IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A NOVEL METHOD FOR MUTUAL AUTHENTICATION IN CLOUD COMPUTING

Gangamma Hediyalad[1], Pooja H[2], Azizkhan F Pathan[3], Dr. Chetana Prakash[4]

[1] Assistant Professor, [2] Assistant Professor, [3] Assistant Professor, [4] Professor,
[1]Dept. of CS&E,
[1] Bapuji Institute of Engineering and Technology, Davangere-577004, Karnataka, India.

Abstract: Cloud computing is the fastest emergent internet centered technology for sharing computer resources on an as-needed base. In the cloud, security is really important. We propose a mutual authentication mechanism for cloud users and the cloud. In a cloud context, the framework also manages session keys. The mutual authentication process in this approach is split into three phases: server initialization, registration and authentication. The framework's security has been thoroughly examined in order to confirm its effectiveness. The proposed system is also immune to a variety of cloud computing assaults.

***Keywords* – Cloud Computing, Authentication, Security.**

I. INTRODUCTION

In the discipline of computer science, cloud computing is a popular technique. The cloud, according to Gartner's report [1,] will alter the IT industry. The cloud is transforming our lives by introducing new types of services to users. Users receive cloud services without paying attention to the finer points [2]. Cloud computing is demarcated by the National Institute of Standards and Technology (NIST) as an exemplary for empowering ubiquitous, expedient, on-demand network contact to a communal pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be swiftly supplied and unhampered with nominal administration effort or service provider contact [3]. Cloud computing is based on the notion of resource virtualization, with on-demand and pay-as-you-go policies.

On-demand self-service, global network access, distributed resource pooling, scalability, and measured service are the five key characteristics of cloud computing as stated by NIST [3].

Clouds are classified into three types based on the domain or environment in which they are used: public clouds which are accessible to clients via the Internet from a third-party service provider, private clouds which are available to customers via the Internet from a third-party service provider, and hybrid clouds which are available to customers via the Internet from a third-party service provider. Private Clouds is the one where a business principally turns its IT atmosphere into a cloud and uses it to supply services to consumers, Hybrid Clouds are two distinct clouds amalgamated together, e.g., IBM and Amazon, Google. Public Cloud is business i.e., public, private, internal, or external cloud server instances, or a blend of virtualized cloud server instances and real-world hardware [4].

Overall, cloud computing proposals us traditional facilities such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [5].Because practically all personal and business data is now stored in the cloud, increasing emphasis is being placed on information security and safety. Because cloud computing is a new technology, it raises a number of concerns, including reliability, ownership, data backup, data portability, multiplatform support, and so on. Virtualization security, identity security, application security, distributed computing security, access control, and authentication are among the most pressing concerns.

Ensuring a system's secrecy does not imply that it is secure. We must ensure that the system has authentication and authorization mechanisms for increased security. The authentication component ensures that both parties to a conversation are who they say they are. The data saved in the cloud can be read and written by an authenticated cloud user. The system may employ a User ID and password approach to accomplish this. Because the cloud is a public environment, it has numerous security issues. As a result, in the cloud computing environment, a strong authentication system is required. The cloud service provider is accountable for the cloud's security and privacy. As a result, cloud service providers include security features such as identity management, authentication, and authorization.

