An Improved Mutual Authentication Framework for Cloud Computing

Sanjeet Kumar Nayak
Dept. of Computer Sc.&Engg.
National Institute of Technology Rourkela
Rourkela, Odisha, India

Subasish Mohapatra
Dept. of Computer Sc.&Engg.
National Institute of Technology Rourkela
Rourkela, Odisha, India

Banshidhar Majhi
Dept. of Computer Sc. &Engg.
National Institute of Technology Rourkela
Rourkela, Odisha, India

ABSTRACT
In this paper, wehave propose a user authentication scheme for cloud computing. The proposed framework providesmutual authentication and session key agreement in cloud computing environment. The scheme executesin three phases such as server initialization phase, registration phase, authentication phase. Detailed security analyses have been made to validate the efficiency of the scheme. Further, the scheme has the resistance to possible attacks in cloud computing.

General Terms
Cloud and Security

Keywords
Cloud computing, Double Authentication, Password change, Mutual Authentication, Session key agreement

1. INTRODUCTION
Cloud computing is the rapid growing Internet based technology that allows computer resources to be shared on an on-demand basis. In cloud computing end-user don't aware about where data is stored and how their data is being processed. They only access data, process and finally store them in the cloud.They can access data at anytime, anywhere if they are having Internet connection. This technology is highly scalable, flexible and distributed in nature.In cloud computing computational resources are provided to the end-user as a service[1]. The most acceptable definition for cloud computing is "a model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[2]. Services provided by cloud computing are virtualization of software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS).Public cloud and private cloud are two basic categories of cloud computing[3]. The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services. On the other hand, private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party[11].

Now-a-days more and more data of individual and companies are placed in cloud, more concerns are given towards the safety and security.As cloud computing is newly evolved technology so there are many issues such as reliability, ownership, data backup, data portability and conversion, multiplatform support and many more. Among all those issues security is one of the important issue[14]. Security issuesinvolve virtualization security, distributed computing security, application security, identity management, access control and authentication[4]. An US research firm Gartner released a report named as "Assessing the security risk ofcloud computing" in June 2008. In this they have mentioned risks in data storage, data recovery, data integrity and data privacy, data confidentiality[5].

Ensuring confidentiality does not guarantee security. Along with it we have to consider the authentication and authorization feature[6]. Authentication is to validate that both parties involved are who they claim they are. The authenticated users can read and write data that is stored in cloud. User ID and a password is required for authentication[7]. Lot of security flaws are present in cloud computing. So strong user authentication framework is required in case of cloud computing[3].

This challenge motivates us to develop an improved mutual authentication framework which contain three phases such as Server Initialization, Registration, Login and Authentication. Besides these three phases we have given a password change phase. We have introduced doubleauthentication[7] in phases. In double authentication first the user enters his password and user ID, if both matches then he proceed for the second round in which server triggers an application which generates a dynamic token. This token is send to his email ID and for authentication he has to enter that token's value when asked for completion of authentication process. In addition to authentication it also provides session key between the client and server and mutual authentication[8][13].

The rest of the paper is organized as follows. Section 2 contains related work. Section 3 describes the cloud security architecture. Section 4 expresses the proposed user authentication scheme for cloud computing. In Section 5 we discussed security analysis of proposed framework. Finally Section 6 accounts conclusion and future work.

2. RELATED WORK
Cloud computing is a version of client server architecture where thousands of clients use the same infrastructure at a large scale. In order to propose a strong authentication framework in cloud computing we have reviewed some existing authentication scheme based on client server architecture.

Most popular remote authentication procedure was suggested by Lamport in 1981[15]. In this scheme server stores both the user's id and hashed password in a table which is used for verification. The password is generated dynamically using a one way hash function which generates a series of passwords. The security of the scheme can be broken if adversary modifies the table.

Recently some smartcard based password authentication schemes have been proposed [16][17]. Smart card is used to prevent from the attack made by adversaries. But due to its low

memory and processing power it can't be suitable for cloud platform.

