http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 5 No. 1, June 2016: 15 - 30
e-ISSN: 2289-2192

# DESIGN AND EVALUATION OF A VIRTUAL PRIVATE NETWORK ARCHITECTURE FOR COLLABORATING SPECIALIST USERS

AKRAM KARGAR RAEESPOUR SISTANI
AHMED MOOSAJE PATEL

## ABSTRACT

The expansion of communication systems is the undeniable advantage of the most contemporary digital technologies. However, when a specialist user such as an inventor or an idea owner communicates through a communication system, their intellects are exposed to theft. Upon the analysis of the requirements of such users, it became evident that in order to implement a global, reliable, yet secure system for specialist users, designing a network architecture that provides centralized private connectivity is crucial. This paper proposes a network architecture that provides centralized private connectivity and accommodates the requirements of the network infrastructure of such a system. The proposed virtual private network (VPN) architecture is designed to provide a trusted environment with centralized control and distributed networking, which is different from existing VPN models. It is entitled as Inventor-Investor Network (IINet) and the name is derived from its significant benefits for inventor and investor sets of users. The real experimental IINet prototype is implemented using OpenVPN. For the purpose of evaluation, round trip time (RTT) is measured and reported as the performance metric based on the different encryption ciphers and digest ciphers as the network metrics.

Keywords: Communication systems, Network architecture, Virtual private network, Round trip time, Inventor-investor Network

## INTRODUCTION

Virtual Private Network (VPN) enables clients and partners to use standard internet public network and high-speed lines to access closed private networks (Hua, 2011). Utilizing VPNs across the internet has achieved wider acceptance as a way to offer more cost-effective access to private data, therefore, in this paper it was chosen to be applied in the network connecting specialist user. VPNs are divided into two architecture types: Site-to-Site VPN and Remote access. Remote access VPN enables a home user to access to the corporation data through public network remotely. On the contrary, Site-to-Site VPNs provide connectivity between geographically dispersed sites of an organization (Lewis, 2006). Figure 1 illustrates Remote Access VPN architecture and Figure 2 illustrates Site-to-Site VPN architecture. This paper proposes a new network architecture that applies VPN to facilitate centralized private connectivity and satisfy the requirements of collaborating specialist users.

The remainder of this paper is organized as follows: first, VPN technologies is reviewed and summarized briefly. Thereafter follows a discussion about which VPN category has more adaption with respect to the requirements of proposing novel network architecture. Then the network architecture for collaborating specialist users is proposed, followed by a discussion on how Secure Socket Layer/ Transport Layer Security Virtual Private Network (SSL/TLS VPN) affects this network architecture. Finally, the prototype of the proposed architectural system implementation is presented and evaluated, which includes the experimental setup, analytical modelling, data collection from the experimental results, its scrutiny and assessment, and final conclusion.

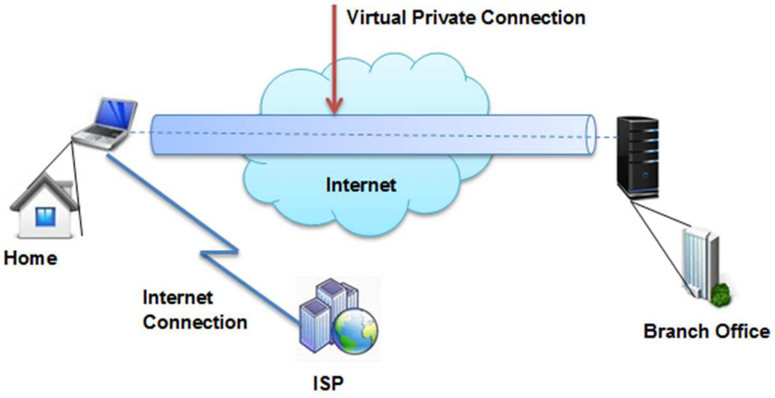

FIGURE 1. Remote Access VPN

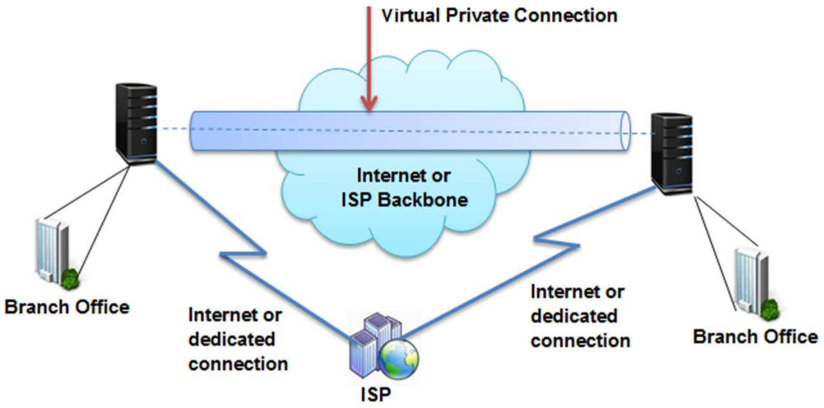

FIGURE 2. Site-to-Site VPN

## VIRTUAL PRIVATE NETWORK TECHNOLOGIES

Virtual Private Network (VPNs) are developed using various protocols and are classified from different perspectives. One of the classifications divides VPNs into: trusted VPN and secured VPN. Trusted VPNs are provisioned by service providers, and the customer traffic is not necessarily encrypted, but instead customers trust the service provider to ensure that their data traffic is kept secure in transit between peers. However, in Secured VPNs, customer data traffic is authenticated and encrypted and is transmitted over the service provider’s backbone or internet.

The specifications of the current VPN technologies are summarized and compared in Table 1. Since Secured VPN technologies significantly offer authentication and encryption have widespread accessibility, are more suitable for our network architecture. In addition, it is apparent that, in this category Poin-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) protocols are not developing any further as opposed to IPsec and TLS/SSL protocols which are presently popular and supported by networking device vendors. IPsec and TLS/SSL attend most of the current demand for secure communication over the Internet: VPNs and electronic commerce (e-commerce) (Wong et al., 2010). Therefore, this study focuses on these two VPN technologies.

