AN INNOVATIVE KIND OF SECURITY PROTOCOL USING FUSION ENCRYPTION IN VIRTUAL PRIVATE NETWORKING

M.Sreedevi[1], Dr. R. Seshadri [2]

[1]Research Scholar, C.S.E, S.V.U.C.E, Tirupati, A.P
srikundu@yahoo.co.in
[2] Director, Computer Center, S.V.U, Tirupati, A.P

ABSTRACT

As a business grows, it might expand to multiple branches across the country and around the world. To maintain things running ably, the people functioning in those locations require fast, secure and consistent way to share information across computer networks. In addition, mobile employees like sales people require evenly secure and reliable approach to connect to their business's computer network from remote locations. One popular technology to accomplish these goals is a virtual private network. A VPN is a private network that uses a public network usually the Internet to connect remote sites or users together. It enables us to transmit the data between two computers across a shared or public network in a manner that follows the properties of a private link. The basic requirements for VPN are User Authentication, Address Management, Data Compression, Data Encryption and Key Management. The private links are launched in VPN using Point-to-Point Tunneling Protocol (PPTP) and Layer-Two-Tunneling Protocol (L2TP). These protocols satisfy VPN requirements in five layers. In user authentication layer, several trusted authorities using Extensible Authentication Protocol (EAP) do the authentication process. In fourth layer the data encryption part using RC4 called Microsoft-Point-to-Point Encryption (MPPE) scheme. The aim of this paper, instead of multiple trusted authorities we focus single trusted authority using public key cryptography RSA in EAP and also we include AES stream cipher algorithm instead of RC4 for MPPE. We propose new type of fusion encryption technique using AES for encryption and decryption and RSA used for key management.

KEYWORDS

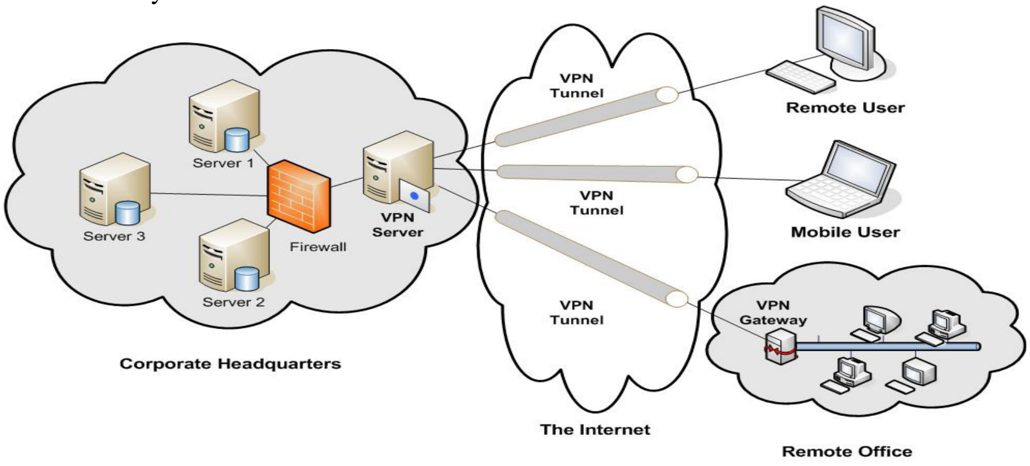
Wireless communication, security, authentication, Tunnel,, Protocol