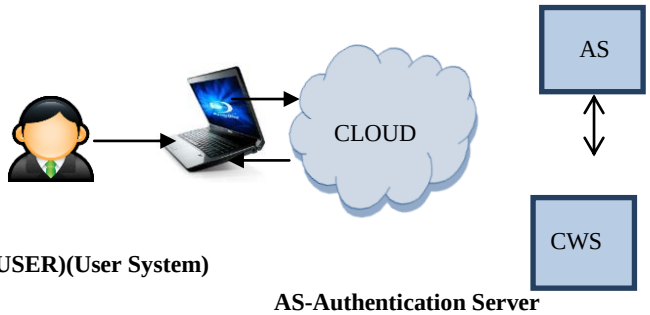
Another scheme proposed by Liao etal.[18] in which they have used public key cryptography. But they send the password andused id in plaintext. Plaintext data can be easily intercepted by intruders. This scheme doesn't care about the confidentiality and privacy of users. In addition to this the scheme doesn't provide password change option which can be a flaw during real time environment.

Some of the recent paper [3] have proposed authentication based on sending one time password to registered mobile number. The SMS system doesn't guarantee to deliver the token at real time. The data can still be intercepted by the malicious persons.

As mentioned in the above literature review, the existing user authentication schemes have many blemishes. In this paper we have suggested a two way authentication process and incorporate password change procedure.We have used registered mail-id to send the dynamic token which is more secure than the mobile SMS system of sending token.

3. CLOUD SECURITY ARCHITECTURE

Cloud security architecture isdepicted in figure 1 where we have proposed our authentication scheme. In the figure Authentication Server (AS) is for authenticating the users and Cloud Web Server is for providing services to end users.



(USER)(User System)

AS-Authentication Server

CWS-Cloud Web Server

Figure 1. Cloud Architecture

3) AS generates a one-time token and sends to the registered email-id.
4) User enters that token in the system within the threshold time because after that the token will expire and user has to login again.
5) After successful login the user is allowed to login to the cloud system.

The next section contains the proposed user authentication process.

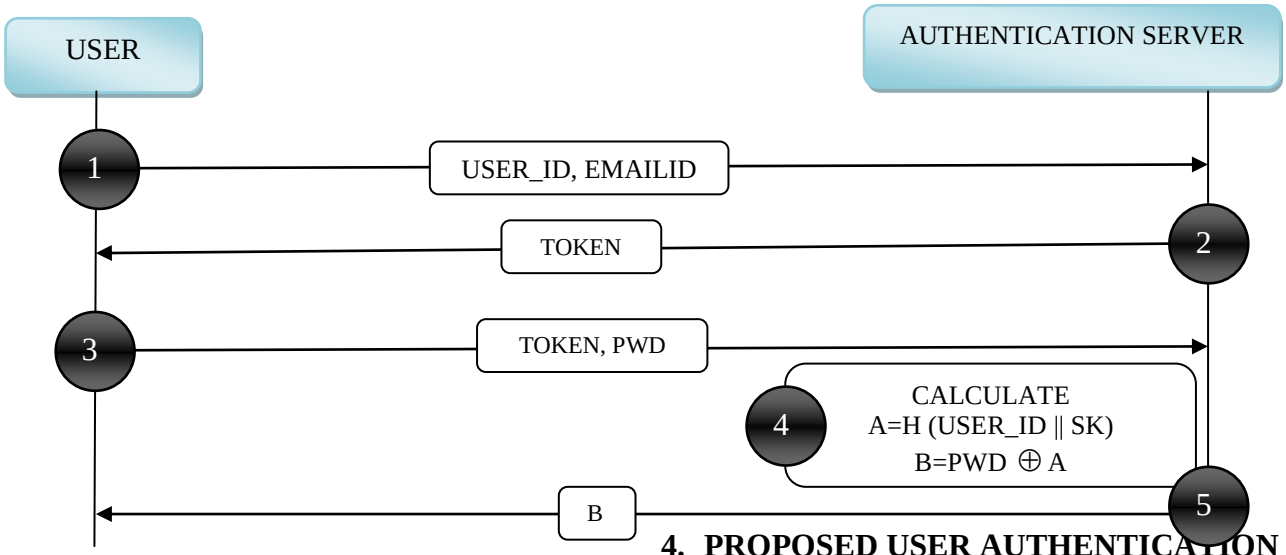


Figure 2. Registration Phase

As shown in figure 1 the basic idea of the proposed scheme is as follows.

1) In the first phase system initializes the secret key for the users.
2) In the second phase registration of the user is done using double authentication.
3) In the third phase authentication is done using nonce. AES encryption function is used to transfer data.

User is authenticated in the third phase in the following way.

1) User enters USER_ID and the PWD in his system.
2) User system sends them to the cloud.

