN. It combines both the characteristics of asymmetric password system and symmetric crypto-system, and provides safe transmission. This algorithm can help us to achieve the goal of fast and securely transmitting information. The sender and receiver programs of this algorithm mainly implement the digital envelope and signature for the transmitted data files. On the whole, the algorithm has such advantages as simple principle, higher security, and so on. Meanwhile it is more convenient to be implemented by hardware and software, better meeting design criteria of encryption algorithm.

***Keywords*:-** Crypto-system, VPN, Digital envelope, *Open SSL*, Asymmetric password system.

## I. INTRODUCTION

When I want to improve network security we need highly secure encryption-decryption algorithm and digital signature technologies. Cryptography [1, 2] is a new study aiming at data encryption, decryption and relevant transformation. Encryption system is generally divided into two types: symmetric and asymmetric crypto-systems. Both symmetric and asymmetric key encryption system has their own advantages, but there are some insurmountable problems at the same time [3, 4]. In this paper, we propose a secure data transmission algorithm based on VPN and Open SSL technique. Cryptography has been widely studied at home and abroad and a lot of practical encryption algorithms are there such as DES, AES, RSA, and DSA and so on. In this paper we describe the secure technology of VPN with the construction VPN server and also analyze the encryption algorithms of AES and ECC with a brief introduction of digital signature and Open SSL.

## II. SECURE VIRTUAL PRIVATE NETWORK WITH TUNNELING

**PE and CE devices**: In order to gain access to the IP backbone, there must be at least one device (such as a switch or a router) at the edge of each customer site that is connected to the service provider's network. These are referred to as Customer Edge (CE) devices. Although these devices are logically part of the customer's network rather than being part of the IP backbone, these devices are in some cases managed (or even owned) by the service provider. Similarly, the device or devices (typically IP routers) that the CE devices connect to in the service provider's network are referred to as Provider Edge (PE) devices. The routers in the service provider network that forward data (including VPN data), but are not providing VPN functionality to a CE device are referred to as Provider (P) devices. A simple VPN illustrating the roles of PE, P and CE devices is shown in the following diagram.

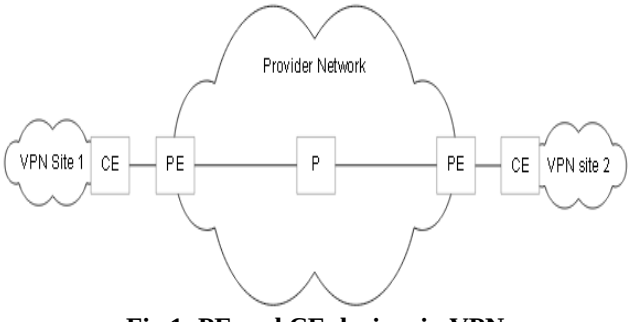



**Fig 1: PE and CE devices in VPNs**

VPNs, whether provider or customer provisioned, fall into one of two broad categories: a) Site-to-site b) Remote access. Site-

to-site VPNs allow connectivity between an organization's (or organizations') geographically dispersed sites (such as a head office and branch offices).Figure 2 illustrates a typical site-to-site VPN. There are two types of site-to-site VPN: i) Intranet VPNs :-Allow connectivity between sites of a single organization, ii) Extranet VPNs:-Allow connectivity between organizations such as business partners or a business and its customers Remote access VPNs (also called access VPNs) allow mobile or home-based users to access an organization's resources remotely. Figure 3 illustrates typical remote access VPNs.