1. INTRODUCTION

Over recent years, the market for wireless communications has the benefit of tremendous growth. Wireless technology at present accomplishes or is capable of reaching virtually every location on the facade of the earth. Hundreds of millions of people exchange information every day by means of pagers, cellular telephones and other wireless communication goods. With incredible achievement of wireless telephony and messaging services, it is hardly amazing that wireless communication is beginning to be useful to the realm of personal and business computing. No longer hurdle by the harnesses of wired networks, people will be competent to access and distribute information on a global scale nearly everywhere they project. The security of the communication is mainly based on the cryptographic algorithms. The VPN [7] is the major role for secure communication in an insecure network. The portion of the connection in which the data is encapsulated is known as the tunnel and some portion of the connection is encrypted this data known as VPN connection. In an Internet solution, few Internet connections through Internet service providers and VPN server computers can serve the remote networking needs of hundreds or thousands of remote clients. By using VPN server, the network administrator can ensure that only those users on the organization network who have appropriate permissions can establish the VPN connection with the VPN server and gain access

DOI : 10.5121/ijdps.2012.3116

to the protected resources of the computer. All the VPN connections can make sure the data confidentiality.



1.1. Types of VPNs

There are primarily three types of VPNs [9]. *L AN N Interconnect VPN, Dial- Up VPN, and Extranet VPN.*

- ***LAN Interconnect VPN***

Helps to interconnect different LANs located at different geographical areas over shared network infrastructure. Typically it is used to connect small offices with their regional main office. The advantages of this type, is that it is very flexible, i.e., both the capacity of a link and the number of necessary link can be changed whenever needed.

- ***Dial-up VPN***

Sustains mobile and telecommuting employees in accessing the company's Intranet as of remote locations. This type of VPN may use either L2TP, or PPTP protocols as described earlier in the tunneling section. The dial-up VPN has two main advantages. It eliminates the need to manage and maintain a RAS, as this is usually done by the service provider. It also provides considerable cost saving as it result in a significant reduction in long distance and Toll Free calls.

- ***Extranet VPN***

Combines the architecture of both LAN interconnects and dial-up VPNs. This kind of VPNs enables vendors, suppliers, and customers to access specific areas of the company's Intranet. The allowed specific area is denoted as Demilitarized Zone (DMZ). The main advantage of Extranet VPNs is that it helps in several e-commerce areas including efficient inventory management and electronic data interchange.

In VPN, generally two types of protocols are mainly used for secure transmission. The PPTP permits multi protocol traffic to be encrypted and then encapsulated in an IP header to be sent across an IP inter network. L2TP permits multi protocol traffic to be encrypted and then sent over any medium that supports datagram delivery.

1.2. BASIC VPN REQUIREMENTS

The basic requirements are mainly focused in VPN [7, 8].

• *Scalability:* allows a solution to grow as the business grows and eliminate forklift upgrades.

• *Performance:* VPN should be able to process close to the input line speed or to the line speed of the slowest link.

- *Reliability:* VPN should be available at all the time, reliability must include redundancy features to
  allow automatic recovery of failed devices with limited interruption of service.
- *Usability:* VPN needs to be very easy to use and understand by the end-users.
- *Ease of Management: T*he management platform must have a simple way to design security
  policy, an easy way to distribute that policy, and an easy way to simultaneously manage a large
  number of devises.
- *Interoperability:* The VPN equipment must be interoperable according to industry standards and
  protocols.
- *Protocol Support: A*t least the following protocols must be supported. IPSec, PPTP, L2TP, and
  RADIUS.
- *Service Level Agreement (SLA):* It is necessary to negotiate with service provider a SLA to
  provide a consistent throughput and service to the connected locations.
- *Seamless Integration:* VPN solution must fit into an organization network system as a complementary service. In the User authentication requirement is to identify the user. The address management is mainly used for the addresses of the client machine will keep secret. The data compression mainly used for when the data is large. The data encryption management is used for secure data exchange. The key management effectively manages the key used for encryption and decryption. In user authentication part EAP protocol followed for user identity checking. In data encryption part MPPE algorithm mainly used RC4 stream cipher[1,2].

