International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.301-310
http://dx.doi.org/10.14257/ijsia.2016.10.2.27

Cryptographic Protocols for Secure Cloud Computing

S. A. Alhumrani[1] and Jayaprakash Kar[2]

[1]*Department of Information Technology*
[2]*Department of Information Systems,*
Information Security Research Group
Faculty of Computing & Information Technology
King Abdul-Aziz University, Kingdom of Saudi Arabia, Jeddah-21589

Abstract

In this paper, we review and analyze some well-known cryptographic protocols for encryption of data that establish a secure communication for clouds. Many protocols are there, which provides various security goals for cloud computing. We have briefed on Secure Shell Protocol, Internet Protocol Security (IPSec), Kerberos, Wired Equivalent Privacy (WEP) and WiFi Protected Access(WPA) and discuss how these have been applied in cloud for secure communication. Further, we present the commands used by these protocols, the various methods used to encrypt data (tunnels and channels for instance) and their advantages for clouds.

Keywords*: Cloud Computing, Encryption, Data Packets, Communication and Authentication*

1. Introduction

The application of cryptography in cloud computing has four basic security requirement such as non-repudiation, authentication, integrity and confidentiality. Cloud computing provides what industry experts call a computing environment that is distributed and consisting of a series of heterogeneous components. The components here include firmware, networking, software and hardware, in addition to other services [1]. The problems of security in the cloud arise because people or entities must often share the downloadable applications, storage medium and other pay services hosted in the cloud. It gets even worse when the cloud consists of a public one where people pay for services that they share with others. In this scenario as well as in the hybrid cloud, one careless mistake such as connecting a device infected with malware, can lead to a data breach. A data breach can also occur if people share passwords with outside entities and allow them to get into the cloud. Cloud computing vulnerabilities also arise from the fact that the cloud can accommodate or use Wireless (WiFi) applications. Analytics, data processing, information processing and application execution could all suffer attacks if the ports for making the Wi-Fi connection remain unsecured [10].

The introduction of advanced Ethernet connection protocols like IPVersion 6 also poses a threat for the cloud computing model [1]. As a result of this threats and the sheer scale of the data held and trafficked through the cloud computing model, a need arose for the use of advanced secure protocols for authentication or variations of these protocols. These cloud computing based protocols can authenticate the user side and the client side and operate on the 802.11b standard. Examples of these protocols include TLS, SSH, IPSec, Kerberos, WEP, WPA, UMTS/LTE, ZigBee and EMV TLS stands for Transport Layer Security Protocol while SSH, WPA and WEP stand for Secure Shell Protocol, WiFi protected access and Wired Equivalent Privacy[8]. Many companies around the world opt for different protocols to protect their cloud based application and storage systems when employees must connect different devices and ports to the cloud [7].

ISSN: 1738-9976 IJSIA

The first protocol the paper will look at is the User Identity Management Protocol for cloud computing applications. The UIDM protocol place a major role with regard to a number of authentication and access issues. To begin with, the UIDM protocol framework determines how accounts with the highest privilege levels undergo authentication and management. It determines how the crucial decisions such as simultaneous large resource block de- provisioning and single or dual authorization occur [5]. Furthermore, concerning allocation of high privilege roles, the UIDM determines if the allocations break the least privilege rules of duty segregation. However, the key role of the protocol comes specifically in the handling of data, especially concerning data in transit, data in the cloud memory and data at rest. The protocol in its most basic form exists at the cloud application layer, Network layer and TCP/UDP physical layer. The protocol uses a sophisticated algorithm of pattern matching which protects a number of resources affiliated to the cloud including the cloud service provider, cloud service registry, cloud service metering and cloud billing [5]. In the algorithm's pattern matching T and P occur as the strings with lengths S and R respectively. These tend to be stored as arrays possessing one character per element. The stated algorithm finds or discovers the INDEX of P in T and the setup process shows the following steps.