TABLE 1. Trusted and Secured VPNs

| VPN type | Backbone | Features | Specific VPN technologies | Network Layer |
|---|---|---|---|---|
| Secured VPNs | Service provide/ Internet | Data traffic is authenticated and encrypted | IPsec | Layer 3 |
| | | | IPsec inside of L2TP | Layer 2 |
| | | | PPTP VPNs | Layer 2 |
| | | | TLS/SSL | Layer 4/7 |
| Trusted VPNs | Service provider | Data is moving over a set of paths that has specified properties and is controlled by ISP | MPLS/ BGP | Layer 3 |
| | | | Transport of layer 2 frames over MPLS | Layer 2 |
| | | | ATM circuits | Layer 2 |
| | | | Frame relay circuit | |

SSL lies between the transport and application layers, relying on a Transmission Control Protocol/ Internet Protocol  (TCP/IP) transport service and providing peer authentication, data confidentiality and message authentication for data integrity (Hua, 2011). SSL/TLS authenticates servers and optionally clients to prove the identities engaged in the secure communication (Wong et al., 2010). SSL/TLS is known as the technology which secures web browser sessions for e-banking and other sensitive tasks. It applies public key cryptography for authentication and symmetric cryptography for encryption to accomplish.

## NETWORK ARCHITECTURE DESIGN

### REQUIREMENTS

The requirements for designing a network architecture that maintains collaboration between specialist users include:

1. The identity of each user shall be proved and verified by the system (authentication).
2. User contents and user interactions shall be protected from unauthorized access.
3. It is essential to realize that, the available data in the network is the actual data that originally sent to network.
4. Specialist users need to be convinced that those who get access their data cannot steal their intellectual contents. However in a more elaborate and fully-fledged system a major requirement of paramount importance concerning intrusion detection and prevention similar to those proposed by (Patel et al., 2013), would be indispensable to overcome cybercrimes. This is an area for further research.

VPN technologies applied in this network architecture provide authentication, confidentiality and data integrity which meets the requirements (i), (ii) and (iii), respectively. Confidentiality means that data must be encrypted at the sender's site and decrypted at the receiver's site which makes data unintelligible to unauthorized parties (Forouzan, 2012) Data integrity is another security technique that detects if the data had been changed during transmission (Stallings, 2010). Additionally, it has to be a centralized architecture because it will facilitate the collaboration system to control, supervise, and monitor all data transmission and user interactions. Centralization is a crucial attribute that helps to detect and record any unauthorized access to the sensitive material of users to be used as evidence in the case of any infringement or dispute.

## NETWORK ARCHITECTURE DESIGN

This section proposes a network architecture that is considered to be integrated with a global communication system for collaborating specialist users. It can be distributed or non-distributed. In the case that there is a large amount of users and the network confronts high loads of data traffic; the distributed architecture is a more appropriate solution. Centralization makes the collaboration environment trustworthy and reliable for specialist users. The distributed architecture encompasses three levels: Central Site, Regional Sites and Remote Users. Regional Sites are located in various regions of the world and are connected to the Central Site using IPSec VPN. Data is transmitted between Regional Sites via the Central Site. Eventually, Remote Users connect to the geographically closest Regional Site through TLS/SSL VPN. The centralized distributed network architecture is an approach for increasing reliability, scalability and accessibility. In order to handle the traffic load of a widespread network, multiple Regional Sites are designed which would be placed in various geographical locations. Both the Web Server and the user (Client) are authenticated to each other using PKI (Public Key Infrastructure) and digital certificates. After successful authentication of both sides of the connection, they start communicating through TLS/SSL VPN protected tunnel. The next section will diverge into detailed stages of establishing connection between the server and the client.

With regard to the sensitivity of the material of the users, the central Web Server keeps track of any attempt to access the contents from different Regional Sites. While SSL/TLS VPN connection used in this architecture is an on-demand connection, the IPsec VPN is a pre-set always-on connection which operates based on the VPN configuration have been done on the gateways located at two sides of the connection. Figure 3 demonstrates the proposed centralized distributed network architecture for collaborating specialist users. The structure of non-distributed architecture is the same of the structure of one Regional site including all its connected clients except that the users connecting to non-distributed architecture can be from any places not only a particular geographical place (Kargar et al., 2014).

## HOW TLS/SSL AFFECTS THE ARCHITECTURE?

For authentication purposes, SSL Handshake protocol uses X.509certificate as strong evidence to the second peer to prove the identity of the peer that holds the certificate and the corresponding private key. The certificate attests to the legitimate ownership of a public key and attributes a public key to a principal, such as a person, a hardware device, or any other entity. The resulting certificates are called public key certificates (Oppliger, 2009) or digital certificates. Basically; CA (Certificate Authority) is responsible for ensuring that the security policy of the system is enforced and for guaranteeing its integrity (Furnell et al., 2008).

