Security Model for Communication and Exchanging Data in Mobile Cloud Computing

Moh'd Fawzi Al-Hunaity [#1], Jawdat Alshaer[#1], Osama Dorgham [#1], Hussam Farraj #2
[#1] *Dept. of Computer Information Systems, Faculty of Information Technology. Al-Balqa Applied University, Salt, Jordan*
[#2] *Sermon Business Solutions Company, Amman, Jordan*

Abstract *Cloud computing technology extended data centers to the cloud; adding new possibilities for devices to access information in anytime and anywhere with reduced costs, faster deployment and maximized flexibility. Although, ensuring high levels of performance that would raise a new security challenges and concerns to be handled. However, most of the cloud computing service providers deploy security policies for data protection. But, in the client side many security approaches can be used to ensure high levels of security, which would assure security of data in the client and provider sides. In this article, security challenges are defined and security model is proposed for handling realistic security holes for cloud computing. The proposed model relies on applying high secure mechanism by using strong factor authentication and encryption process using ElGamal algorithm. Also, a new security rule is proposed by using Serpent encryption algorithm for encrypting data before being uploaded to the cloud storage. Moreover, a Secure Authentication System (SAS) was Implemented, Applying the proposed security approaches, SAS proved to provide more security compared to recently used ones.*

Keywords — *Cloud Computing, Cloud Security, Communication , Encryption , Data Exchange.*

I. INTRODUCTION

Most of the enterprises try to reduce the cost of computing environment and use secure remote services on virtual servers, in order to reduce real hardware devices cost, management responsibility and renewal cost of software licenses. Also, to minimize the risk of sudden disasters and lost, of servers, hardware, work database and any other important information.

Portable devices with limited processing capabilities, limited memory space and internet availability would extend the demands for information availability anywhere and anytime. Therefore, cloud computing is essential for personal and enterprise users of databases, special systems and applications without installing them on their own portable devices by using providers servers [1]. As a result, that would allow terminal users to store data and process it online by running their applications remotely on virtual machines at private cloud then get results at local workstations.

Generally, cloud computing is an internet based computing technology which uses computer resources as services that are located on centralized remote servers and can be used through the internet protocols serving different kinds of clients as shown in Figure1. This technology, allows the businesses and users to share, save and process remote resources. Cloud computing considered as a new computing paradigm with implications for greater flexibility, availability, scalability at lower cost and time. It is on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort.

II. MOTIVATION

Enterprises moving their services to the cloud, face emerging and changing risks and must adjust their security programs accordingly for

Figure1. Cloud Computing with multiple services for different clients

cloud computing risk management and business. Personal and business information security and privacy, are the two most important challenging factors in cloud

computing, where data is stored on remote server at any physical location and those servers are public and can be accessed anytime form thousands of clients, the servers can be hacked and data can be stolen if special security roles were not enforced in excellent procedure.

However, some of the cloud computing service providers do not have strong security aspects and still use insecure or weak authentication methods, enhancing of cloud computing security is still open research area; as hackers continuously gaining more knowledge and experience. Precisely, clouds now are used by smart phones and multi internet access devices, and will be used as universal technology in the world requiring security policies with strong encryption, authentication, and access control process to protect the clouded data and ensuring the availability and privacy. This triggers the contributions of this article: proposing security model to be used in personal mobile smart phones (e.g. Android O.S), portable devices, computers and workstations to access the cloud storage service in secure way and assuring privacy and protection of clients' sensitive and personal data.

III. Related Work and Literature Review

Security is very important in cloud computing since many users and companies stores their confidential data in the cloud storage. Therefore, there are big security concerns when using cloud services which lead the researchers to search and develop solutions in cloud computing security. Which has been taking large area and importance, following are some of the important cloud computing security researches, that explain the structure and bases of cloud computing security.

In the article Mobile One Time Passwords and RC4 Encryption for Cloud Computing, Johnson et .al. in [2], authors proposed policies for securing data transmission over the internet, wide area network and authentication.

RC4 encryption algorithm was used to ensure the security of data as this algorithm is secure enough and fast to be run. Compared to AES, which together with RC4 are the most common encryption methods are being used over the internet. Authentication phase achieved by using one time password for the login to cloud computing services by being generated on regular mobile phone as a third party to confirm the client credibility before allowing the client to access cloud computing services. The difference here, with static passwords is that the passwords in the proposed method are only valid for one time only to ensure more secure. All data exchange among the server, clients and mobile agents will be encrypted by RC4 algorithm. Priyank et. al. in [3], present a model of security depends on mobile agent to acquire useful information from the virtual machine which the service provider and user used it to keep track integrity and privacy of virtual machine that used for cloud computing service.