2. Related works

Baijian Yang et al [10] proposed a scheme to incorporate VPNs and multi-homed networks. The incorporation of the two techniques is challenging and beneficial. The proposed solution can be implemented either at networking layer or at application layer by changing the cost of the routing table on the fly. The resulting routing paths can provide auto fail over features and are helpful to balance the network traffic. In the future, they would like to further test the performance of multi-tunnel solution on different platforms and a variety of networks to gain deeper understanding as how the scheme impacts the network and the end users. They would also like to propose a load balancing scheme that is more appropriate for VPN connections. In addition, a general solution to support NAT over IPSec will be examined.

Christoforos Ntantogian et al [11] proposed a security protocol that enhances the authentication procedure of EAP-SIM by employing the “strong” authentication mechanism of IKEv2. Thus, the identified security weaknesses of EAP-SIM and the accompanied vulnerabilities described above are eliminated. The mobile user and the AAA server are authenticated each other using protected EAP-SIM messages by IKEv2. In addition, the NAS is authenticated to the user by using its certificate within the secure IKEv2 negotiation. On the other hand, the main drawback of the proposed protocol is that its deployment may increase the computational overhead of the involved entities compared to the pure EAP-SIM.

M. C. Niculescu et al [12] proposed mobile IP security in VPNs. They firstly examined the ESP, the AH and the IKE protocols defined in the IETF's IPSec architecture. Based on these protocols, protection against denial of service, passive eavesdropping, session stealing and other active attacks in campus intranets were discussed. These discussions were further extended to the Internet-wide context, where the use of the secure tunnel as a main protection mechanism was examined. The recurring pattern in the counter measures against all of these attacks is that security mechanisms and services concern authentication and encryption techniques to prevent security attacks. Security mechanisms, services and protocols to provide communications throughout the Internet with confidentiality, authentication and integrity are under elaboration within the IETF. The works cover both IPv4 and IPv6 and ranges from the link layer up to the application layer.

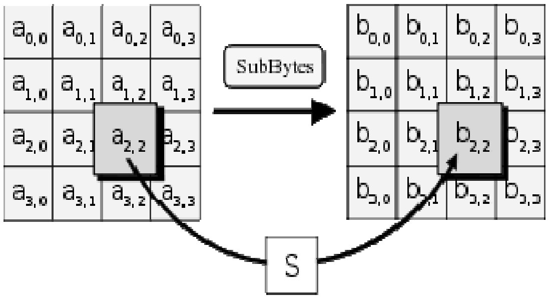
3. AES-ALGORITHM

3.1. Overview of AES Cipher

The AES algorithm takes an input block of a definite size, typically 128, and generates a corresponding output block of the similar size. The transformation needs a second input, which is the secret key. It is significant to recognize that the secret key can be of any size (depending on the cipher used) and that AES uses different key sizes: 128, 192, 256 and 512 bits. AES was believed to provide much more security without any limitations. In AES algorithm, the number of rounds involved in the encryption and decryption depends on the length of the key and the number of block columns. So, the number of rounds is increased to improve the strength of the AES. The strength of the AES algorithm is enhanced by increasing the key length and there by the number of rounds is increased in order to provide a stronger encryption method for secure communication. The Advanced Encryption Standard (AES) [5] is a computer security standard that became effective on May 26, 2002 by NIST to replace DES. The cryptography scheme is a symmetric block cipher that encrypts and decrypts 128-bit blocks of data. Lengths of 128, 192 and 256 bits are standard key lengths used by AES [2-4]. The algorithm consists of four stages that make up a round, which is iterated 10 times for a 128-bit length key, 12 times for a 192-bit key and 14 times for a 256- bit key. There are four stages that AES [14] operates as explained below.

The first stage "SubBytes" transformation is a non-linear byte substitution for each byte of the block as follows.