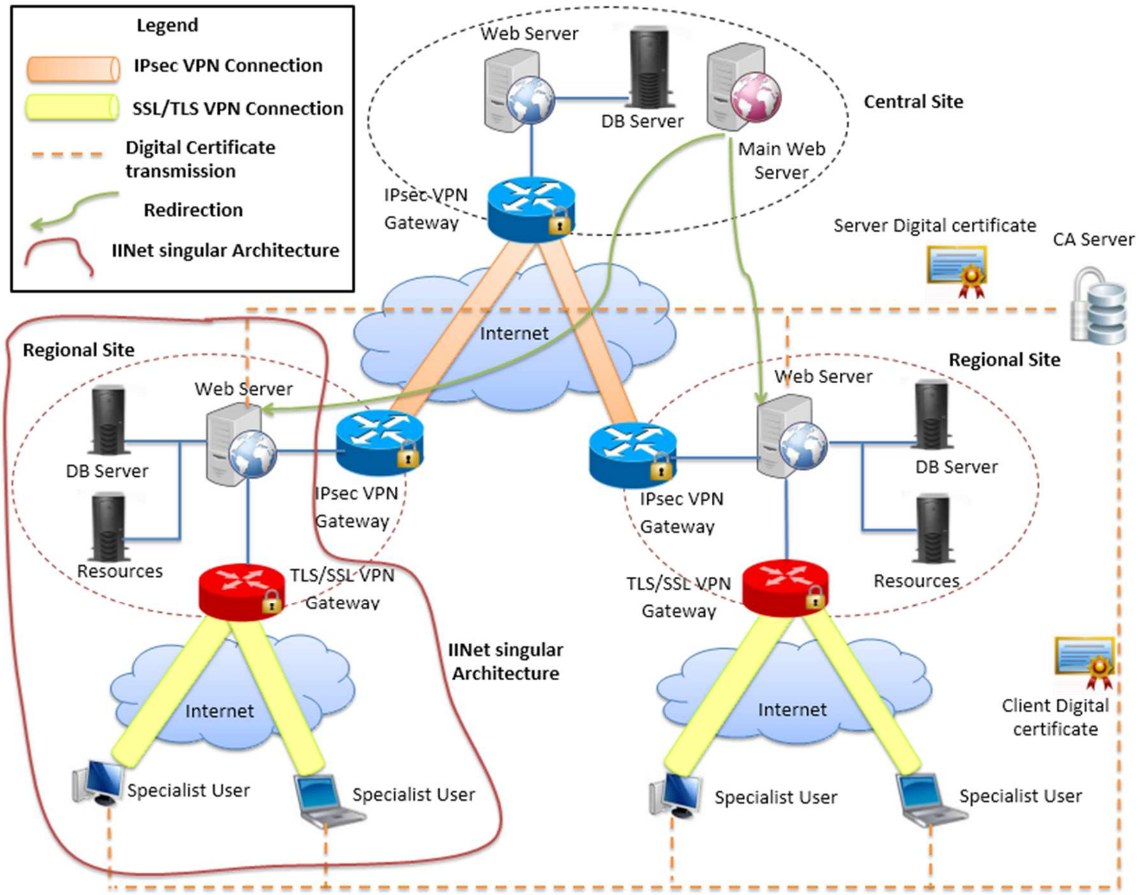

FIGURE 3. Distributed Centralized Network Architecture for Collaborating Specialist Users

The following steps explain how a client (specialist user) connects to the network which encircles authentication of the client and the Regional Web Server using SSL/TLS VPN:

1. Each client sends its Client ID and Public key to the trusted third party CA and requests for a digital certificate.
2. Each regional Web Server sends its Server ID and Public key to the CA and requests for digital certificate.
3. The CA issues the digital certificate for each Web server which includes Server ID, Server's Public key, expiration date of certificate and digital signature of the CA and sends it back to the server.
4. The CA issues a digital certificate for each client (specialist user), which includes Client ID, Client's Public key, expiration date of certificate and digital signature of the CA and sends it back to the client.
5. A client starts connecting to the network by entering the address of the Main Web Server in its standard web browser software.
6. The Main Web Server redirects the client to the regional Web Server which is geographically located close to the client.
7. The regional Web Server presents its digital certificate to the client.
8. The client verifies the Web server's certificate and checks if the CA is a trusted CA.
9. The client presents its digital certificate to the regional Web Server.
10. The regional Web Server verifies the client digital certificate.

At this point of time of operation, the server has been authenticated to the client and the identity of the client has been proved to the server. Moreover, both client and server know the public key of the other side. Figure 4 illustrates the protocol of these steps.

Confidentiality is done by cryptographic encryption methods. There are two main encryption forms: symmetric key (pre-shared key) and asymmetric key (public key). In symmetric key encryption both sender and receiver parties use the same key for encryption and decryption of data. Asymmetric encryption uses a pair of keys called the private key and public key. One key is used for encryption and a different but related key is for decryption. It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key (Furnell et al., 2008). TLS/SSL uses the public key for key exchanges and the symmetric key for encryption.

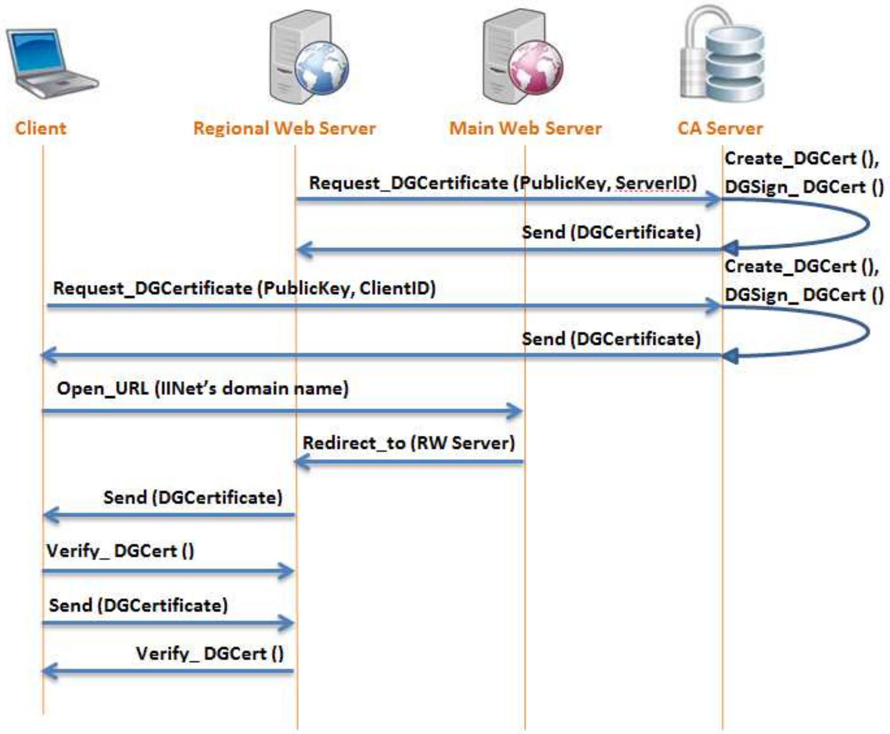

FIGURE 4. Protocol of Connecting a User to the Network

In order to enforce data integrity, before a message gets exchanged between the parties, it is run through a hashing algorithm. A hash function is an efficiently computable function that takes an arbitrarily sized input (data) and generates an output (data) of fixed size (Oppliger, 2014), known as a hash or digest. The sending party sends the encrypted hash (digital signature) with the message to the recipient. The following steps explain how a client after being authenticated to the server, starts sending messages of data to the Regional Web Server while confidentiality and data integrity is ensured. Figure 5 illustrates the protocol of these steps.

1. The client and the server negotiate the encryption and hash algorithms. The client chooses the encryption method and hash algorithm from the list that is provided by the server.
2. The client generates a Symmetric Key, encrypts it with the server's public key and sends it to the server.
3. The server receives the message; decrypts it with server's private key and gets the Symmetric Key which is now shared by both sides.
4. The client creates the message of data and calculates the message digest using the hash algorithm.