Initialization: Here, one sets MAX: = S-R+1 and K: =1

In Step 2: K is less than MAX

Step 3: L= 1 to R and test each character of P.

1.1 Security Layer for the Transport Protocol

The TLS or the Security Layer for the Transport Protocol in the cloud computing purposes refers to a protocol with a built in capability that allows the client server applications in the virtual mode to carry out communication across the network. The design occurs in such a manner that the encryption prevents tampering, hacking or packet sniffing. The protocols here can operate with or without TSL or SSL and therefore the client on the cloud must indicate to the virtual server the TLS setup connection. Two main ways exist of achieving this and encrypting data and transmissions. The first involves using a different port number for the client side for HTTPS. The second involves using a protocol specific mechanism for applications such as mail. Examples of these protocol mechanisms include STARTTLS. Once the client on the cloud agrees to use TLS based protocol mechanisms, they can negotiate for a stateful connection and handshaking encryption procedures. The handshake encryption facilitated by this protocol, refers to a connection procedure where the handshake begins with the client connecting to a server affiliated with the above mentioned protocol, making a request for an un-hacked or intercepted connection, and then presenting a complete checklist of the available cipher modes or suites. The cipher suites in this case come in the form of hash functions and ciphers. From the list, the cloud server then proceeds to pick a hash function and a cipher which it offers support for, and then alerts the user of the choice made. This cloud or virtual type server then returns in feedback form the identity in a digital certificate which has the server name, the public encryption key and the specific trusted certificate authority.

In simple terms, when people share a cloud for data storage, application storage and resource access everyone who logs via the secure virtual server, gets a specific digital certificate tied to the device they use and the particular resource they want to access from the cloud. The cloud based protocol outlined above possesses high level encryption because the user does not need to go through the service provider to confirm the digital certificate validity. Log in with a password, a specific device with a specific IP address and MAC number will enable the user to conform that the certificate did not come from a cloned remote application elsewhere trying to masquerade as a service provider hosted on the cloud.

The success of this cloud based protocol relies on the fact that its design aims to perfectly match the TCP/IP conventional architecture. The protocol maintains this original architecture's design principles for the layer and hence inherits all its advantages. It therefore interacts at a high level with the TCP/IP protocol. The Transport Layer Security adds a new layer of encryption to the TCP/IP stack and as with other layers in that stack, the TLS act independently of the protocols below and above. The layer however, speaks the same digital or program language as the same layer on the opposite side of the communication channel. The protocol and its design therefore ensure full network technology compatibility based on the standard TCP/IP protocol, but also enables switching to secure versions without the need to reinvent or rebuild the system from the ground up (Dua, 2012). Thus, on this cloud based protocol, HTTP switches to HTTPS or FTP changes to FTPS, without the need to modify specifications. The TLS protocol for a secure encrypted cloud computing application possesses dual layers, namely the security layer record protocol and security layer handshake protocol. The first named one is placed on top or above the protocol of transport, which hardly breaks down such as Transmission Control Protocol in order to ensure that connections remain private. The connections remain private in the cloud through the use of symmetric data encryption. The TLS record protocol also plays a key role in higher level protocol encapsulation in cases like the TLS Protocol that carried out handshakes. The protocol of handshake permits or enables authentication to occur between a virtual server and the client, and encryption algorithm /cryptographic key negotiation before transmission of data by the application protocol.

One should note that the TLS tends to be independent of the application protocol and advanced stage protocols can position or layer above the security transmission layer protocol in a transparent manner. As said before encryption and cryptography in the cloud computing model consists of non-repudiation, authentication, integrity and confidentiality. Two steps principally form the basis of this factors namely entity authentication and exchanged data symmetric encryption. Entity authentication refers to the authentication or proofing of entities involved in cryptographic parameter negotiation and data exchange. In this step, the protocol uses X509 digital certificates and asymmetric cryptography. In the second step, calculation of message authentication code (MAC), transmitted data verification and exchanged data symmetric encryption occurs as a way to assure confidentiality.