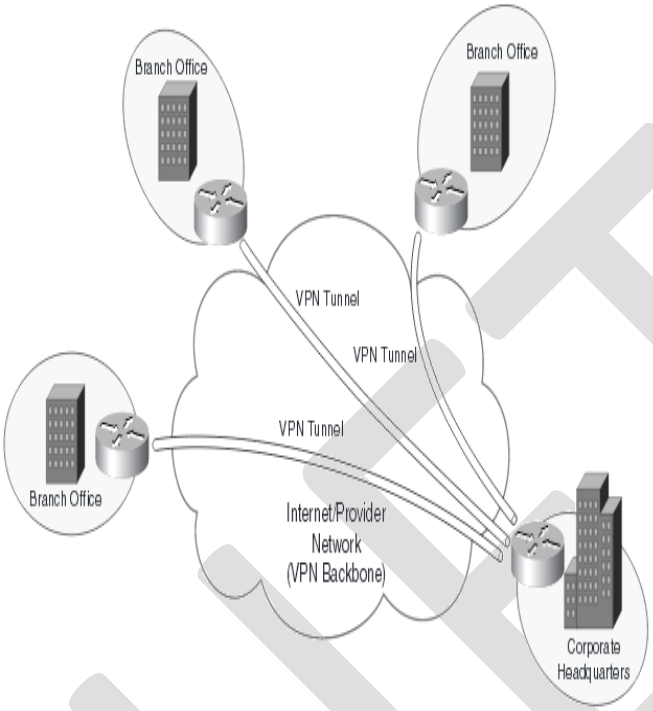



**Fig 2: Typical Site-to-Site VPN**

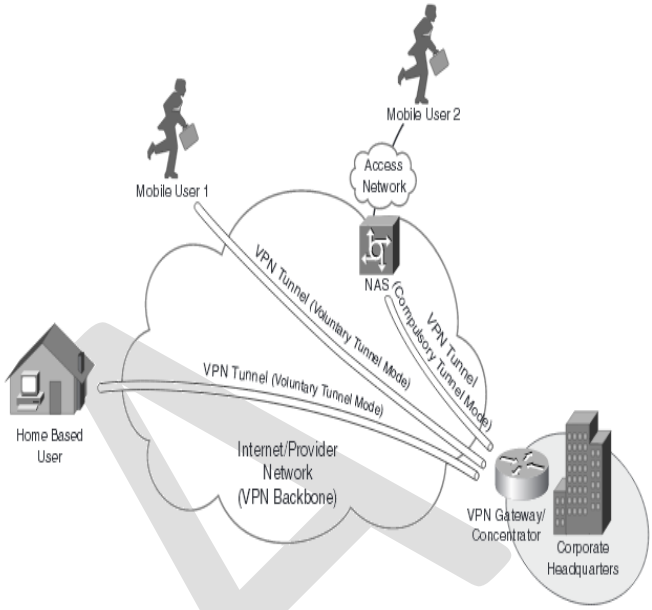



**Fig 3: Remote Access VPNs**

A tunnel is a means of forwarding data across a network from one node to another, as if the two nodes were directly connected. This is achieved by encapsulating the data - an extra header is added to data sent by the transmitting end of the tunnel, and the data is forwarded by intermediate nodes based on an outer header without looking at the contents of the original packet. This is illustrated in the diagram below, which shows data going from A to B being sent through a tunnel between X and Z. The intermediate tunnel no de, node Y, does not need to be aware of the final destination, B, but just forwards the data along the tunnel to Z. (In this scenario, X is known as the ingress to the tunnel and Z as the egress.)