5. The client encrypts the message using the shared Symmetric Key and encrypts the digest by using its private key to produce the digital signature.
6. The client appends the digital signature to the encrypted message and sends it to the server.
7. When the message arrives at the server, the server decrypts the message using the shared Symmetric Key to get the data.
8. The server recalculates the digest based on the data, decrypts the digital signature using client’s public key to get the received digest.
9. The server compares the new digest with the received digest. If the values do match the data will be processed, otherwise the data has been corrupted and will be rejected.

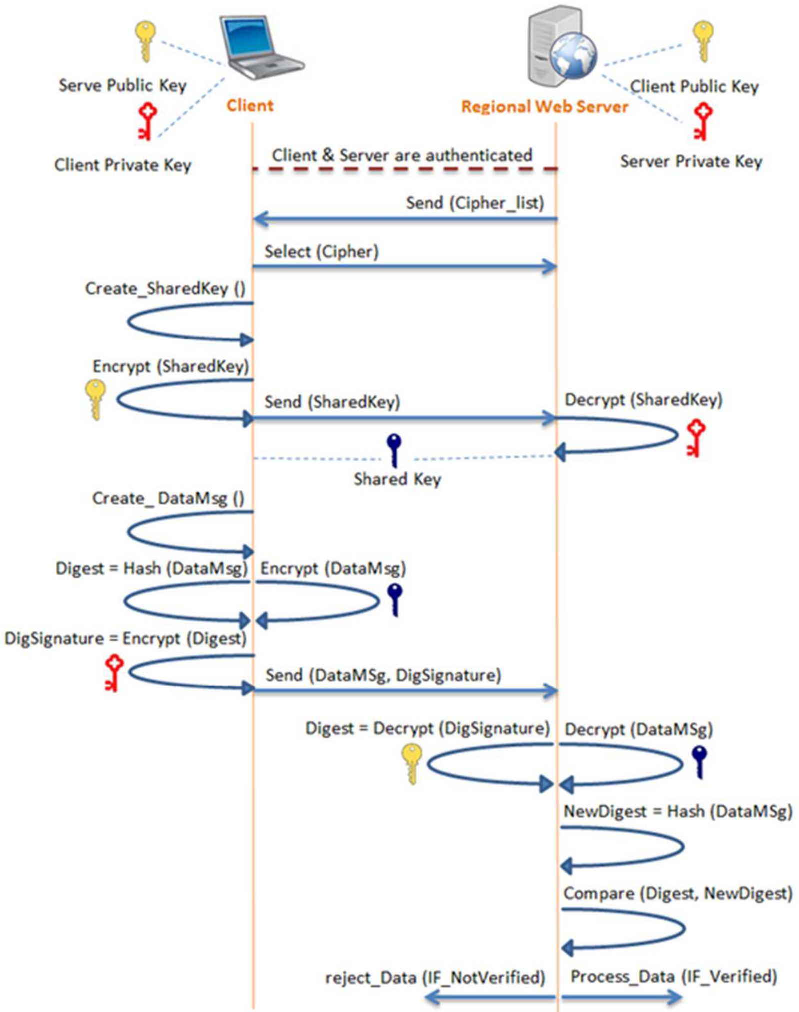

FIGURE 5. The Protocol of Protecting Data Transmission between Client and Regional Web Server

## PROTOTYPE IMPLEMENTATION AND EVALUATION

### EXPERIMENTAL SETUP

The prototype of the network architecture proposed in this paper has been implemented using OpenVPN and OpenSSL cryptographic library. OpenVPN is a cross-platform, secure and highly configurable VPN solution that provides TLS/SSL VPN tunnels.

Network performance is usually evaluated by using a set of performance metrics and network metrics. Performance metrics are used to characterize the performance of the network. The representative ones are as follows: utilization, throughput, RTT (Round Trip time), jitter and overhead. Network metrics are network parameters that are controlled and varied to study their impact on performance metrics. This experiment chooses, RTT for measurement as the performance metric and the encryption algorithm and digest cipher are chosen as the network metrics.

The measurement tools used in this paper are Wireshark and Iperf. Wireshark is a network protocol analyser with a rich feature set for capturing and analysing network traffic. It has deep inspection and filtering capabilities of hundreds of protocols making it a valuable tool for monitoring network traffic (Wu, 2011). In this experiment, it was used to monitor OpenVPN encapsulated packets. Iperf is a network testing tool for generating and measuring TCP and UDP streams. In this paper it was used for generating and sending TCP stream from the client to the server. Table 2 shows the specification of the systems participating in the tests. Figure 6 illustrates the topology of the experimental network.

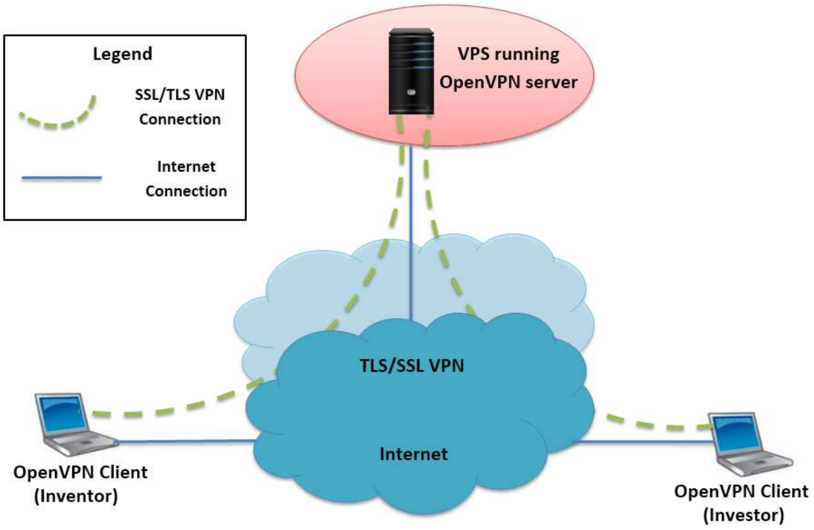
Legend
SSL/TLS VPN Connection
Internet Connection
VPS running OpenVPN server
TLS/SSL VPN
Internet
OpenVPN Client (Inventor)
OpenVPN Client (Investor)