D.H. Patil et .al. in [4], addresses several issues of security problems that is related to cloud computing services environments such as key generation, data security, authentication and access control. Authentication process uses Two-Factor authentication technique with Diffie-Hellman key exchange used for key generation and exchange a symmetric key among the client and cloud computing servers, which is not used in encryption and decryption for user data access, this technique solved the key distribution and management problem. Antonios in [5], explained concepts of access controls that used in cloud computing, concentrating on characteristics of the cloud computing, by using conceptual categorization to explain them, then presented a comparative of two most common models of access controls: Role-Based access control model and the usage of control model. In[6], the authors concentrate on the modern encryption algorithms that take main role in data security of cloud computing, compare and evaluate eight modern encryption algorithms: RC6, MARS, AES, DES, 3DES, Two-Fish, and Blow-Fish. The evaluation achieves on two independent platforms that are desktop computer and Amazon EC2 Micro Instance cloud computing environment rendering on randomness testing by using NIST statistical testing in cloud computing environment. The results of comparisons and evaluation as found in the paper:"AES encryption method is suitable algorithm for Amazon EC2 environment, but Blow-Fish and DES is more suitable when we focus on time of encryption method and encryption method is suitable algorithm for traditional PC environment, but Blow-Fish is more suitable when we focus on time of encryption method[7]. Katzan et .al. in [8] explained new technology cloud computing concepts like Software-as-a-Service, architecture and economics of scale on business.

IV. Security Challenges in the Cloud Computing .

Cloud computing offers valuable service with cost-saving for small enterprises and business, it has some of security risks that will be in consideration to find solutions for them. The top security risks in cloud computing are listed below in table 1.

Table 1. Lists of possible authentication attacks[2].

Attack	Description
Eaves dropper attacks	Attacker gains information from an authentication exchange and restoring data, such as authentication key values may be used to authenticate.
Customer fraud attacks	Where the customers consciously compromise their authentication key. Using multiple authentication factors can prevent customer fraud attacks.
Key logger attacks	Malicious code, hardware or software based attacks that track keystrokes of a person with the target to get any password typed in or other manually input authentication key data by the person.
Insider attacks	Where authenticator or systems managers intentionally compromise the authentication system or steal authentication keys or associated data.
Man -in- the-middle attacks	Where an attacker inserts himself in between the client and the verifier in an authentication process. The attacker attempts to authenticate by pretending as the client to the verifier and the verifier to the client.
Password discovery attacks	This includes a series of attacks, including brute force, common passwords and dictionary attacks, which aim to set a password. The attacker can try to guess a specific customers password, try common passwords to all customers or use an already made list of passwords to match against the password file (if they can restore it), in their attempt to find a valid password.
Phishing attacks	Social engineering attacks that use fake emails, web pages and other electronic communications to encourage the customer to disclose their password and other susceptible information to the attacker.
Replay attacks	Where the attacker traces the data of a successful authentication and replays this information to get an untruly authentication to the verifier.
Session hijacking attacks	Where the attacker hijacks a session following successful authentication by stealing session key or session cookie.
Shoulder-surfing attacks	Attacks definite to password systems where the attacker secretly directs observing the password when the customer enters it.
Social engineering attacks	A social engineering attack is one in which the anticipated victim is somehow trapped into

	DOING THE ATTACKERS REQUEST. AN EXAMPLE WOULD BE REPLYING TO A PHISHING EMAIL, FOLLOWING THE LINK AND ENTERING YOUR CLOUD COMPUTING CREDENTIALS ON A FAKE WEBSITE.
VERIFIER IMPERSONATION ATTACKS	WHERE THE ATTACKER PRETENDS TO BE THE VERIFIER TO THE CUSTOMER TO OBTAIN AUTHENTICATION KEYS OR DATA THAT MAY BE USED TO AUTHENTICATE FALLACIOUSLY TO THE VERIFIER.

A. ***Data Exchange Security:***

Usually, all network transactions and events among local networks and cloud computing services is being navigated through internet, this requires the use of secure connection channels for example (https protocol); data must be encrypted during the exchange process or it can be hacked in the network route.

B. ***Security of Software APIs:*** Software interfaces and API are considered as vulnerable to hack and steal on cloud computing services by using some scripts and phishing websites if the software and API have some security holes.