II. RELATED WORK

Lamport proposed a method that became quite popular in 1981[6]. The server keeps User ID and hashed password in a table according to this technique. This information is used to verify the user's identity. A one-way hash function is used to dynamically generate the password. . If the attacker modifies the table storing password, security of the system can be easily broken. After this came the smartcard based password authentication scheme proposed by change and lee [7][8] in 2003. In this scheme the remote system and the user authenticate each other in such a way that there is no server spoofing attack. It also resists the reply attack and allows users to change the password. Smart card based authentication prevents the attack by the third parties. As the smart cards have low memory and processing power they are not suitable for the authentication in cloud environment. A new scheme was proposed by Liao I-En [9] which uses public key cryptography. But, in this scheme when the user is logging in he sends the User ID and password in plain text format. The sending of information in plaintext format makes the information more vulnerable. The verification table not being stored in server makes the scheme secure. This scheme requires a different password for each transaction. This structure doesn't attention about the confidentiality and privacy of the consumers. It also doesn't provide any option for password change which will be a flaw in most of the real time environment. In 2010 John Grundy, Ingo Muller and Mohamed Al. Morsy analyzed the various security problems in cloud computing environment [10]. They refer to multi-tenancy, SOA, virtualization and isolation as the major areas where security issues are faced in cloud computing environment. Eren U., Yates D. J [11] proposed a fraud management scheme for enterprises in a cost effective way. Enterprise fraud management system analyses the transaction data for fraudulent patterns. If any fraudulent patterns are detected then investigation is carried out. These systems are made cost effective with the help of cloud computing. Almulla S. A., Yeun C. Y [12] discussed about the information security problems such as integrity, availability and confidentiality. They address the security challenges such as identity and access management, auditing, authorization and authentication of users. Federal Information Processing Standards Publications [13] published a paper on the most popular encryption algorithm, AES (Advanced Encryption Standards). The information regarding the different functions, parameters, symbols used in the report are described. Various input and output parameters, mathematical calculations carried out are discussed step by step. Sonasinky. B discussed about the details of cloud computing in his text book ref. [14]. Right from the introduction to the cloud computing concept basics, cloud architecture, various cloud deployment models, cloud service models, various virtualization techniques and many more concepts have been dealt in detail. Forouzan by his book ref. [15] gives a detailed insight into the various cryptographic techniques and the network security issues and the different ways to solve them. Wang G, Ritter E., Yasmin R.,[16] proposed a framework for authenticating users in wireless sensor networks using cryptography and signature schemes to maintain the confidentiality of information. Awodele O, Kuyoro S. O and I bikunleF[17] analyzed the various security issues and challenges in cloud computing mainly focusing on the cloud service models and different cloud computing types.

III. SYSTEM ARCHITECTURE

The essential principle of the suggested scheme is as follows, as shown in figure 3.1.
1) The system constructs the secret key for the users in the first phase.
2) The user is registered in the second phase employing double authentication.
3) In the third phase, nonce authentication is used.

Mutual Authentication

Both the user and the authentication server must confirm their identity to each other in mutual authentication. As a result, the user and the authentication server should verify each other's identities. This prevents the attacker from impersonating a server and getting system access. This ability is provided by our system using the nonce. This method also protects against frauds such as man-in-the-middle attacks and key loggers.

Session key agreement

If the registration step is completed successfully, the authentication server and the user share a secret key (K). The user and authentication server then communicate with each other for a certain amount of time termed a session, using the secret key.

Password change

The system is more adaptable than static password-based methods because of the password update phase. This feature makes the system more user-friendly by allowing users to change their passwords. Changing the password more frequently improves the system's security.

Non-Reply attack

In response, the attacker compromises the data and resends it to another user. The use of a nonce in our method ensures that the message received is not repeated. Nonce is a time invariant with a huge amount of bits created. As a result, the chances of receiving the same nonce again are extremely slim.

Identity management

The authentication server keeps track of all registered users and assigns each one a USER ID. During each registration, the authentication server verifies that each user has a unique ID. This prevents the user IDs from being duplicated.