FIGURE 6. Topology of Experimental Network

TABLE 2. Specifications of test systems

| System | Description |
|---|---|
| OpenVPN Server | Server Type: VPS (Virtual Private Server)<br>Virtualization Type: OpenVZ<br>OS: CentOS Linux 5.10.<br>CPU: Intel(R) Xeon(R) CPU E3-1240 v3 3.40GHz, 2 cores<br>Memory: 256 MB<br>Bandwidth: 500 GB<br>Iperf 2.0.4<br>OpenVPN version 2.0_rc16, OpenSSL version 0.9.7e |
| OpenVPN Client | System Model: Acer AOD270<br>CPU: Intel(R) Atom(TM) CPU N2800 1.86GHz<br>OS: Windows 7 service pack 1<br>Memory: 2 GB<br>Iperf 2.0.5<br>Wireshark 1.12.1<br>OpenVPN Client 2.3.4 i686 |

OpenVPN client runs on Laptops, while OpenVPN Server runs on a VPS (Virtual Private Server). During OpenVPN installation PKI certificates and keys files are generated and placed in the required machine. In order to establish an OpenVPN connection both the server and the clients need to be configured based on OpenVPN configuration instructions. The configuration files are used to change the encryption algorithm and digest cipher for each test. The process of each test is as follows: first, the configuration file on the client and the server are changed based on the chosen encryption algorithm and digest cipher for the current test. Then OpenVPN client and server are authenticated to each other. After the connection is established, the OpenVPN server distributes virtual IP for the client and itself. The experiment uses Iperf to generate and send TCP streams from client to the server. Wireshark also was configured measure RTT in each test. Each of the tests chose one of seven encryption algorithms and one of five digest ciphers for the connection. For the purpose of reducing errors, each test was replicated 8 times. The time interval between each replication was 5 seconds. RTT is calculated by:

$$T_{RTT} = (T_{AR} - T_{S}) /1000 \qquad (1)$$

Where: $T_{RTT}$: Round Trip Time (RTT) in Milliseconds
$T_{AR}$: time of receiving acknowledgment of test packet
$T_{S}$: time of sending test packet

## ANALYTICAL MODEL

In this experiment, the two-factor full design with replications was used as the analytical model. An effective two-factor design (Jain, 1991) is used when there are two parameters that are carefully controlled and varied to study their impact on the performance metric. Replications allow separating out the interactions from experimental errors. In this paper the effects and variations of two factors: encryption algorithm and digest cipher are analysed on RTT.

The two-factor design model considers an experiment design with *r* replications of each of the *ab* experiments corresponding to the levels of factor A and *b* levels of factor B. The model equation in this case is:

$$y_{ijk} = \mu + \alpha_{j} + \beta_{i} + \gamma_{ij} + e_{ijk} \qquad (2)$$

Where: $y_{ij}$ = response (observation) in the kth replication of experiment with factor A at level *j* and factor B at level *i*
$\mu$ = mean response (total mean)
$\alpha_j$ = effect of factor A at level *j*
$\beta_i$ = effect of factor B at level *i*
$\gamma_{ij}$ = effect of interaction between factor A at level *j* and factor B at level *i*
$e_{ijk}$ = experimental error

The effects are computed so that their sum is zero:

$$\sum_{j=1}^{a} \alpha_{j} = 0, \quad \sum_{i=1}^{b} \beta_{i} = 0 \qquad (3)$$

The interactions are computed so that their row as well as column sums are zero:

$$\sum_{j=1}^{a} \gamma_{1j} = \sum_{j=1}^{a} \gamma_{2j} = \ldots = \sum_{j=1}^{a} \gamma_{bj} = 0 \text{ and}$$

$$\sum_{i=1}^{b} \gamma_{i1} = \sum_{i=1}^{b} \gamma_{i2} = \ldots = \sum_{i=1}^{b} \gamma_{ia} = 0 \qquad (4)$$

The errors in each experiment add up to zero:

$$\sum_{k=1}^{r} e_{ijk} = 0 \qquad (5)$$

After averaging the observations in each cell, the total effect, each factor’s effect and the interaction can be calculated:

$$\Rightarrow {}_{ij.} = \mu + \alpha_j + \beta_i + \gamma_{ij} \quad \Rightarrow \quad \begin{aligned} \mu &= \bar{y}_{...} \\ \alpha_j &= \bar{y}_{j.} - \bar{y}_{...} \\ \beta_i &= \bar{y}_{i..} - \bar{y}_{...} \\ \gamma_{ij} &= \bar{y}_{ij.} - \bar{y}_{i..} - \bar{y}_{j.} + \bar{y} \end{aligned} \qquad (6)$$

After this, variations need to be calculated. Squaring the main equation helps to calculate variations:

$$\sum_{ijk} y_{ijk}^2 = abr\mu^2 + br \sum_j \alpha_j^2 + ar \sum_i \beta_i^2 + r \sum_{ij} \gamma_{ij}^2 + \sum_{k=1}^{r} e_{2_{ijk}} \qquad (7)$$

$$SSY = SS0 + SSA + SSB + SSAB + SSE \qquad (8)$$

$$SST = SSY - SS0 \qquad (9)$$

Each term in the equation (8) above refers to that in the equation (7). After computing these terms, variance can be analyzed by computing the ratios SSA/SST, SSB/SST, SSAB/SST and SSE/SST. Using these results, the effect and variation of each of the two factors on the RTT of SSL/TLS VPN can be estimated and analyzed.

## EXPERIMENTAL RESULTS

The experiment followed the steps mentioned above and measured RTT of SSL/TLS VPN for seven different encryption algorithm (DES-CBC, DES-EDE-CBC, BF-CBC, DES-EDE3-CBC, AES-128-CBC, AES-256-CBC, CAST5-CBC) and for five different digest cipher (MD5, RSA-MD5, SHA1, RIPEMD160, HMAC-SHA1) with 8 replications of each test. The initial observation results gathered and prepared for verifying the usability of the data of the experiment and estimating the effect of the two factors (encryption algorithm and digest cipher) on the performance of SSL/TLS VPN, which are accomplished by using the two-factor analytical model with replications. Equation (6) computes the effects of encryption algorithms and digests ciphers and the analysis is shown in Table 4. For each row (or column), the mean of observations in that row (or column) is computed. Overall sum and means are also computed. The difference between a row (or column) means and overall mean demonstrates the row (or column) effect which is the effect of the factor corresponding to that row (or column).