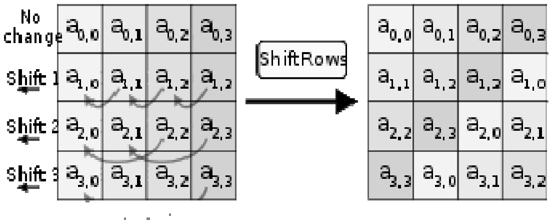
The Sub Bytes step


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

In the Sub Bytes step, every byte in the state is substituted with its entry in a fixed 8-bit lookup table, *S*; $b_{ij} = S(a_{ij})$. In the Sub Bytes step, every byte in the matrix is revised using an 8-bit substitution box , the Rijndael S-box. This operation offers the non-linearity in the cipher. The S-box used is developed from the multiplicative inverse over GF (2^8), known to have excellent non-linearity properties. To circumvent attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine renovation. The S-box is also preferred to avoid any preset points, and also any opposite preset points.

The next stage "ShiftRows" transformation regularly shifts (permutes) the bytes within the block as follows.

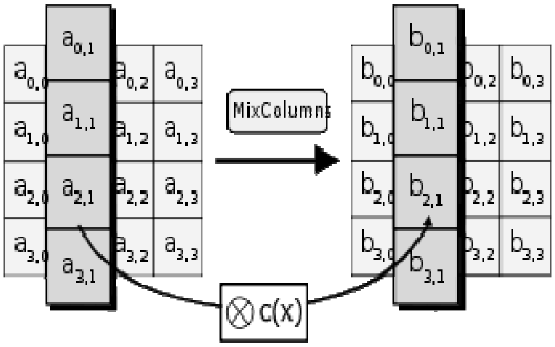
The Shift Rows step


No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,2}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,2}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

The Shift Rows stage operates on the rows of the state; it cyclically shifts the bytes in every row by a definite offset. For AES, the first row is left unaffected. Every byte of the second row is shifted one to the left. Likewise, the third and fourth rows are shifted by offsets of two and three respectively. For the block of size 128 bits and 192 bits the shifting pattern is the similar. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). In the case of the 256-bit block, the first row is unchanged and the shifting for second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively - this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks.

The third stage "MixColumns" transformation groups 4-bytes together forming 4-term polynomials and multiplies the polynomials with a fixed polynomial mod (x^4+1).

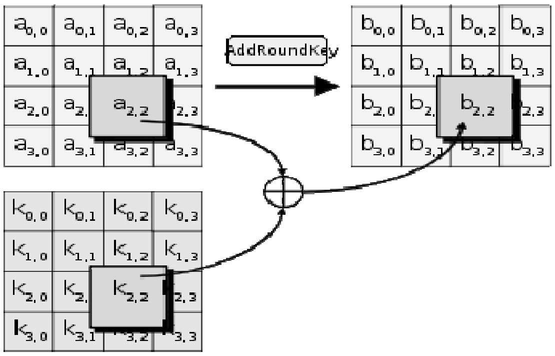
The Mix Columns step


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

In the Mix Columns step, each column of the state is multiplied with a fixed polynomial *c(x)*. In the Mix Columns step, the four bytes of each column of the state are combined using an invertible linear transformation. The Mix Columns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes.

The fourth stage "AddRoundKey" transformation adds the round key with the block of data as follows.

The AddRoundKey step


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

In the AddRoundKey step, all bytes of the state is combined with a byte of the round subkey using the XOR process .In the AddRoundKey stage, the subkey is combined with the position. For each round, a subkey is derived from the foremost key using Rijndael key list; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the equivalent byte of the subkey with bitwise XOR.

In most ciphers, the iterated change (or round) generally has a Feistel Structure. Typically in this structure, some of the bits of the intermediate state are transposed unaffected to an additional position (permutation). AES does not have a Feistel structure but is poised of three distinct invertible transforms based on the Wide Trial Strategy design method. The Wide Trial Strategy design method provides resistance against linear and differential cryptanalysis.

In the Wide Trail Strategy, every layer has its own function:

* The linear mixing layer: guarantees high diffusion over multiply rounds

* The non-linear layer: analogous application of S boxes that have the best possible worst-case nonlinearity properties.