4. PROPOSED USER AUTHENTICATION

In our proposed scheme some notations are used. List of those notations and their meaning are listed in Table 1.

Table 1. Terminology used in our authentication scheme

Notation	Meaning
SK	Secret key
USER_ID	User identification
PWD	Password
H	Hash function
$\|\|$	Concatenation
$\oplus$	XOR operation
N_USER	Nonce generated by user
N_SERVER	Nonce generated by server
M_USER	User message
M_SERVER	Server message
O_PWD	Old password
N_PWD	New password

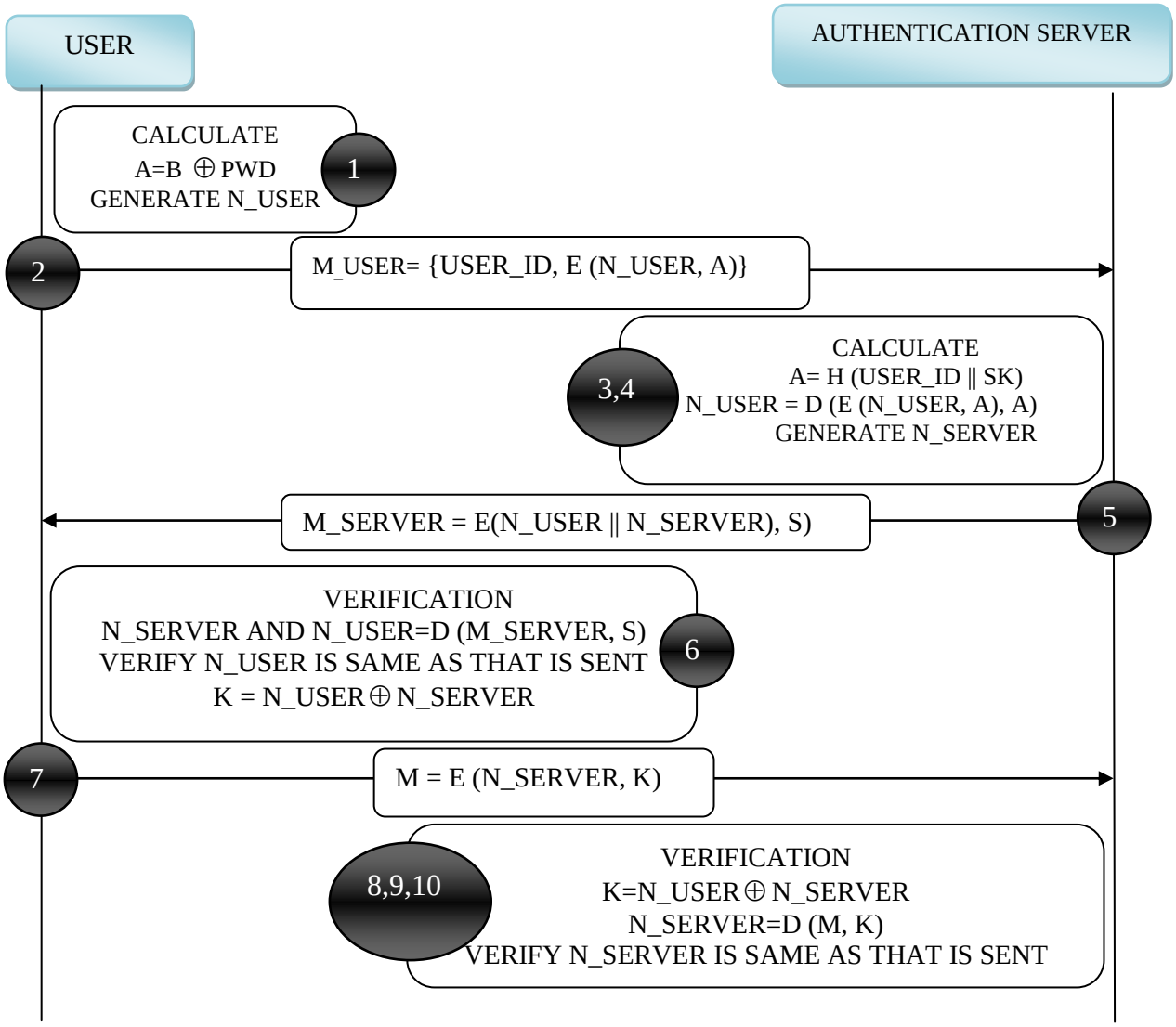


Figure 3. Login and Authentication Phase

4.1 Server Initialization Phase

In this phase the Authentication Server generate secret keys(SK) for the users. SK is unique in nature and usually it varies from user to user. This key is also used in third phase while authenticating the users. This is hidden from the registeredusers.