After this, the effects of interaction between two factors (or cell effects) for the (i, j)th cell are computed by subtracting μ+αj +βi from the cell mean yij. The computed interactions are listed in Table 5. The computation can be verified by checking that the row as well as column sums of interactions are zero. The results of the analysis are interpreted in the next section. Considering the encryption algorithm as factor A and the digest cipher as factor B, then A1, A2… A7 corresponds to the encryption algorithm at column 1, 2…7 in Table 4 and B1, B2… B5 corresponds to the digest cipher at row 1, 2… 5 in Table 4.

According to the results of the analysis listed in Table 4. Figure 7 illustrates the variation of effects of seven different encryption algorithms on RTT and Figure 8 illustrates the variation of the effects of five different digest ciphers on RTT according to the analysis results listed in Table 4. Figure 9 illustrates the variation of interaction effect between encryption algorithm (Factor A) and digest cipher (Factor B) on RTT in SSL/TLS VPN according to analysis results listed in Table 5.

The first five columns in this graph display the interaction effect of the first encryption algorithm (HMAC-SHA1) with the five digest ciphers (MD5, RSA-MD5, SHA1, RIPEMD160, HMAC-SHA1 ). Similarly the next five columns in this graph show the interaction effect of the second encryption algorithm (DES-EDE-CBC) with the five digest ciphers (MD5, RSA-MD5, SHA1, RIPEMD160, HMAC-SHA1 ) and so on.

TABLE 4. Computation of Effects for Encryption Algorithm and Digest Cipher using Two-factor Analytical Model

| Digest Cipher | Encryption Algorithm | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DES-CBC | DES-EDE-CBC | BF-CBC | DES-EDE3-CBC | AES-128-CBC | AES-256-CBC | CAST5-CBC | Row Sum | Row Mean | Row Effect |
| MD5 | 311.03 | 260.06 | 285.38 | 271.09 | 264.03 | 271.27 | 319.08 | 1981.94 | 283.13 | -1.73 |
| RSA-MD5 | 268.01 | 270.19 | 285.91 | 265.09 | 268.72 | 262.89 | 316.07 | 1936.9 | 276.7 | -8.16 |
| SHA1 | 287.77 | 279.72 | 266.43 | 290.25 | 267.9 | 269.45 | 301.63 | 1963.15 | 280.45 | -4.41 |
| RIPEMD160 | 273.3 | 306.91 | 259.07 | 263.2 | 309.34 | 301.86 | 310.71 | 2024.39 | 289.2 | 4.33 |
| HMAC-SHA1 | 266.57 | 261.26 | 293.25 | 291.94 | 316.98 | 310.72 | 323.19 | 2063.91 | 294.84 | 9.98 |
| Col Sum | 1406.68 | 1378.14 | 1390.04 | 1381.57 | 1426.97 | 1416.19 | 1570.69 | N/A | N/A | N/A |
| Col Mean | 281.34 | 275.63 | 278.01 | 276.31 | 285.39 | 283.24 | 314.14 | N/A | 284.86 | N/A |
| Col Effect | -3.53 | -9.24 | -6.86 | -8.55 | 0.53 | -1.63 | 29.27 | N/A | N/A | N/A |

TABLE 5. Interactions between Factors

| Digest Ciphers | Encryption Algorithms | | | | | | |
|---|---|---|---|---|---|---|---|
| | DES-CBC | DES-EDE-CBC | BF-CBC | DES-EDE3-CBC | AES-128-CBC | AES-256-CBC | CAST5-CBC |
| MD5 | 31.42 | -13.84 | 9.1 | -3.49 | -19.63 | -10.24 | 6.67 |
| RSA-MD5 | -5.16 | 2.73 | 16.07 | -3.06 | -8.5 | -12.18 | 10.1 |
| SHA1 | 10.85 | 8.51 | -7.16 | 18.35 | -13.07 | -9.37 | -8.09 |
| RIPEMD160 | -12.37 | 26.95 | -23.27 | -17.45 | 19.61 | 14.29 | -7.76 |
| HMAC-SHA1 | -24.74 | -24.35 | 5.26 | 5.64 | 21.6 | 17.51 | -0.92 |

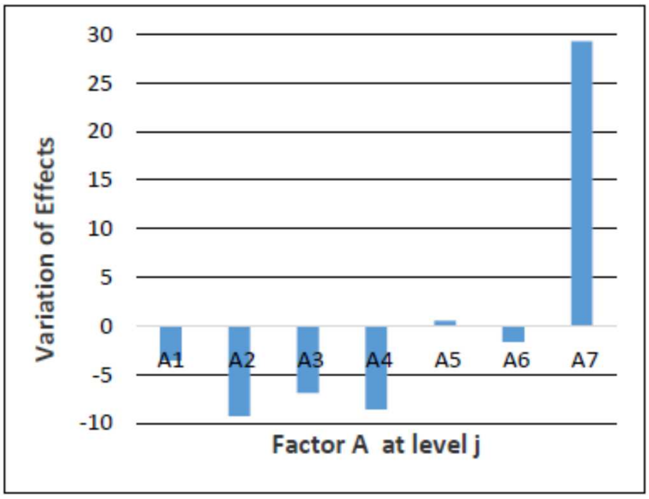

FIGURE 7. Variation of Effects for Encryption Algorithm (Factor A) on RTT using Two-factor Analytical Model with Replication

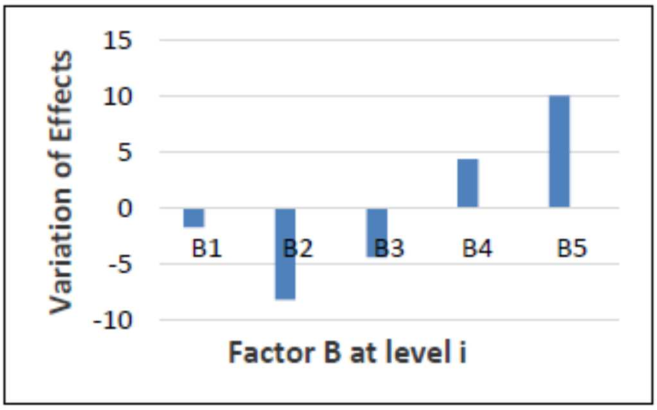

FIGURE 8. Variation of Effects for Digest Cipher (Factor B) on RTT using Two-factor Analytical Model with Replication