* The key addition layer: a simple XOR of the round key to the intermediate state

The Rijndael function for AES defined a cipher in which the block length and the key length can be separately specified to be 128, 192 and 256 bits. exploit of three key size alternatives but confines the block length to 128 bits.

The algorithm was designed to have the following characteristics:

* Resistance against all known attacks

* Speed and code compactness on a wide range of platforms

* Design simplicity

* Input to the encryption algorithm, decryption algorithm in a single 128 bit block

In AES, four different stages are used

i. Substitution bytes

Use S-box to perform byte-to-byte substitution of the block

ii. Shift rows

A simple permutation

iii. Mix columns

A substitution that makes use of arithmetic

iv. Add round key

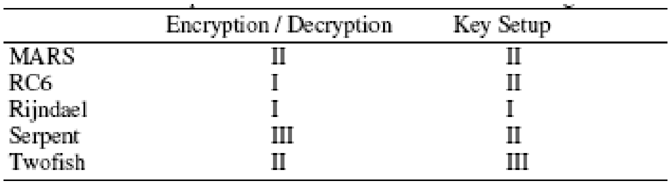
A straightforward bit wise XOR of the existing block with the section of the extended key. In add round key stage makes use of the key. Any other stage applied at the beginning or end is reversible without knowledge of the key, this method is more efficient and secure. Each stage is easily reversible. For the alternative byte, shift row, mix column stages, as inverse purpose used in the decryption algorithm. For add round key stage, the inverse is achieved by XOR the similar round key to the block. The decryption algorithm is not the same for the encryption algorithm. This is a result of the meticulous structure of the AES.

3.2. AES-Rijindael

We analyze various AES-standard algorithms like MARS, RC6, Rijndael, Serpent, and Twofish for encryption and decryption performance, key scheduling performance and overall performance. An enormous amount of information has been gathered on the speed of the AES-algorithms on a variety of software platforms. The Table 1 summarizes the overall performance of the finalists on the various platforms when using 128-keys. Furthermore, an overall performance table is also built-in.

The following Table 1 shows the overall performance of various AES algorithms and the graph-1 represents diagrammatic representation. In this overall performance the MARS provides average performance for encryption, decryption and key setup. RC6 provides regular to high-end performance for encryption and decryption and average performance for key setup. Rijndael provides always high-end performance for encryption, decryption and key setup, even though performance decreases for the 192 and 256-bit key sizes. Serpent provides always low-end performance for encryption and decryption and platform-dependent performance for key setup. Twofish provides platform dependent performance for encryption and decryption and consistently low-end performance for key setup.

Table 1: Overall performance of various AES standard algorithms



	Encryption / Decryption	Key Setup
MARS	II	II
RC6	I	II
Rijndael	I	I
Serpent	III	II
Twofish	II	III

3.3. Overview of RSA

In this fusion Encryption technique, we take the data to encrypt by AES-Rijndael using a key. The key should be received as an encrypted form using RSA from user. A public-key-encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique. The RSA algorithm based on the fact that there is no efficient way to factor very large numbers. The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to replace a secret key discretely. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the complexity of factoring huge integers.

Party A can launch an encrypted message to party B without any previous exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can confirm it using A's public key.

Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time. The RSA system is a block cipher in which the plain text and cipher texts are integers between 0 and n-1 for some n. We inspect RSA in this part in some detail, beginning with an explanation of the algorithm. Then we inspect some of the computational and cryptanalytical of RSA.

3.4. Description of the Algorithm

Plain text is encrypted in blocks, with every block having a binary value fewer than some number n. That is, the block size must be fewer than or equal to log2 (n); in practice, the block size of 2k bits, where $2^{k}<n<=2^{k}+1$. Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$C = M^{e} \bmod n$

$M = C^{d} \bmod n = (M^{e})^{d} \bmod n = M^{ed} \bmod n$

Both sender and receiver must recognize the value of n. The sender will know the value of e and only the receiver knows the value of d. Thus, the public key encryption algorithm with a public key of KU = {e, n} and private key of KR = {d, n}. For this algorithm to be satisfactory for public key encryption, the following requirements must be met:

* It is possible to find values of e,d, n such that $M^{ed} = M \bmod n$ for all M<n.