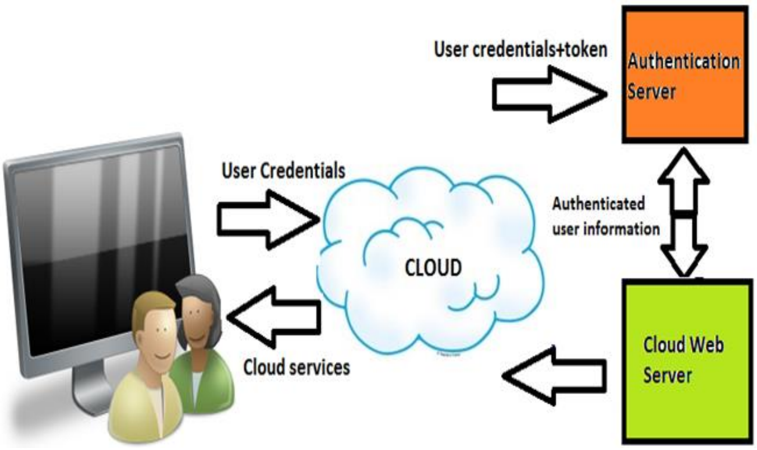


Figure 3.1 System Architecture

IV. ADVANCED ENCRYPTION STANDARD ALGORITHM

Figure 4.1 depicts the Advanced Encryption Standard (AES) algorithm, which is used to encrypt electronic data. The National Institute of Standards and Technology (NIST) of the United States of America established this standard in 2001. The Rijndael cypher structure is used in the AES algorithm. There are various versions of the algorithm depending on the cipher key length which could be of 128, 192 or 256 bits. A special set of keys are derived from the cipher key. They are called as round keys. The whole encryption process uses these round keys. The operations are carried out on an array of data that holds exactly one byte, which takes these round keys as input. This array is called as the state array.

Description of the Algorithm

1. Key Expansions — Using Rijndael's key schedule, each round key is a 128-bit block formed from the cypher key. Each round of AES requires a single 128-bit round key block, plus one extra.
2. Initial Round
3. Add Round Key- On each byte of the state array and the round key for that step, an XOR operation is performed.
4. Rounds

a. Sub Bytes- Each byte in the state array is changed with another pointing to the lookup table in this stage, which is a non-linear substitution.

b. Shift Rows- this is transposition step where the last three rows of state array are cyclically shifted a certain number of steps.

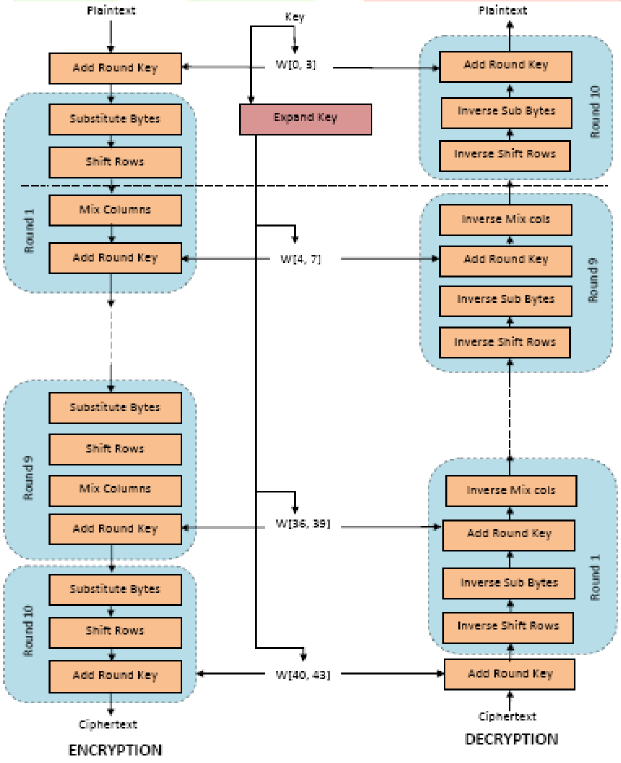


Figure 4.1 AES structure

V. SECURITY ANALYSIS

The vulnerability of the secret key SK determines the system's security feature. As a result, SK must remain a well guarded secret, even from authorized users. The server will choose this SK value to make it harder for the attacker to predict.

Security at registration phase

The attributes of the hash function utilised in our system, which make it more robust, are as follows. Even if the imposter knows what A is worth, he won't be able to figure out what SK is worth because A is calculated using a hash function.

1. Pre-image resistance

Given a hash function H and Y = H(M), it is hard to find any message M`, such that Y=H(M`)

2. Second pre-image resistance

Given M and H(M), it is hard to find M ≠ M`, but H(M) = H(M`).