C. ***Security of Data in Cloud*** *:* Sometimes cloud computing service providers secure data transfer only, after that the data is stored without encryption or with weak encryption, if the data is stolen or exposed in some way then your private data will be compromised. The Cloud Security Alliance (CSA) recommends that you be aware of the software interfaces, or APIs, that are used to interact with cloud computing services."Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability, and accountability.

D. ***Data Separation :*** Cloud environment is a shared resources (Hardware and Storage) among several subscribers by using subscriber virtual machines, definitely, each client data must be separated from others by creating a virtual container for each.

E. ***Clients Access Control and Authentication***

Data stored in the providers private cloud storage may accidently accessed by an authored user if the cloud service provider does not deploy strong access control policy; authentication plays basic rule in information protection and computer security in general. Authentication was defined as "the act of creating or validating something (or someone) as authentic and claims made about the topic are true[2]. Network authentication in private and public networks usually done through static user name and password to access the network or the system, if the username and password validated as declared previously during registration, then the user is trusted to access the network or the system. However, this authentication process has some of vulnerabilities for attacks because if the username and password is stolen in some ways, forgotten or accidently exposed, the data and privacy will be compromised.

V. AUTHENTICATION SECURITY CHALLENGES

Analysing the different type of attacks in Table 1. The authentication process is the most weak point in securing data in the cloud .In this article, Authentication algorithm will be proposed and tested. Authentication arises in more secure process (Single-Factor Authentication, Multi-Factor Authentication).

A. Single-Factor Authentication

Traditional security process that requires one factor to grant and authenticate user to access specific cloud service with predetermined permissions.

CHARACTERISTICS (SOMETHING YOU ARE?)	GEOMETRY, FACIAL IMAGE, IRIS, RETINA, DNA, VOICE, SIGNATURE PATTERNS

Types of Single-Factor authentication can be shown in Table 2.

Table 2.Types of Single-Factor Authentication

SINGLE-FACTOR AUTHENTICATION	TYPES
PROOF-OF-KNOWLEDGE (SOMETHING YOU KNOW?)	PASSWORDS, PIN, MOMS NAME, PHONE# ,ETC.
PROOF-OF-POSSESSION (SOMETHING YOU HAVE?)	SMARTCARDS, TOKENS, DRIVER'S LICENSE, PKI CERTIFICATES
PROOF-OF-	FINGERPRINTS, HAND

B. Multi-Factor Authentication

Multi-Factor Authentication extends security on access over traditional single-factor authentication, the multi-factors are: something you know and something you have at the same time to grant access[9].like static username and password with fingerprint or with one time password (OTP).

C. One-Time Password

One-Time Password(OTP) is a technology that requires a new password every time the user want to authenticate themselves for login to an online service on any system, OTP can support strong, two-factor authentication, in which users enter something they know-Personal Identification Number (PIN)—and something they have-hardware token. This technology protect against an intruder replaying a captured password. OTP generates passwords using either the MD4 or MD5 hashing algorithms. Traditional static passwords are easily stolen, frequently lost and need time and effort to recover it. More complex, "stronger" passwords consisting of secret and combinations of characters and numbers and special characters, which lead users to write their complex passwords on somewhere to remember it.

OTP is more secure and simple way to validate and authenticate a user by generating random password for each login session to the system, this generated password is valid for a specific duration (e.g. 30 Sec, 1 min) to use it and should only be available to be used once. OTP can deliver to the user via several ways, for example by:

- Authentication device (called token): that could be a standalone device communicates with authentication server to check new password requested.
- Out-of-band channels: OTP send to the users by SMS, Phone Call and Email.
- Software solution: running several other devices, such as portable devices (laptop, PDA or Smart phone).

VI. PROPOSED SECURE AUTHENTICATION APPROACH

The proposed authentication model applies a high secure multi-layer authentication process, in which each layer checks some factors based on layer requirements, every layer defend against some attacks and require the user to provide some factors (something he has) to pass the authentication layer.

In the authentication model all users should have a trusted device which is responsible for creating new users, trusting device (which will use the model services), and generating OTP. The authentication layers factors:

- Static User Name and Password.
- (MAC) Address.
- Trusted Third-Party (Open ID).
- Time-Based Dynamic One Time Password
- ElGamal Data exchange cipher.

Using Java language, Secure Authentication System Application (SAS) was developed using the proposed authentication factors with the configuration as shown in Figure 2.