* It is comparatively easy to calculate M^{e} and C^{d} for all values of M<n.

* It is infeasible to determine d given e and n. For now, we focus on the first question; we need to find a relationship of the form

$M^{ed} = M \bmod n$

According to the Euler’s theorem, given two prime numbers, p and q and two integers, n and m, such that n= pq and 0<m<n and arbitrary integer k, the following relationship holds:

$m^{k \varphi (n) +1} = m^{k(p-1) (q-1) +1} \equiv m \bmod n$ where φ (n) is the Euler function, which is the number

of positive integers less than n and relatively prime to n.

Suppose p, q prime, φ(pq) = (p-1)(q-1). Thus, we can achieve the desired relationship if

$ed \equiv k \varphi (n) + 1$

This is equivalent to saying:

$ed \equiv 1 \bmod \varphi (n)$

$d \equiv e^{-1} \bmod \varphi (n)$

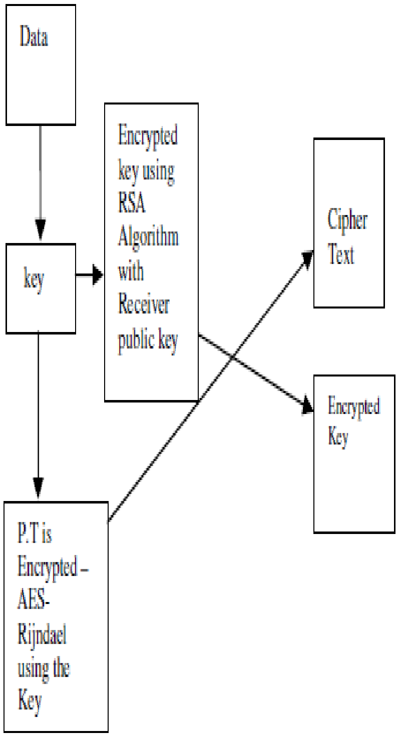
That is, e and d are multiplicative inverses mod φ (n). Make a note of that, according to the convention of modular arithmetic, this is true only if d (and therefore e) is relatively prime to φ (n). Equivalently, gcd (φ (n),d) = 1.

We are now ready to state the public-key RSA crypto scheme. The ingredients are the following:

p, q, two prime numbers (private, chosen) n=pq (public, calculated) e, with gcd((φ (n),e)=1; 1<e<(φ (n) (public, chosen) $d = e^{-1}$ mod (φ (n) (private, calculated)

The private key contains {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates $C = M^e$ (mod n) and transmits C. On receipt of this cipher text, user A decrypts by calculating $M = C^d$ (mod n).

So, $^{ed} \equiv M$ mod n. Now, C = Me mod n $M = C^d$ mod n $\equiv (M^e)^d$ mod n $\equiv M^{ed}$ mod n $\equiv$ M mod n


Data
key
Encrypted key using RSA Algorithm with Receiver public key
Cipher Text
Encrypted Key
P.T is Encrypted – AES-Rijndael using the Key

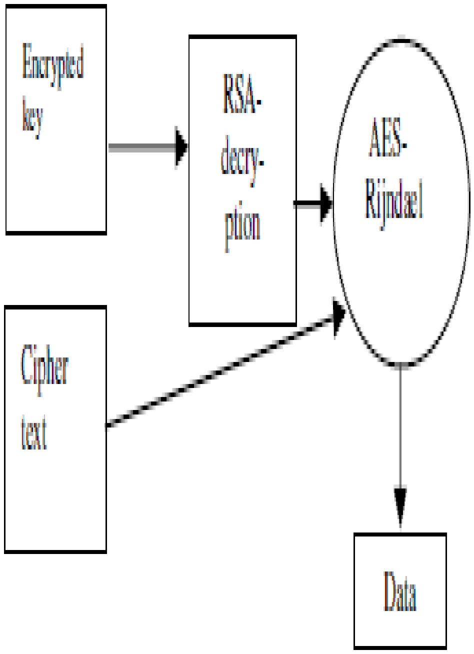


Fig. 1a: Sender side encryption process (Ex. VPN client)