3. Collision resistance

It is hard to find two messages M and M` such that M ≠ M', but H(M)= H(M`).

Security at login and authentication phase

Because of the following qualities of the AES function employed in this method, the login and authentication phase is more secure.

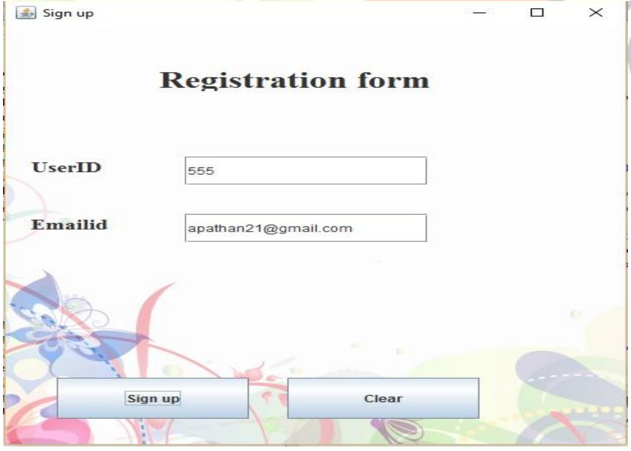
1. Without knowing the secret key's value, decrypting the message M USER, M SERVER, M is challenging. This safeguards data from a data leakage attack.
2. The reply attack is avoided by using nonce in our system. A new nonce denotes the present moment, while a used nonce denotes the past.

After running the Authentication Server, the next step is for the user to register. For this run the Sign up class, which gives a form to enter the user id and e-mail id of the user as shown in figure 6.2. After entering the credentials the user clicks 'sign up'. If the user id entered does not have an entry in the USER table, a new entry is created and the user is registered successfully, else an error message is shown saying that the user already exists.

VI. RESULTS AND DISCUSSION

The figure 6.1 shows that we run the AS class first which runs the authentication server.

Figure 6.1 Authentication Server

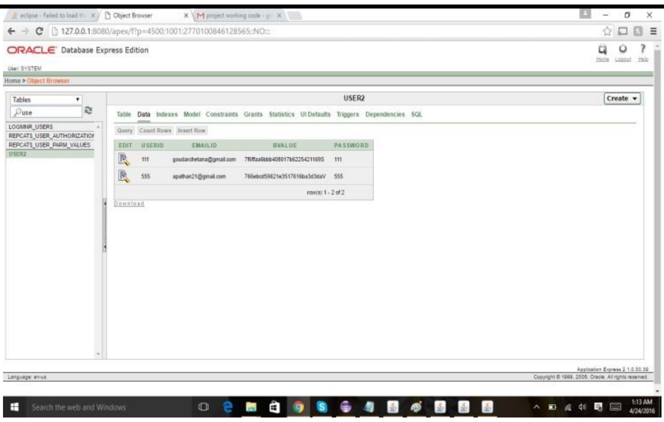


UserID 555

Emailid apathan21@gmail.com

Figure 6.2 Sign up

Now let us see if the new user just registered has an entry created in the MUTUAL table. Click on the 'object browser' to see the list of tables in the database homepage. Click on the 'MUTUAL' table to see the table as shown in the above figure 6.3. We can now see that the entry for the new user who has been registered now is created.


Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:2770100846128565::NO:::
ORACLE Database Express Edition
User: SYSTEM
Home > Object Browser
Tables
use
LOGMNR_USERS
REPCATS_USER_AUTHORIZATIOI
REPCATS_USER_PARM_VALUES
USER2
Create
Table Data Indexes Model Constraints Grants Statistics UI Defaults Triggers Dependencies SQL
Query Count Rows Insert Row
Download