4.2 Registration Phase

When a new user wants to access the cloud resources, he has to register. In order to interact with the cloud system user should have a valid e-mail ID. Our scheme assumes they are providing right information. The registration process is described below.

STEP 1 The user chooses an identity (USER_ID), and inputs through his system to AS. Then AS checks whether that USER_ID is already registered. If not then scheme goes to STEP 2 else it asks the user to give a new USER_ID.

STEP 2 User inputs his valid email id to the server. The authentication server generates a dynamic token and sends this to user's Email-ID via text message.This step provides double authentication in registration phase.

STEP 3 The user enters that token by checking his registered Email-ID and his password (PWD) to confirm his registration.

STEP 4 AS computes A = H(USER_ID || SK) and B = PWD $\oplus$ A, where H is a hash function [9], || denotes concatenation and $\oplus$ denotes exclusive-or operation.

STEP 5 AS sends B to user's registered Email-ID.

Adiagrammatic representation is shown in Figure 2.

4.3 Login and Authentication Phase

Whenever the user wants to communicate with CWS second time onwards, he must go through the following steps to authenticate himself. Here AS decides user should be allowed to login or not.

STEP 1 The user enters his USER_ID and PWD in the login interface of his system. Then, the user's system computes the secret value A = B $\oplus$ PWD using the stored value of B which was already sends by AS in registration phase.

STEP 2 The user'ssystem generate a nonce (random number used once) N_USER, and then sends to the authentication server the message M_USER, containing
the USER _ID and an encrypted value of the nonce N_USER, as M_USER = [USER_ID, E (N_USER, A)]
where E is AES[10] encryption function. Here N_USER
is encrypted using A as key. Encrypted value of N_USER is used to achieve confidentiality.

STEP 3 AS receives the message M_USER,it computes the secret value A as H(USER _ID || SK).

4.4 Password Change phase

This phase is used when the users want to change his password from O_PWD to N_PWD. The steps of this phase are listed below.

STEP 1 User enters his USER_ID and O_PWD in his system and request message for password change to AS.

STEP 2 AS checks this with the stored password in the database and if both are matched then the AS send a dynamic token to his registered Email-ID.

STEP 3 Upon receiving the token the user inputs it when the server asks to enter N_PWD.