Fig. 1b: Sender side encryption process (Ex. VPN Server)

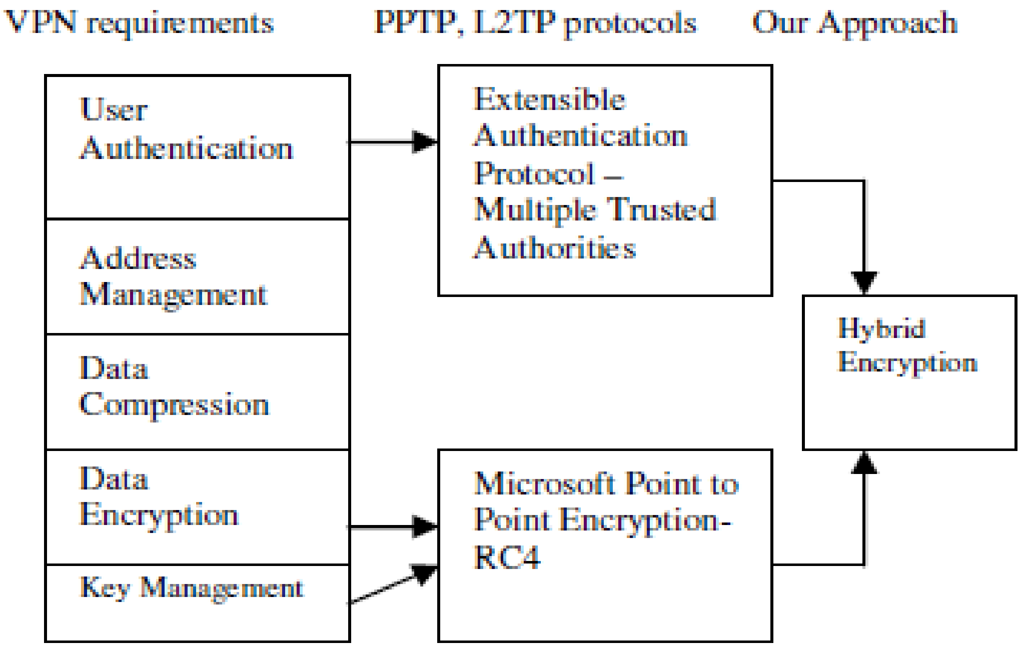


Fig. 2: New proposed amalgam encryption protocol

3.5. Overview of proposed system

In this paper we are going to perform new type of encryption technique in EAP and MPPE. In Amalgam Encryption, a key is agreed between the VPN client and the VPN server [6]. This key can be dynamic or can even be static. A key of length says, 128 bits are chosen. This is used to encrypt the plain text using AES Rijndael steam cipher algorithm. The key is encrypted using the RSA algorithm with receiver's public key.

Both are attached and sent. Now, the VPN client can apply its private key to decipher the key and using the key with AES-Rijndael can decrypt the Cipher text to get back the plain text. The main advantage of this method is that it takes much lesser time when compared to normal encryption with secure key transformation process. The design of our system shown in Fig. 1a and b. This proposed fusion encryption method is used instead of RC4 in MPPE. This will be illustrated in Fig. 2. The above protocol is only our view of to implement fusion encryption technique in data encryption and user authentication part. This protocol is to reduce the user authentication and data encryption layers into a single protocol layer.