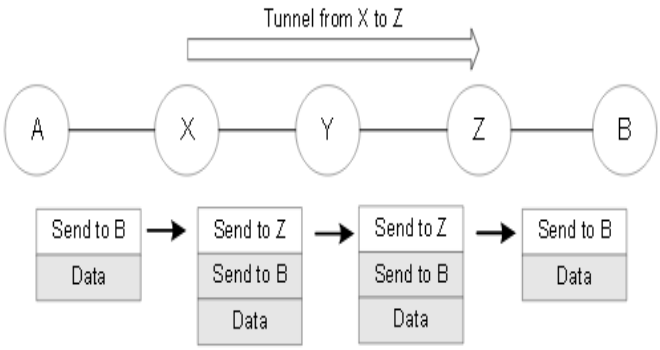



**Fig 4: Tunneling in VPNs**

## III. ENCRYPTION-DECRYPTION ALGORITHM

### A. AES ENCRYPTION ALGORITHM:

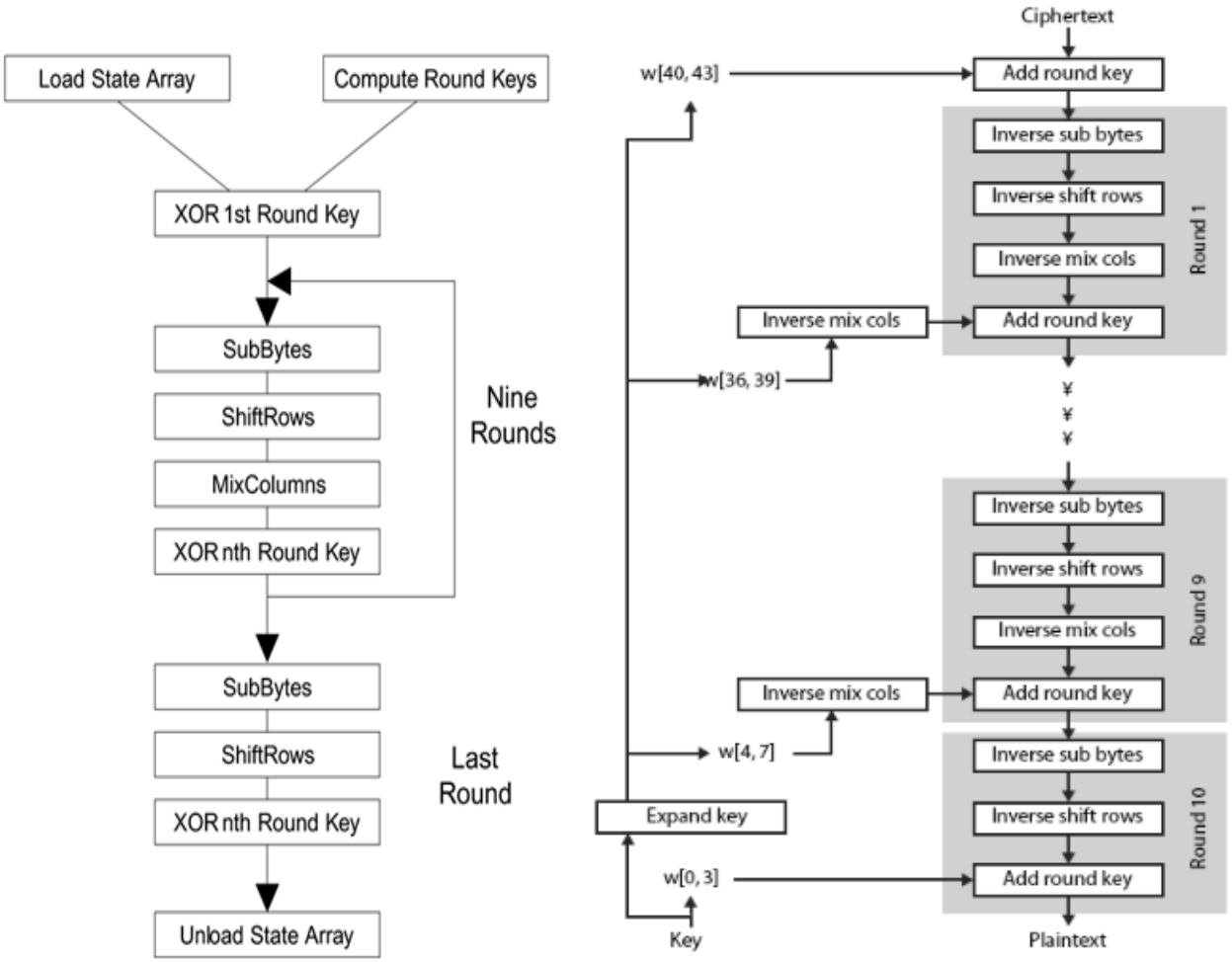



**Fig 5: AES encryption-decryption**

The block and key length of Rijndael encryption algorithm can be specified independently for the 128-bit, 192-bit or 256-bit. Rijndael block cipher algorithm mainly includes the nonlinear components, linear elements and round key. All the operations of the algorithm are complete byte operations. The Rijndael algorithm uses round iterative structure during the encryption process and s-box, which is selected by the inverse operation of multiplication in the finite field GF.