2. Secure Shell Protocol

Secure shell protocol refers to an encrypted protocol for networks that allows several functions such as remote login. It primarily enables the network services to operate in a secure and encrypted manner over an unsecured network. Secure Shell Protocol therefore provide secure channels over unsecured networks in a given client server framework. That architecture or framework connects an SSH client application with a SSH virtual server. Common applications in cloud computing for the secure shell protocol include remote command execution and remote command line login. One should note that in the cloud computing model, any network service can receive encrypted and hence security with SSH. Two main types of this protocol currently exist namely SSH1 and SSH2. SSH2 plays a key role in cloud computing in terms of speedy connectivity after encryption [4]. It helps avoid the security challenges that arise when a cloud based virtual machine gets exposed directly on the Internet. The SSH prevents these security challenges by providing a secure path or channel over the internet, via a firewall to a virtual machine.

3. Internet Protocol Security (IPSec)

IPSec or the Internet Protocol Security suite refers to a transmission protocol suited for secure IP communications in the cloud. It works by providing encrypting and authentication services for each and every packet in the communication session. The protocol includes others commonly used for the establishment of shared authentication between entities at the commencement of the resource use session. The included protocols also establish authentication during cryptography key negotiation. More importantly, the IPsec's can act as data protectors between host pairs and also between security gateway pairs. They can additionally provide data protection between a host and a security gateway. IPSec protects communication over IP networks by encryption, but also supports other functions such as replay protection, data origin authentication and network level peer authentication. The IPsec protocol version used here for cloud computing purposes will consist of a type known as MYSEA. In general terms, the MYSEA IPSec protocol for cryptographic encrypted cloud services has the function of promoting scalability, agility, sharing of resources and collaboration on the cloud platform [6]. The cloud platform can in this case come in the form of private ones, hybrid or public ones.

The protocol provides enhancement or support for the various functionalities of cloud computing, with very reinforced security elements and characteristics brought about via multi domain system. That multi domain system possesses high assurance and the main architectural elements of the protocol consists of a federation or collection of trustworthy servers and special purpose components for authentication. The primary security features for the protocol include reinforced cross domain access controls, resource isolation, protection of services and data in the cloud via varying system classification and service replication. Other components come in the form of dynamic control of the QoSS [9]. MYSEA as a protocol framework also can host the MLS restricted teamed up application type services, which remain only accessible through regular protocols.

These protocols include common types such as SMTP/IMAP, SIP type VOIP and HTTP. The MYSEA TCB Protocol (Trusted Computing Base) protocol requires a MYSEA virtual server, the TCM and the TPE as common elements. The common core of the protocol however consists of the three man TCB components called the high assurance operating environment, the STOP OS and the Protected Communication Service or PCS. Another crucial element comes in the form of the DSS. The Protected Communication Service implements the IPSec tunnels as a way to encrypt the data and communications and more specifically to protect the communication that happens between the MYSEA virtual server and the TPE. It also protects communication between the server and the TCM. The DSS, on the other hand, serves the function of performing dynamic service management. Dynamic service management implies negotiating session keys and changing IPSec configurations. One should note that the TPA (Trusted Path Application) and the TPS (Trusted Path Service) tend to show tight coupling. The Path Application located on TPE provides the element of human interface for the users and hence an encryption. That occurs through the invocation of the trusted path to the login interface and the establishment of a session. The TPS on the server helps in cryptography and hence encryption on the MYSEA virtual server by carrying out authentication of the user and also a multitude of functions based on session negotiation [3].

The integrity based channel application and the integrity based channel services serve in tandem to make sure that the data traffic passing between the MYSEA server and single level network receive the proper labeling at the particular network classification level. Communication between the different virtual MYSEA servers in the cloud computing model tends to be served by the FSS or as the full name says the Federated Security Service, which as a part creates the Federated Security Service session between the servers (two in number). The reason for this is that so that they can trade or swap single sign on data or information and federation management. The Security Service

carries out additional functions related to encryption, such as cleanups and federation wide initialization, with the Trusted Remote Session and the Secure Session Service acts as trusted components [3].