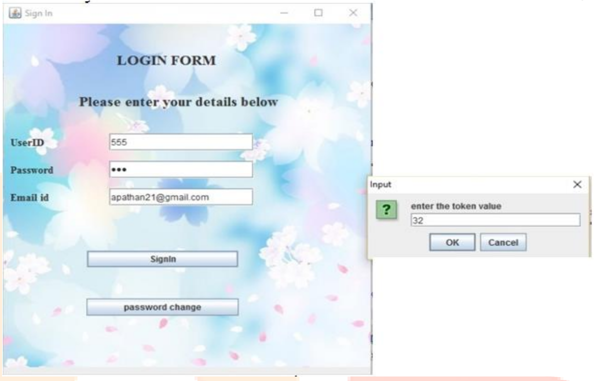
USER2

EDIT	USERID	EMAILID	BVALUE	PASSWORD
	111	goudarchetana@gmail.com	7f6ffaa8bbb408017b62254211695	111
	555	apathan21@gmail.com	766ebcd59621e3517618ba3d3daV	555

row(s) 1 - 2 of 2

Figure 6.3 Mutual Table in Oracle Database

After the user is registered, he has to login into the system. For this the user runs the sign-in class which shows up a form as shown in the figure 6.4. User has to enter the User id, password and e-mail id and then click on sign-in. This will ask user to enter the token value that will be sent to his mail. User enters this token and then clicks ok. Now the user is successfully signed in into the system.



LOGIN FORM

Please enter your details below

UserID 555

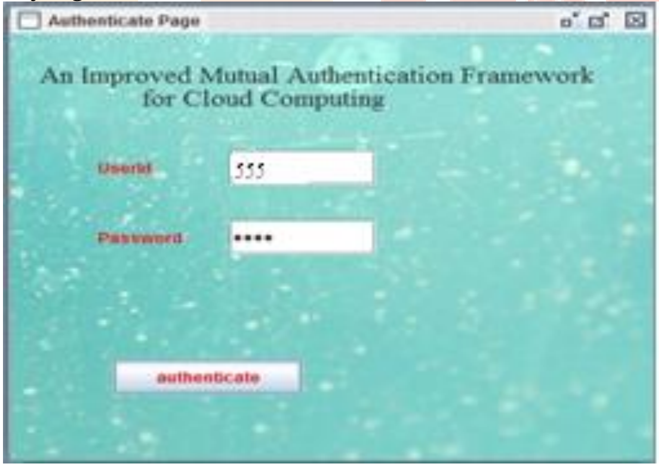
Password •••

Email id apathan21@gmail.com

enter the token value 32

Figure 6.4 Sign-in Page

Figure 6.5 shows the authentication stage, where the user runs the authenticate class and enters the valid user-id and password and clicks on authenticate button. If the user is already registered and entered credentials are correct, then the user is authenticated successfully.



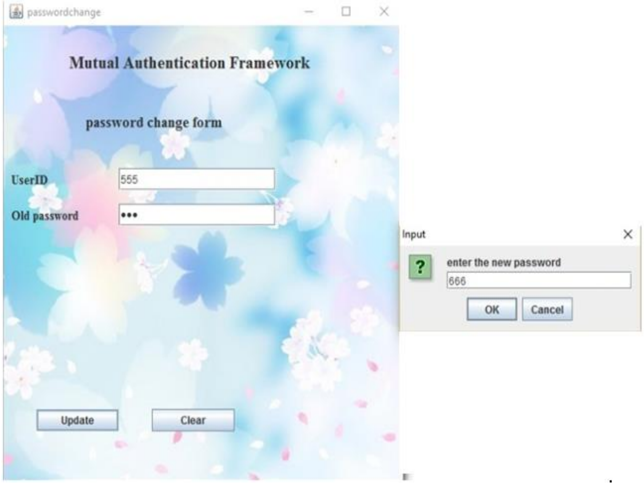
An Improved Mutual Authentication Framework for Cloud Computing

Userid 555

Password ••••

Figure 6.5 Authentication

Figure 6.6 shows the password change phase. Here user clicks on the password change button on the sign-in form which prompts him with another form to enter the credentials for changing the password and then clicks update. After this, if both the entered details are correct, then the user is asked to enter the token sent to his mail.