The security of the proposed schemes. Basically, the security of the projected schemes is based on the difficulty of cryptographic hypothesis as follows.

1. The security part of the AES-Rijndael algorithm is very high than other stream ciphers like RC4, RC5, RC6 and so on.

2. The RSA is very high securing than other public key cryptographic algorithms. But the RSA is very slow when we try to convert large number of data.

To avoid this we used our proposal RSA to convert only the key values.

4. CONCLUSIONS

In this study we presented a new type of fusion encryption protocol for VPN data encryption and key management. In this approach the VPN server is the trusted authority. The VPN client initiates the request; the VPN server gives the key value. Using the key value VPN client securely encrypt data with the help of AES-Rijndael. Then the key value encrypted using receivers public key with the help of RSA. Then these encrypted values integrated together and send to the receiver. The receiver using its private key and RSA identify the original key value. Using original key the encrypted data is decrypted with the help of AES-Rijndael. The main advantage of this method is that it takes much lesser time when compared to normal encryption with secure key transformation process. Compared to the previous approach, the proposed approach is more secure to transfer sensitive information through public network.

REFERENCES

[1] James, N., E. Barker, L. Bassham, W. B urr, M. Dworkin, J. Foti and E. Roback, 2000. Report on the development of the advanced encryption standard (AES). Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.

[2] Srdjan,C. L.Buttyan and J.-P. Hubaux, 2003. Self-organized public-key management for mobile ad hoc Networks. IEEE Trans. Mobile Computing: pp: 52-64.

[3] Philip, R., M. Bellare and J. Black OCB, 2003. A block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Information System and Security, pp: 365-403. [4]Mary, R.T., A. Essiari and S. Mudumbai, 2003..

[5] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag, Berlin Heidelberg, 2002.

[6] Jingsha He, Blight, D., & Chujo, T. (2000). A unified architecture for virtual private networking. Paper presented at the International Communication Technology.

[7] Venkateswaran, R. (2001). Virtual private networks. *IEEE potentials, 20*(1), 11-15.

[8] Jingsha He, Blight, D., & Chujo, T. (2000). A unified architecture for virtual private networking. Paper presented at the International Communication Technology.

[9] Ferguson, P., & Huston, G. (1998). *What is a VPN*. Retrieved, from the World Wide Web: http://www.clark.net/timw/vpn/Tech/vpn.pdf.

[10] Baijian Yang and Tianguang Gao," Building a Secure and Reliable Network via Multi-homed VPN", Session IT 303-088, Proceedings of the 2006 IJME - INTERTECH Conference.

[11] Christoforos Ntantogian and Christos Xenakis, "A security protocol for mutual authentication and mobile VPN deployment in B3G networks ",The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications ,2007 .

[12] M. C. Niculescu, Elena Niculescu and I. Resceanu, "Mobile IP Security in VPNs", Proceedings of the 5th WSEAS Int. Conf. on Data Networks, Communications & Computers, Bucharest, Romania, October 16-17, 2006.

[13] "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication197, November 26, 2001.

[14] Dunkelman, Nathan Keller, and Adi Shamir. In *ASIACRYPT'10*, volume 6477 of Lecture Notes in Computer Science, pages 158–176. Springer, 2010.

Authors

M.Sreedevi , MITS, Madanapalle , inward B.Tech in Electronics and communication Engineering from S.V.U.C.E, Tirupati, Andhra Pradesh, M.Tech Degree in Information Technology from Punjabi University , Patiala , Punjab and pursuing Ph.D in Cryptography and Network Security from S.V University, Tirupati, and having 13years of professional experience.

Dr.R.Seshadri ,S.V.U, Tirupati, Received B.Tech Degree in Electronics & communication Engineering from Nagarjuna university in 1981,Received M.E Degree from PSG College of technology, Coimbatore in 1984 , Received Ph.D in **Simulation modeling and compression of ECG signals** from S.V.UNIVERSITY. He had 29 years of Professional experience.