The SSS takes up the role of managing application requests sent from the user workstations to the cloud. The Trusted Remote SS handles the encryption in network queries or requests sent from applications that are remotely excluded. This is via specially accorded privileges. Another key thing to note about IPSec is the fact that the Remote Application Components does not rank as trusted. It runs at the user session security level, which invokes them. Also, the APS functions as a standard transmission and control protocol handler, enhanced as a way to give cross domain functions [9] The IPSec protocols for encrypted cloud computing can support other protocols such as HTTP, IMAP and SMTP (Simple Mail Transfer Protocol) which serve a critical function of hosting cloud based webmail and information gathering.

The IPSec coding prompt and command line shown below demonstrates the typical way to encrypt data and communications in the cloud.

Configuration Setup for the Cloud on the Administrator's Workstation

```
1.  protostack equals  auto
2.  nat_traversal equals yes
3.  Keep- alive equals 30
4.  Conn cloud adds vpn
5.  authby equals secret
6.  Auto equals start
7.  Key exchange equals Ike
8.  ESP equals aes_sha1
9.  pfs equals no
10. Type equals tunnel
11. Left equals1. 2.3.4
12. leftsubnet equals 1.2.3.4 /32
13. right equals 4.3.2.1
14. rightsubnet equals 10.1.1.0/24
15. lifetime equals1h
```

It is important to note that one has to provide extra sysctl rules to the given code string (/*etc*/sysctl.conf) as a way for the for the disable mode redirects on a given device network card to allow proper functionality of the openswan.

1. net.ipv4.conf.all.accept_redirects equals 0
2. net.ipv4.conf.all.send_redirects equals 0
3. net.ipv4.conf.default.send_redirects equals 0

One can then go on to run a sysctl command:

```
1.  sysctl -p /etc/sysctl.conf
```

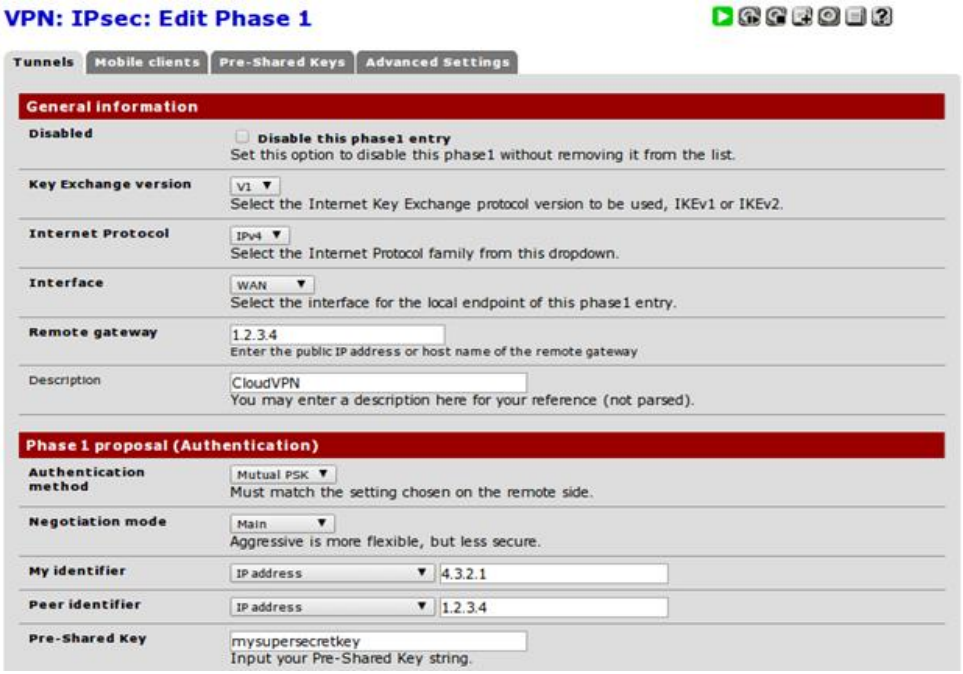
The command called netstat can be employed to confirm whether is functioning as it is supposed to function be; Also ipsec acts in a listening mode on UDP ports 4500 and 500 across all the given interfaces.

```
1.  # netstat –luntp// grep pluto
2.  udp 0 0 127.0.0.1:500 0.0.0.0:*// 19147/pluto
3.  udp 0 0 1.2.3.4:500 0.0.0.0:*// 19147/pluto
```