### B. ELLIPTIC CURVE CRYPTOGRAPHY BASED ALGORITHM

Elliptic curve cryptography is gaining popularity because it offers similar security to traditional systems, such as Ron Rivest, Adi Shamir and Leonard Adleman (RSA), but with significantly smaller key lengths. It is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. The ECC method was employed during encryption of text data, the below flow chart shows the steps involved in generating public and private key to encrypt and decrypt the data respectively.

Step 1: Generate domain parameters
Step 2: Calculate the generator point.
Step 3: Generate private key and public key
Step 4: Encode the message to generator point.
Step 5: Select random numbers and Choose public key
Step 6: Encrypt generator point to cipher text.
Step 7: Send cipher text.
Step 8: Use private key to decrypt the cipher text and get generator point.

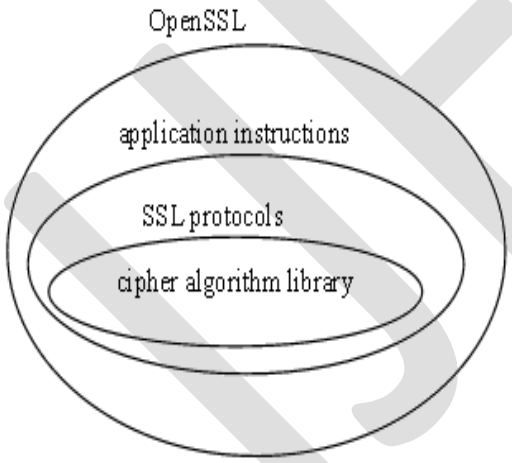
Step 9: Message in generator point is decoded.

### C. DIGITAL SIGNATURE

Digital signature refers to the data obtained by the users to encrypt the Hash digest of original data with their own private key. The data receiver uses the sender's public key to decipher the digital signature attached on the original information to get Hash digest, and compares it with the Hash digest generated by the original data, thus he can be sure whether the original information is to be forged or not. This helps to ensure that the source of the authenticity and the integrity of data transmission.

## IV. INTRODUCTION TO OPEN-SSL

The Open SSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library. SSL is the abbreviation of secure socket layer, which can provide secret transmission on the Internet. Open SSL has realized the protocols of SSL/TLS (Transport Layer Security). Generally speaking, Open SSL is divided into three parts, that is, SSL protocols, cipher algorithm library and application instruction.




## V. OUR PROPOSED ALGORITHM FOR SECURE DATA TRANSMISSION

### A. PURPOSE OF PROPOSED APPROACH

Purpose of this approach is mainly ensuring the security in VPN data transmission by using the concept of Open-SSl, where we want to design an algorithm which is based on the combination of public key cryptography and symmetric cryptography. We want to propose an innovative cipher technology related information security transmission technique where we combine the advantages of two kinds of crypto-systems to put forward a kind of secure data transmission algorithm. Here we encrypt the plaintext with the symmetric cipher algorithm, and then encrypt the key and digital signature belonged to the symmetric encryption algorithm with the public key algorithm. The sender encrypts the plaintext T with the key named $Key_{AES}$ belonged to the AES algorithm. To ensure the security of the cipher algorithm and simplification of key management, the sender uses the key $Key_{AES}$ only once (that is, one at a time). The working process of the secure data transmission algorithm is listed below.