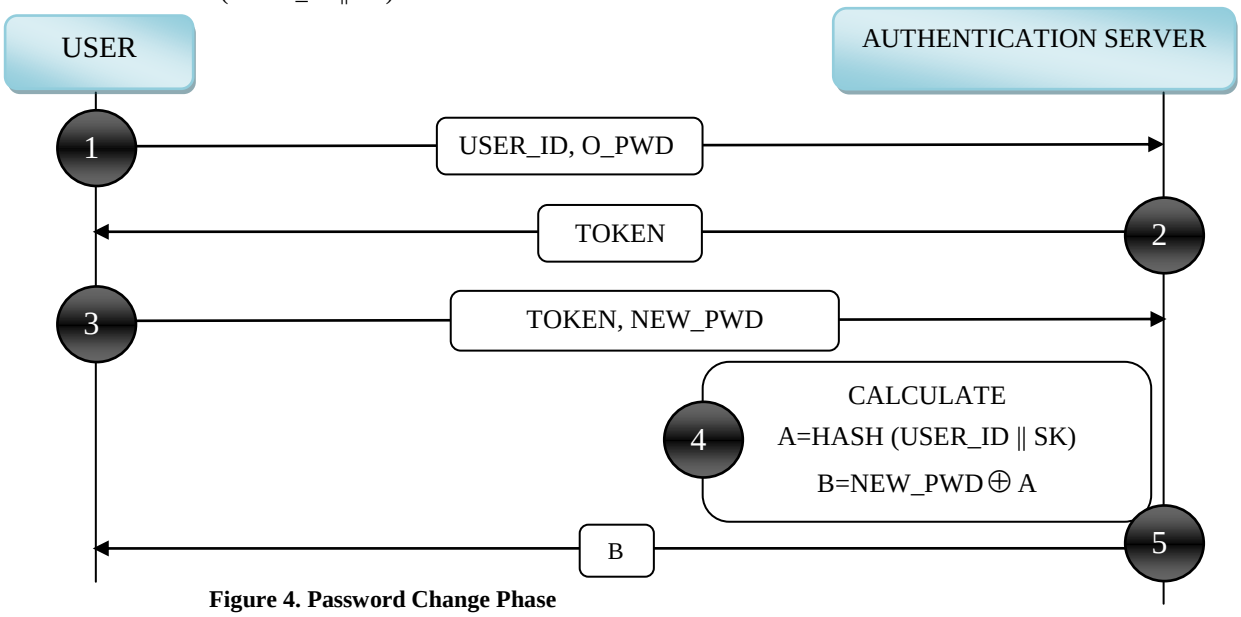


Figure 4. Password Change Phase

STEP 4 AS decrypts the message M_USER and extracts N_USER as D(E (N_USER, A), A) where D is AES decryption function.

STEP 5 The server generates a nonce N_SERVER and sends M_SERVER = E (N_USER || N_SERVER, S) to the user's registered Email-ID.

STEP 6 User check's his Email-ID and upon receiving the message M_SERVER, the user's system decrypts it and
extract N_USER and N_SERVER. User's system verifies that the received N_USER is equal to the sent N_USER.This step is used for double authentication in login phase.

STEP 7 If both are equal, the user computes K = N_USER $\oplus$ N_SERVER and then sends M = E (N_SERVER, K) to the server.

STEP 8 Upon receiving the message M, AS decrypts M and then extracts N_SERVER. AS verifies that N_SERVER received is equal to N_SERVER sent.

STEP 9 If both are equal, the cloud server trusts the user and allows him to communicate with the cloud server.

STEP 10 The key K established between the user's system and the cloud server can be used as a secret key for secure communication.

Adiagrammatic representation is shown in Figure 3.

STEP 4 Then the server calculates A = H (USER_ID || SK) and B = N_PWD $\oplus$A.

STEP 5 Server sends B to the user's Email-ID and a successful message of password changed.

Adiagrammatic representation is shown in Figure 4.

5. SECURITY ANALYSIS

The security of the proposed scheme depends on how vulnerable the secret key SK. SoSK must be kept secret. We mustn't reveal this SK to Authorized users also. The server should choose a value that can't be guessed by attacker (to avoid guessing attack).

Due to the following properties of hash function [9] [12] we have used in our scheme.

I. Given a hash function H and Y=H(M), it is difficult to find any message M′, such that Y=H(M′). This criterion of cryptographic hash function is called as preimageresistance. If the hash function is not preimage resistance, adversary can intercept the digest H(M) and can create message M′. He can then send M′ to AS pretending it is M.

II. Given M and H (M), it is difficult to find M ≠ M′, but H (M) = H (M′). This criterion of hash function is called as second preimage resistance. If intruder can find a message M′ such that H (M)=H(M′), then he can forge the message.

III. Finding M and M′ such that M≠M′, but H (M) = H (M′).

This criterion of hash function is called as collision resistance. It restricts adversary to find two messages that hash to same digest.

Based on the above properties of hash function, the registration phase of proposed scheme is secured. If the imposter knows the value of A, still he can't find the value of SK as A is found using hash function.

Due to the following property of AES function we have used it in our scheme.

I. It is difficult to decrypt the message M_USER, M_SERVER, M without knowing the value of the secret key. This protects data from disclosure attack. It takes lot of time to do brute-force attack on AES. This would be almost impossible.

II. We have used Nonce in our scheme to avoid replay attack. A new nonce means present time and a used nonce means past time. So reply attack can't possible with nonce.

Due to the above two reason login and authentication phase is also secured.In addition, the suggested scheme satisfies the following security features.

Next section explains our proposed authentication model that satisfies following security features.

5.1 Mutual Authentication

In case of mutual authentication user must prove its identity to the server and server must prove its identity to user. It is also called as two way authentication.In our scheme both the user and the server authenticate each other. This avoids the attacker to behave like a server. In login and authentication phase user check's server's authenticity in step-6 and vice versa is done in step-8. Usage of nonce in our scheme provides this facility. Mutual authentication also protects against frauds like man in the middle attack, pharming, keyloggers.

5.2 Session Key Agreement

In our scheme, the secret key (K) is shared by both the AS and user if third phase of propose scheme is successfully ends. Using this key they can communicate with each other for a particular session.