The protocol communication pfSense

Phase -I

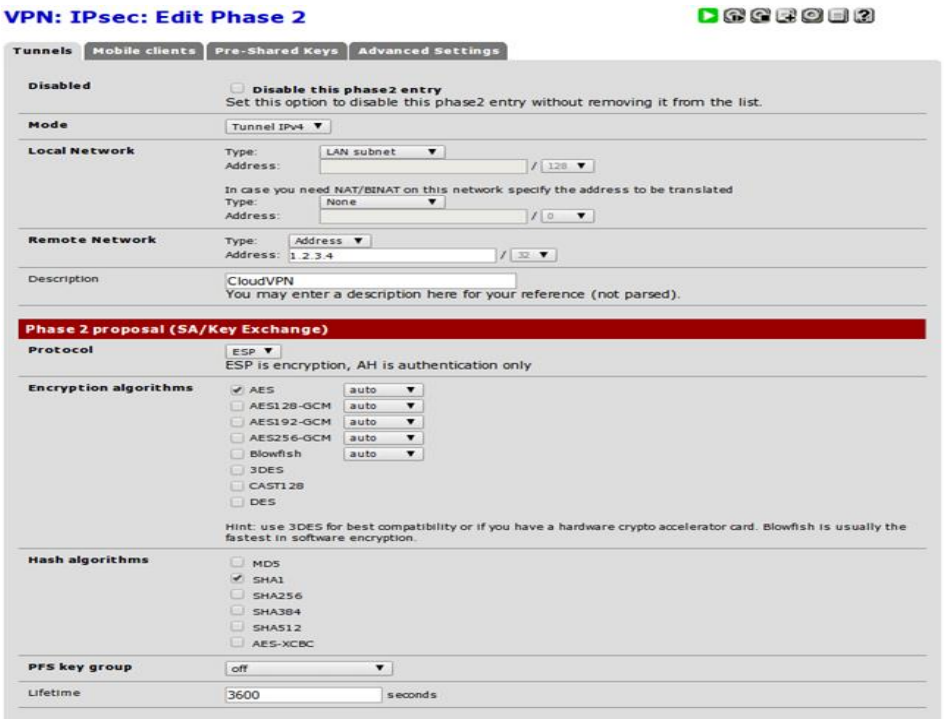
It makes a determination of the establishment of what is the secure IPsec tunnel. During the act of configuring this first phase, one must determine and identify the remote gateway. The gateway here is the make-up IP address 1.2.3.4 and therefore the Internet Protocol address of the server in the cloud. It should also be set to a known concealed or secret key and set by both of the endpoints in the system.



Phase-II

This makes a determination of how traffic routing occurs through the IPsec tunnel established in the past. The key fields include LAN or Local Network defining the local subnet. The accessibility factor will enable the user to access it at the extreme end of the other VPN tunnel.

Network.



4. Kerberos

Kerberos defines an authentication protocol for the computer network, working on the idea of items called 'tickets'. The tickets permit the nodes to communicate over a network (non –secure) and therefore provide proof of their identity to each other in a secure manner. Kerberos builds on what industry experts call key cryptography that is symmetric. It requires a so called third party (trusted one) and can uses cryptography of a public key nature, during specific authentication phases. The protocol works in a two-step manner in the cloud computing model for encryption which consists of client authentication and client authorization [2].