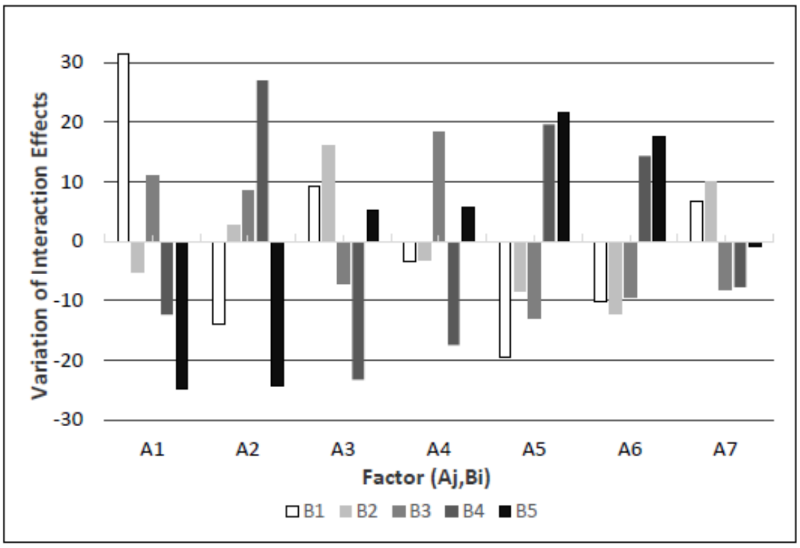

FIGURE 9. Cipher (Factor B) on RTT using Two-factor Analytical Model with Replication Variation of Interaction Effect For Encryption Algorithm (Factor A) and Digest

The computed results of the total effect and each factor effect are listed in Table 4 and illustrated in Figures 7 and 8. These results are interpreted as follows: An average encryption algorithm with an average digest cipher result a RTT of 284.86 ms. The effect of BF-CBC algorithm on RTT is 6.85 ms less than average algorithm, RTT with CAST5-CBC algorithm is 29.27 ms more than average algorithm, and so on. The ratio of RTT of DES-CBC and DES-EDE-CBC encryption algorithms using an average digest cipher is 5.7 ms, and so on.

The effects of interactions of two factors which are listed in Table 5 and displayed in Figure 9 are interpreted as follows: The RTT of SSL/TLS VPN when using BF-CBC encryption algorithm with HMAC-SHA1 digest cipher is 5.263 ms more than that of using BF-CBC encryption algorithm with an average digest cipher or equivalently 5.263 ms more than that of using HMAC-SHA1 digest cipher with an average encryption algorithm. The rest of the interactions can be interpreted similarly.

According to the two-factor analytical model, the total variation of y can be allocated to the two factors (encryption algorithm and digest cipher), the interaction between them, and the experimental errors. To do so, equations (7), (8) and (9) is used. In these equations SSY, SS0, SSA, SSB, SSAB, SST and SSE can be calculated, among which the term SSA is the variation explained by the factor encryption algorithm, the term SSB is the one explained by the factor digest cipher, the SSAB is the variation explained by the interaction between two factor, the SSE is the unexplained and SST is the total variation. Thus, the total variation can be divided into parts explained by factors A and B, the interaction AB, and an unexplained part. In other words, the percentage of variation explained by a factor or interaction is computed by SSA/SST, SSB/SST, and SSAB/SST which can be used to measure the importance of the corresponding effect of factor A and B and effect of interaction AB.
By comparing equations (7) and (8) various sums of squares are:

$$SSY= \sum_{ijk} y_{ijk}^2 = (375.98)^2 + (261.39)^2 + \ldots + (249.77)^2 = 23142192.39$$

$$SS0 = abr\mu^2 = 7 \times 5 \times 8 \times (284.86)^2 = 22721459.1$$

$$SSA= br \sum_j \alpha_j^2 = 5 \times 8 \times [(-3.53)^2 + (-9.24)^2 + \ldots + (29.27)^2] = 43107.77$$

$$SSB= ar \sum_i \beta_i^2 = 7 \times 8 \times [(-1.73)^2 + (-8.16)^2 + \ldots + (9.98)^2] =11620.43$$

$$SSAB= r \sum_{ij} \gamma_{ij}^2 = 5 \times [(31.42)^2 + (-5.16)^2 + \ldots + (-0.92)^2] = 38743.11$$

SSE = SSY – SS0 – SSA – SSB – SSAB = 23142192.39 - 22721459.1- 43107.771 - 11620.43 - 38743.110 = 327261.98

Using equation (9) the total variation is:

SST= SSY – SS0 = 23142192.39 - 22721459.1 = 420733.29
The percentage of variation explained by each factor and interactions are as follows:

$$\text{Explained by encryption algorithm} = \frac{SSA}{SST} \times 100 = \frac{43107.771}{420733.29} \times 100 = 10.245\ \% \quad (10)$$

$$\text{Explained by digest cipher} = \frac{SSB}{SST} \times 100 = \frac{11620.43}{420733.29} \times 100 = 2.76\ \% \quad (11)$$

$$\text{Explained by Interactions} = \frac{SSAB}{SST} \times 100 = \frac{38743.110}{420733.29} \times 100 = 9.21\ \% \quad (12)$$

$$\text{Unexplained} = \frac{SSE}{SST} \times 100 = \frac{327261.979}{420733.29} \times 100 = 77.78\ \% \qquad (13)$$

The experiment explains a total of 22.21 % variation on RTT which is obtained by adding the variation explained by each factor and variation explained by interactions between them. Moreover, the interactions explain more than 5% variation, so it cannot be assumed negligible and ignored as errors. According to equations (10), (11) and (12), variation explained by encryption algorithm is the highest value in total variation. As a result, encryption algorithm affects more than digest cipher on the performance of SSL VPN. Furthermore, the percentage of interaction between the two factors is a bit less than that of encryption algorithm, so that the interaction between encryption algorithm and digest cipher is the second important effect on the performance of SSL VPN. Nevertheless, 2.76 % variation explained by digest cipher alone indicates that its effect also exists. The graph in Figure 7 indicates that CAST5-CBC encryption algorithm has the most effect on RTT and the effect of DES-EDE-CBC encryption algorithm of OpenVPN is the least. Therefore DES-EDE-CBC presents the higher performance of SSL/TLS VPN among seven encryption algorithms which is followed by DES-EDE3-CBC and BF-CBC encryption algorithms. The graph in Figure 8 indicates that HMAC-SHA1digest cipher provides the highest effect while RSA-MD5 presents the least effect on RTT.