A. Authentication Process

For the authentication process the user must has smart phone with android O.S, then downloading the proposed mobile application, which flows as in figure 3.

Now we will go through the user creation process and the security issues concerning it.

B. User Creation Process (Sign Up):

The users can sign up to the proposed application model from mobile device, only by using the proposed mobile model application.

To create a new user, the user must provide a static user name and password. After that the program will associate the devices MAC address with the created user. Then the user must provide Open ID that will be used to generate OTP at the server and client (mobile) side.

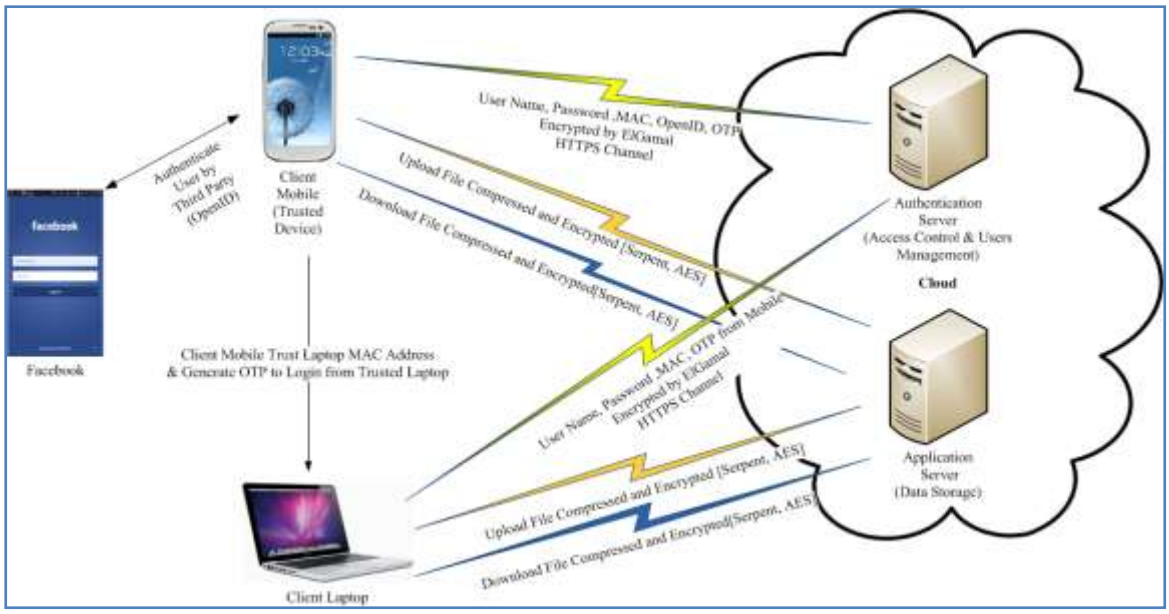

Figure 2: Design and Structure for Proposed Secure Authentication System(SAS)

Open ID is an open standard that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service, such as Face book, AOL, Yahoo and others. The goal of the Open ID initiative is to allow users to log in at websites around the Internet with one ID, instead of having to create multiple unique accounts. To use Open ID, firstly a user must be a membership in one website that support Open ID service (e.g. Face book) by registering procedure, then when visiting other websites that support login with Open ID, he can login with Open ID account like Face book account to be authenticated accessing this website services.

Face book (RP) in SAS was chosen as proposed Open ID provider to authenticate the user in our experimental model, the user will be directed to Face book website or application if installed for entering his Face book credentials , providing Face book with the a valid credentials the Face book returns back the Open ID which is then associated with the user information (Username, Password, MAC).

At this moment we have a static user name and password which is a first authentication factor, MAC address as a second authentication factor and finally Open ID as a third authentication factor, these three factors are collected during the sign-up process which will be used later to authenticate the user during the login. These are transferred by the SAS application to the authentication server to complete the user creation process, however this is a very high sensitive data thus it should be secured before sending it through the internet shown in Figure 3.