### B. PROPOSED ENCRYPTION –DECRYPTION PROCESS DISCUSSION STEP BY STEP

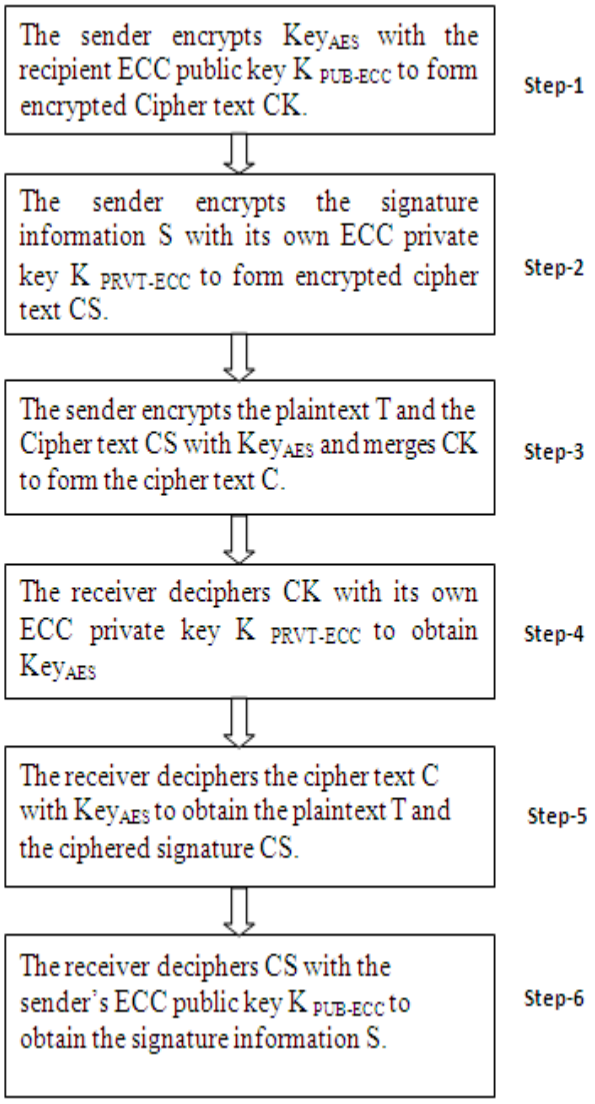



**Fig-6. Our Proposed approach**

## VI. EXPERIMENTAL ANALYSIS

We assume that one 1MIPS computer can perform 4x104 times of elliptic curve addition per second, this is an optimistic estimate. Therefore the number of one 1MIPS computer can perform elliptic curve addition is $(4x10^4)$ x (60 x 60 x 24 x365) $\approx 2^{40}$.Similarly, if 10,000 computers can perform parallel process, each has a speed of 1000MIPS per second, then the modulus length will reach $n \approx 2^{160}$ it will take 6,000 years to solve the ECDLP problem. A single calculation of elliptic curve discrete logarithm can only reveal one user's private key. Thus, under the existing conditions of solving methods and computing power, it is impossible to solve the ECDLP problem from the aspect of calculation quantity, so the security of ECC is ensured.

## VII. CONCLUSION

Our proposed algorithm combines characteristics of public key cryptography and symmetric cryptography. As is known to all, the former is easy to distribute keys and the latter is easy to calculate and provides a good and fast way for the secure information transmission. It has simple principle and high security to some extent, and greatly meets the design criteria for the encryption algorithm. This algorithm can help us to achieve the goal of fast and securely transmitting information. The sender and receiver programs of this algorithm mainly implement the digital envelope and signature for the transmitted data files. It is more convenient to be implemented by hardware and software, better meeting design criteria of encryption algorithm. Besides, our practice in water conservancy practice shows that the adoption of this algorithm can well realize fast and secure information transmission.

## REFERENCES


[1] Man Young Rhee, Internet Security: cryptographic principles, algorithms and protocols, Beijing: Tsinghua University Press, 2007.

[2] John Talbot, Dominic Welsh, Complexity and Cryptography An Introduction, NewYork: Cambridge University Press, 2006.

[3] ZHANG Yan, LIN Ying, HAO Lin,"Summarize of Elliptic Curve Crypto-system Research", Computer Engineering, vol.30, pp. 127-129, 2004.

[4] Mandy Zandra Seet, Elliptic Curve Cryptography Improving the Pollard Rho Algorithm[D], The University of New South Wales, 2007

[5] Wang chun hai, The instances of VPN network Construction, Beijing: Science Press, 2008.

[6] CHEDDAD A, CONDELL J, CURRAN K, et al. A Hash-based image encryption algorithm [J]. OptComm., 2010, 283:879-893.

[7] TAO R, MENG X Y, WANG Y. Image encryption with multiorders of fractional Fourier transforms[J]. IEEE.