It can be concluded that RSA-MD5 presents the highest performance of SSL/TLS VPN among five digest cipher and SHA1 shows the second highest performance on the SSL/TLSVPN in terms of RTT. Additionally, the graph in Figure 9 indicates that the interaction between DES-CBC encryption algorithm and MD5 has the most effect on RTT but interaction between DES-CBC and DES-EDE-CBC encryption algorithms with HMAC-SHA1 digest cipher presents the least effect on RTT. It means that, interaction of two factors DES-CBC encryption algorithm and HMAC-SHA1 digest cipher provide the best performance in our experimental SSL/TLS VPN network (Figure 6). Meanwhile interaction of two factors DES-EDE-CBC encryption algorithm and HMAC-SHA1 digest cipher presents the second best performance.

## CONCLUSION

In the light of the need for a network that supports the security requirements of collaborating specialist users, this paper proposes a centralized distributed network architecture which is designed to be integrated with a collaboration system. Contemporary VPN technologies were reviewed and summarized and the most appropriate ones were chosen to be implemented in the network architecture. SSL/TLS VPN was used to protect the connection between remote users and Regional sites. IPSec VPN was utilized to link geographically separated Regional Sites to the Central Site. The concept of centralization is a crucial attribute of this architecture since it will makes the environment trustworthy and reliable for communicating. For evaluation purpose, real experimental prototype of the proposed network architecture was implemented using OpenVPN which establishes SSL/TLS VPN connections. This paper has tested and analysed seven encryption algorithms and five digest ciphers using two-factor analytical model with 8 replications. Gathered data has been fully assessed and analysed, which has produced the results to estimate their effects on the performance of SSL VPN in terms of RTT. The proposed network architecture in this paper can be used to extract the basic network infrastructure of the collaborative system, which will be very useful in our future research work. In addition, the cryptographic evaluation results help to realize the appropriate cryptographic algorithms to be used for confidentiality and data integrity in the collaborative network.

## REFERENCES

Chen, F., Wu, K., Chen, W., & Zhang, Q. 2013. The research and implementation of the VPN gateway based on SSL. *International Conference on Computational and Information Sciences*, Shiyang, 21-23 June 2013.

Feilner, M. 2006. *OpenVPN, Building and Integrating Virtual Private Networks*. Olton: Packet Publishing.

Forouzan., B.A. 2012. *Data Communications and Networking*. New York: McGraw-Hill.

Furnell, S., Katsikas, S., Lopez, J. & Patel. A. 2008. *Securing Information and Communications Systems Principals, Technologies, and Applications*. London: ARTECH HOUSE.

Ishimura, K., Tamura,T., Mizuno, S., Sato, H. & Motono, T. 2010. Dynamic IP-VPN architecture with secure IPsec tunnels. *8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT).* Kuching, 15-18 June 2010.

Jain, R. 1991. *Art of Computer Systems Performance Analysis Techniques for Experimental Design Measurements Simulation and Modeling*. New York:Wiley Computer Publishing.

Kehe W., Jianping, H., & Shuangbao, C. 2011. Test and Analysis of Sensitive Factors of SSL VPN on Kylin. *International Conference on Electrical and Control Engineering (ICECE).* Yichang, 16-18 Sept. 2011

Kotuliak, P. Rybár, & P. Trúchly. 2011. Performance Comparison of IPsec and TLS Based VPN Technologies. *9th International Conference on Emerging eLearning Technologies and Applications (ICETA),* Stara Lensa, 27-28 Oct. 2011.

Koyama, T., Karasawa, S., Kikuchi, Y., Kishi, K., & Iwamura, S. 2010. New Architecture for a VPN On-demand Interconnection System. *8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT),* Kuching, 15-18 June 2010.

Lakbabi, A. Orhanou, G. & el- Hajji, S. 2012. VPN IPSEC & SSL Technology Security and management point of view. *Proceedings of the Next Generation Networks and Services (NGNS).* Faro: IEEE, 202-208.

Lewis, M. 2006. *Comparing, Designing, and Deploying VPNs*. Indiana:Cisco Press.

OpenVPN Technologies. OpenVPN HowTO. http://openvpn.net/index.php/open-source/documentation/howto.html [September 2014]

Oppliger, R. 2009. *SSL and TLS Theory and Practice*. London: ARTECH HOUSE.

Oppliger, R. 2014. *Secure Messaging on the Internet*. London: ARTECH HOUSE.

Patel, A. Taghavi, M., Bakhtiyari, K . & J. C. Jr. 2013. An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review. *Journal of Network and Computer Applications*. 36(1): 25-41.

Raeespour, A. K. & Patel, A. 2014. An Innovative VPN architecture for Collaborative Specialist Users. *International Conference on Innovations in Engineering and Technology,* Penang, 19-20 Sept. 2014

Raji, E., Miri, A., & Davarpanah, M. 2012. CP2: Cryptographic privacy protection framework for online social networks. *Computers & Electrical Engineering*. 39(7): 2282-2298.

Su, H. S. 2011. The advantages and the implementation of SSL VPN. *2nd International Conference on Software Engineering and Service Science (ICSESS),* Beijing, 15-17 July 2011.

William Stallings. 2010. *Cryptography and network security Principles and Practice*. New York: Pearson Education.

Wong, W. Maurício, F., Magalhães, F. & VerdiIDSec, L .2010. IDSec: an Identification Layer Security Model. *24th International Conference on Advanced Information Networking and Applications,* Perth, 20-23 April 2010.

Yi, Pang, Shuyuan, Jin, Shicong, Li, Jilei, Li, & Hao Ren. 2013. OpenVPN Traffic Identification Using Traffic Fingerprints and Statistical Characteristics. *International Conference on Trustworthy Computing and Services,* Beijing, May 28- June 2 2013.

Akram Kargar Raeespour Sistani
Centre of Software Technology and Management (SOFTAM),
Faculty of Information Science and Technology (FTSM),
Universiti Kebangsaan Malaysia
ak.kargar.r@gmail.com

Ahmed Patel
Vieira Computer Networks and Security Laboratory (LARCES),
State University of Ceará
(UECE), Fortaleza, Ceará, Brazil.
whinchat2010@gmail.com

Received: 18 November 2015
Accepted: 27 January 2016