For Client Authentication, a client sends a crystal clear text message of the human user identification to the Authentication Server. The message requests certain services on the behalf of the human element or user. It is important to note that neither the secret key nor for that matter the coded password goes to the Authentication Server. This authentication server then goes on and creates the concealed secret key by using the hash function on the user password found at the cloud database storage [2]. The AS then carries out an analysis to see if the certain user or client exists in the database. If I the client exist, the AS dispatches feedback of back two distinct message queries to the client:

Message A: *TGS/Client Session Key* occurs in an encrypted manner using the concealed secret key of the client/user.

As soon as the user or client receives both messages, an attempt occurs to decrypt message A. That is through the concealed key produced from the user generated password. If the user generated password happens to correspond to the password in the Authentication Server database, the secret key of the client will differ. Therefore the A message will remain deciphered and thus encrypted. A valid secret key and password will enable the client decrypt the first message (the message A) as a way of obtaining the *TGS/Client Session Key*. The key also serves in other roles such as further communications to TGS.

For Authorization of Client Service, the user proceeds to send dual queries or messages to the TGS:

Message C: Composed of the ID of the requested service and TGT from message B.

Message D: Encrypted via the *Client/TGS Session Key* and the Authenticator (which is composed of the timestamp and Client ID).

Upon reception of these messages D and C, the TGS retrieves the B message from message C. and then carries out decryption on message B. That action requires the utilization of TGS secret key and gives or provides the “CT (Client)/TGS session key". Upon reception of this key, the TGS carries out an encryption on the authenticator (message D) and forwards dual messages to the user/ client:

Message F: *Client/Server Session Key* encrypted via the given Client*/TGS Session Key*.

5. Wired Equivalent Privacy(WEP)

WEP employs a stream cipher called RC4 Ron’s code, with a 24 rated bit initialization vector and 40- or 104-bit keys. The protocol uses a symmetric algorithm whereby two devices share a single secret key to facilitate secure communication in the cloud with each other. Two authentication methods occur in this protocol to encrypt cloud communication. These include SK or (the Shared Key authentication) and the OS (Open System authentication). In the latter the WLAN (Wireless Local Area Network) client does not provide credentials to the Access Point during the authentication process. Thus, any client can provide authentication with the AP (Access Point), associate with a device and access resources in the cloud. However, in Shared Key or SK authentication, the Wired Equivalent Privacy key is used for the purposes of authentication. That occurs via a detailed four-step called a CRH (Challenge-Response Handshake:

1. The client begins by first sending an authentication request to the AP (Access Point)

2. The AP (Access Point) replies with a coded challenge in the form of sending a clear text.
3. The user client then encrypts the challenge-text before sending it back in another request authentication. That occurs using the configured WEP key.
4. 4. The AP (Access Point) finally decrypts the response. If the response has an identical match to the challenge text, the Access Point provides instant feedback in the form of a plus or positive reply.

6. WiFi Protected Access(WPA)

WPA refers to a computing protocol which implements the IEEE 802.11i standard. WEP uses a 104 bit or a 40 ranked bit encryption key that the administrator's must put in manually on wireless access points (WAP) and various devices using resources from the cloud. That key does not change. TKIP on WPA employs a per-packet key type. That means that it flexibly generates a specific new 128-bit key for every data transmission packet .That in turn prevents the types of attacks on the cloud resource that compromised the WEP in the past. WPA also possesses a MIC (Message Integrity Check) as part of the encryption to protect the cloud resource. The check replaces the (CRC) cyclic redundancy check employed in a WEP standard.