5.3 Password Change

In our scheme the password change phase makes the scheme stronger than the static password based schemes. Hence it gives flexibility for the user to change the password. So our scheme is a user friendly scheme. Regular change in password increases the security of the framework. This phase can help the users if they forgot the password by recovering it using their registered Email-ID.

5.4 Non-Reply Attack

In case of reply attack adversary intercepts the data and retransmit it.We know time-stamp, session tokens, one-time password are methods used to ensure that the message is not a replayed one. We have used a nonce in our scheme which ensures that the message is not a replayed one. Nonce is time-invariant. Nonce is generated with a large number of bits. So the probability of repetition of same nonce is very low.

5.5 Identity Management

The AS stores all the registered USER_IDs. AS checks availability of unique ID in each new registration. This is provided in the registration phase of our proposed scheme. Identity management avoids duplication of user ids.

5.6 Scalable, Secure and Faster

As highly scalable servers are used in our scheme it can handle large number of simultaneous users request at a time. This increases the scalability of the scheme.

Dynamic token is used in the authentication phase. The login phase uses HTTPS protocol for sending tokens and interaction with the users. Hence our scheme is more secure than existing schemes.

Our scheme uses XOR operation for performing calculation. It isn't a costlier mathematical operation. Hence the scheme is faster as compared to schemes based on public key cryptography.

6. CONCLUSION

In this paper, we have proposed a mutual authentication scheme to enhance the security mechanism in cloud computing with many security features such as mutual authentication, session key agreement between the users and the cloud server. We have introduced the flexibility of changing password to the user. In addition, cloud computing being a repository of computingresources, resource constrains are given less priority to provide high security to the cloud. The proposed protocol can resist many popular attacks such as replay attack, password stolen attack etc. Currently, study on some formal security proofing technique is on process,and providing formal security proof to the proposed framework will be the future research goal. Future research also includes preserving the privacy of the user's information provided to the server.

7. REFERENCES

[1] Morsy M. A., GrundyJ. and Muller I., "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[2] Mell P. and Grance T., "The NIST Definition of Cloud Computing", vol 53, issue 6, 2009.

[3] Choudhury A. J., Kumar P., Sain M.,Hyotaek L. andHoon J., "A Strong User Authentication Framework for Cloud Computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific,2011.

[4] BlumenthalM. S., "Hide and Seek in the Cloud", Security & Privacy, IEEE, vol 8, pp. 57-58, 2010.

[5] Eren U., Yates D. J., "Enterprise fraudmanagement using cloud computing: A cost-benefit analysis framework",18th european conference on information systems, 2008.

[6] Almulla S. A., Yeun C. Y., "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), Second International Conference, 2010.

[7] Prasadreddy P., Rao T.andVenkat S., "A Threat Free Architecture forPrivacy Assurance in Cloud Computing" , 2011 IEEE World Congress on Services (SERVICES),2011.

[8] Cheikhrouhou O.,Koubaa A., Boujelben M. andAbid M., "A lightweight user authentication scheme for Wireless Sensor networks", IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 2010.

[9] Cid C., "Recent developments in cryptographic hash functions: Security implications and future directions",Information Security Technical Report, vol. 11, no. 2, pp. 100 – 107, 2006.

[10] "National institute of standards and technology (nist), advanced encryption standard (aes)", Federal Information Processing Standards Publications (FIPS PUBS) 197, 2001.

[11] Sonasinky B., "Cloud Computing", Wiley india Pvt.Ltd, ISBN:978-81-265-2980-3.

[12] ForouzanB.A.,"Cryptography & Network Security", Tata Mc.Graw-Hill, ISBN:978-0-07-066046-5.

[13] YasminR., RitterE, WangG.,"An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures", 10th IEEE International Conference on Computer and Information Technology, 2010.

[14] Reddy B. et. Al., "Cloud computing security issues and challenges", 2009.

[15] Lamport L., "Password authentication with insecure communication," Communications of the ACM, vol. 24, issue 11, Nov 1981.

[16] Hwang M.S., and Li L H., "A New Remote User Authentication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics, vol. 46, issue 1, 2000.

[17] ChienH.Y., JanJ.K., TsengY.M., "An efficient and practical solution to remote authentication: Smart card," Computer Security, vol. 21, issue 4, 2002.

[18] LiaoI-En., LeeCheng-Chi., HwangMin- Shiang., "A password authentication scheme over insecure networks," Journalof Computer System Science, vol 72, issue 4, 2006