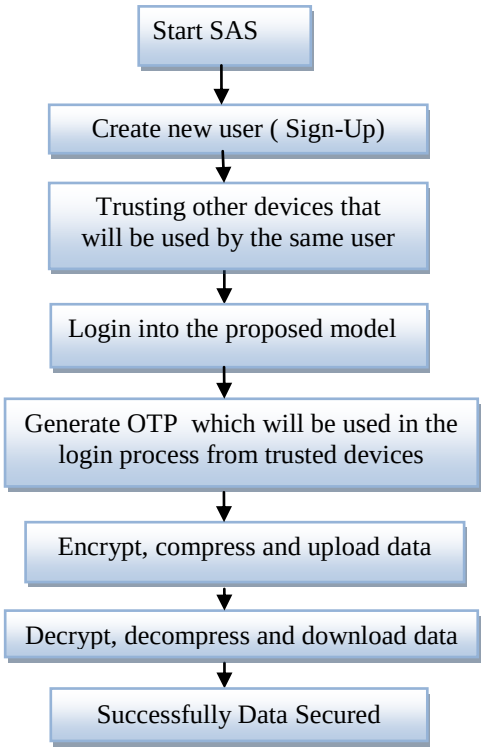

Figure 3.authentication process flow chart

C. Securing the Exchange Transfer of data

For exchanging sensitive data, ElGamal encryption is used as exchange algorithm providing very high security along with small

encrypted data footprint compared to other data exchange algorithms. ElGamal is asymmetric key encryption algorithm for public key cryptosystem which is based on the Diffie–Hellman key exchange, its strength comes from the difficulty of computing discrete logarithms over finite fields[10]. When comparing ElGamal and RSA in strong and speed factors, Elgamal might be considered stronger and more secure than RSA since calculating discrete logs is at least as tough as integer factorization. For speed comparison factor, ElGamal can be considered faster in total terms, that mean it does not depend on encryption or decryption time separately, but on total cost of operation, ElGamal generate cipher text double size of plaintext as shown in table 3. RSA generates cipher text equals to key length, for instance, 10 bytes is encrypted to 20 bytes using ElGamal algorithm and 256 bytes using RSA algorithm [11], when using 2048 bit key.

Table 3. Comparing RSA to ELGAMAL

	RSA-1024 (1024-BITS)	ELGAMAL (1024-BITS)
ENCRYPT	8	109
DECRYPT	93	77

As comparison results suggests and because of the limitation of mobile hardware resources; ElGamal encryption algorithm in the data exchange is more suitable to be used in enhancing the security specially for mobile cloud computing.

The SAS application will encrypt all the data sent to authentication server through a secured channel (HTTPS), in the server side, the user information will be decrypted and stored it in secure database.

VII. USER LOGIN PROCESS

After signing up to the proposed model and ensuring the user membership using trusted mobile device, the user can proceed with the login process to use the cloud storage service through two options:

- Using the Android Mobile Application.
- Using Desktop Application

A. Login using the Android Mobile Application

The mobile Version of SAS will prompt the user to enter his his credentials (Static User Name & Password) then will send these information associated with device MAC address encrypted using ElGamal cipher. When the authentication server receives the login request, it validates the sent user information (Static User name, Password and MAC address) then grants user to access then redirect the user to OTP Activity page if the information is valid. Now the user should provide his OpenID through logging into Face book in order to generate OTP, Face book (RP) will provide the application with the user Open ID, and then the application generates OTP locally (on mobile device).

The user will not have to login to Face book every time if he has Face book application installed on his mobile, the SAS application will automatically use the credentials stored locally to get the Open ID without prompting the user.

B. OTP Generation Process:

To generate OTP the following inputs are needed:

Open ID

1) Device current time
2) Salt (static string)

The Open ID is concatenated with a static string (salt) and passed with the device time to generation hash function HMAC-SHA-1[7].

The hash function returns a seven digits string that represents the OTP for the user with the given Open ID at that time. Now the user should be able to generate OTP by using "Generate OTP" function in the SAS.

SAS will validate the user information, retrieve the users Open ID from a relying party (Face book) and generate OTP which is valid for 60 seconds during the login process.

SAS sends OTP to the server to complete the login process and authenticate the user to use the the requested service using SAS functionality "Send OTP to Server".

By using OTP we can make sure that the user entered a valid user name and password from a trusted device and using a valid Open ID at a specific time just from checking the OTP at the server side. The server in its turn generates OTP using the Open ID it has (from the signup process) and from its local time and validates it by comparing with the OTP that received from the user during the login process.

C. Login using the Desktop Application

The desktop version of SAS application will prompt the user to enter his login credentials Static User Name, Password, and OTP.

User enters his static login credentials, and get OTP by generating it via trusted mobile device, the desktop which will be used in first time login, should be owned trusted one. The Device ID(MAC) is entered in the Trust Device ID field in the SAS mobile application. Then the OTP is entered which was generated using the mobile version of SAS, transferring these information compounded with device MAC address

encrypted using ElGamal cipher. The authentication server in the other side receives the login request, validates the information (Static User name, Password, OTP and MAC address) and grants access.