Mutual Authentication Framework

password change form

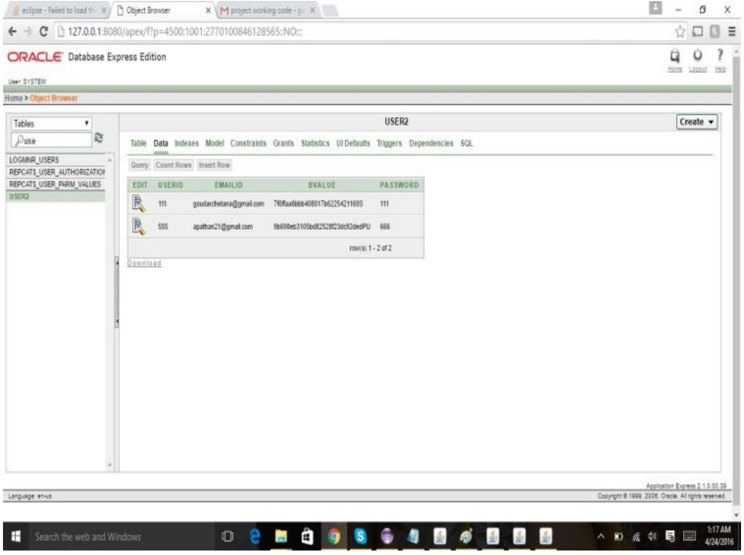
UserID 555

Old password •••

enter the new password 666

Figure 6.6 Password Change-Entering a new password

After user enters the token sent to the user's mail id, he is asked to enter the new password which he wants to set. After the user enters the new password it is updated in the user table as shown in figure 6.7.



127.0.0.1:8080/apex/f?p=4500:1001:2770100846128565::NO:::

User: SYSTEM

Home > Object Browser

USER2

EDIT	USERID	EMAILID	BVALUE	PASSWORD
	111	goudarchetana@gmail.com	7f6ffaa6bbb408017b62254211695	111
	555	apathan21@gmail.com	9b698eb3105bd82528f23dc92dedPU	666

row(s) 1 - 2 of 2

Figure 6.7 Password is updated in User Table

CONCLUSION

This proposed mutual authentication scheme enhances the security mechanism of cloud environment. The double authentication mechanism is introduced and implemented into the system to improve the security features of cloud computing environment. The confidentiality and security of the cloud is improved by allowing only registered users to use the cloud facility. This is bought into action by the registration and authentication facilities. The identity of the cloud users is preserved by identity management and more user friendly cloud environment is created by providing password change facility.

REFERENCES

[1] R. Hunter, "The why of cloud", 2012.

[2] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali, "Cloud computing: Distributed internet computing for IT and scientific research", Internet Computing, vol.13, no.5, pp.10-13, Sept.-Oct. 2009.

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

[4] AlexaHuth and James Cebula, "The Basics of Cloud computing", 2014.

[5] RajkumarBuyya, Chee Shin Yeo, SrikumarVenugopal, James Broberg, and IvonaBrandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems", Volume 25, Number 6, Pages: 599-616, ISSN: 0167-739X, Elsevier Science, Amsterdam, The Netherlands, June 2009.

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

[7] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards", IEE Proceedings-E, vol. 138, no. 3, pp. 165-168, 1993.

[8] Chin-Chen Chang., Jung-San Lee., "An efficient and secure remote authentication scheme using smart cards", An International Journal, Vol.18, 2006.

[9] Liao I-En., Lee Cheng-Chi., HwangMin- Shiang., "A password authentication scheme over insecure networks", Journal of Computer System Science, Vol. 72, issue 4, 2006.

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

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

[12] Almulla S. A., Yeun C. Y., "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), Second International Conference, l(1), 1-7, 2010.

[13] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publications (FIPS PUBS), pp. 197-26, 2001.

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

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

[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[17] Kuyoro S. O., Ibikunle F. &Awodele O., "Cloud computing security issues and challenges", International Journal of Computer Networks, Vol.3, Issue 5, 2011.