TKIP and WPA standard implement three new security features to defeat threats encountered in the cloud computing model. TKIP begins by first implementing a key mixing function that matches or combines the secret root key with the initialization vector. After this it passes on to the RC4 initialization. WPA then implements a sequence counter. The sequence counter serves the purpose of protecting against replay attacks. Unsynchronized packets will be rejected by the access point. The final part of the security and data protection in the cloud computing model involves TKIP is implementing a 64-bit MIC or Message Integrity Check. One can say that the TKIP uses RC4 as its cipher and also provides a rekeying mechanism to ensure that every data transmission coming into or leaving the cloud possesses its own secure and unique encryption key.

Conclusions

Cloud computing using these protocols remains a major challenge due to the sheer scale of the number of attacks made on the cloud. In addition, the amount of resources in the cloud and the different functions, it carries out means that eventually, hackers and others penetrate the system and learn how the various security functions work. One should also note that the cloud functions in different ways when employed with different operating systems and different file systems. The entry of IP version 6 will, however lead to more secure cloud operations as the protocol possesses more authentication layers.

References

[1] Alowolodu, O, D & Ogundele, O,S. (2013). Elliptic Curve Cryptography for securing Cloud Computing Applications. *International Journal of Computer Applications,* Vol. 6,pp: 1-7.
[2] Bharill, S, Hamsapriya, T & Lalwani, P. (2012) A Secure Key for Cloud using Threshold Cryptography in Kerberos. *International Journal of Computer Applications,* Volume 79, 7: pp:1-11.
[3] Dinesha, H & Agrawal, V, K. (2013).Framework Design of Secure Cloud Transmission Protocol. *International Journal of Computer Science Issues*. Vol 10, pp: 1-10.
[4] Dua, I. (2012).Data Security in Cloud Oriented Application using SSL/TLS Protocol. *International Journal of Application or Innovation in Engineering & Management,* Vol.11, pp:1-6.
[5] Eludiora, S, Olatunde, A, Ayodeji, O, Adeniran, O, Onime, C & Kehinde, L (2012). A User Identity Management Protocol for Cloud Computing Paradigm. *International Journal of Communications, Network and System Sciences,* Vol 5, pp: 1-7.
[6] Nguyen, T, Gondree, M, Shifflett, D, Khosalim, J, Levin, T& Irvine, C. (2012). A Cloud Oriented Cross Domain Security Architecture. *Military Communications Conference. Cyber Security and Network Management,* Vol.18, pp 1-10.

[7] Pardeep, K & Peteriya, P.K (2012).A Pragmatic Study on Different Stream Ciphers and on Different Flavors of RC 4 Stream Ciphers. *International Journal of Communication, Network and System Sciences*, Vol 12, pp: 1-8.
[8] Ruiter, J & Poll E. (2013). Formal Analysis of the EMV protocol suite. *Digital Security Group. Institute for Information and Digital Science (ICIS*). Vol 8, pp: 1-12.
[9] Sridhar, T. (2012). Cloud Computing. *The Internet Protocol Journal*, Vol.11, pp:1-19.
[10] Stehle, D & Steinfield, R. (2013). Faster Fully Homomorphic Encryption. In proceeding of Asiacrypt2010, Vol 6477 of LNCS, pp 377-394.

Authors

Sultan Ahmed S. Alhumrani is pursuing M.S in Information Technology at Faculty of Computing & Information Technology, IT Department, King Abdul-Aziz University, Saudi Arabia, Jeddah. His current research interest is on Network Security and Cloud Computing.

Jayaprakash Kar has received his M.Sc and M.Phil in Mathematics from Sambalpur University, M.Tech and Ph.D in Computer Science (Cryptographic Protocols) from Utkal University, India. Currently he is working as Assistant Professor in the Department of Information Systems, Faculty of Computing and Information Technology. He is actively associated with Information Security Research Group, King Abdulaziz University, Saudi Arabia. His current research interests is in development and design of provably secure cryptographic protocols and primitives using Elliptic Curve and Pairing based Cryptography