D. Downloading & Uploading Encrypted Data:

After validating all user credentials and logging successfully, the user can access the cloud services (Uploading / Downloading encrypted data) to cloud storage.

VIII. EXPERIMENTAL RESULTS AND EVALUATION

The proposed security model was evaluated regarding to its access control security phases, encryption, and the overall performance parameters using the cipher algorithm. In Table 4. , detailed analytical comparisons were made to the existing commercial models. Outlining the advantages and the disadvantages of the proposed model.

Table 4. Comparing Results of SAS and Existed Models

AUTHENTICATION FACTORS	ADVANTAGES OVER PRESENT MODELS
STATIC USER NAME & PASSWORD	ELGAMAL ENCRYPTION PRODUCES SMALLER AMOUNT OF DATA ON ENCRYPTION THAN RSA AND THE AVERAGE TIME FOR ENCRYPTION AND DECRYPTION IS SMALLER THAN RSA
ACCESS LIST USING MAC ADDRESS	CREATE ACCESS LIST DATASET FOR TRUSTED DEVICES
OTP	GUARANTEE THE OTP IS GENERATED VIA TRUSTED DEVICE WITH TRUSTED USER IN (PROPOSED MODEL AND THIRD-PARTY)USING THE PROPOSED APPLICATION AND IN SAME SPECIFIC TIME IN BOTH SIDE.(SPYING PROTECTION)
OTP ELEMENTS	INPUT ELEMENT OPEN ID IS PROVIDED FROM A THIRD PARTY

IX. CONCLUSION

Current security models in the cloud computing was studied regarding communication process, and data securing. The weak holes in the existing models were defined. In this paper we proposed a new high security model for mobile cloud computing environment which enhances security of user access control, communication, data transmission, and data store security. The proposed communication and access control model applies high secure multi-layer authentication process based on several factors, Static User Name and Password, Trusted (MAC) Address for smart phones and other used devices, Trusted Third-Party (Open ID), Time-Based Dynamic One Time Password and ElGamal algorithm for securing data exchange and communication over the internet. To Illustrate and evaluate the proposed approaches, two applications were developed for Android smart phones and desktops.

Further new security policy was proposed by using Serpent encryption algorithm for encrypting data before storing and uploading to the cloud storage. The proposed model proofed to be more secure than all existing ones with more processing cost.

REFERENCES

[1] Chang-Lung Tsai and Uei-Chin Lin, (February 2011) Information Security of Cloud Computing for Enterprises, Volume 3, issue1.16, Number 1.

[2] Markus Johnsson & A.S.M FaruqueAzam,(March *2011*) Mobile One Time Passwords and RC4 Encryption for Cloud Computing, Master Thesis,Computer and Electrical Engineering Halmstad University.

[3] Priyank Singh Hada ,Ranjita Singh ,MukulManmohan,(2011) A Mobile Agent Based Trust Model for Cloud Computing,nternational Journal of Computer Applications Volume 36 - Number 12.

[4] D.H. Patil, Rakesh R. Bhavsar, Akshay S. Thorve, (2012) Data Security Over Cloud ,Emerging Trends in Computer Science and Information Technology -(ETCSIT2012) Proceedings published in International Journal of Computer Applications® (IJCA)

[5] GouglidisAntonios, (2011)Towards new access control models for Cloud computing systems. University of Macedonia, Department of Applied Informatics, European Cup 2011.

[6] Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)", in Federal Register, Volume62, Number 177, pp 48051-48058.

[7] Sherif El-etriby, Eman M. Mohamed, Hatem S. Abdul-kader, (2012) Modern Encryption Techniques for Cloud Computing, Umm Al-Qura University, and Menoufia University, Computer Science Department.

[8] Harry Katzan, Jr. (2009) Cloud Software Service: Concepts, Technology, Economics, Savannah State University, Savannah, GA 31404, Service Science 1(4).

[9] Roger Elrod, (July,2005) Two-Factor Authentication, Semester Project. East Carolina University. DTEC 6870.

[10] TaherELGamal, (Jul 1985)APublic Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, Transaction on information theory, Page(s): 469 – 472, VOL. IT-31, NO. 4.

[11] Ron Rivest, Adi Shamir, and Leonard Adleman Certification: PKCS#1, ANSI X9.31, IEEE 1363.1977