Cloud Cognitive Authenticator (CCA)

A Public Cloud Computing Authentication Mechanism

L. B. Jivanadham[1], *A.K.M. Muzahidul Islam [2]
[1,2,4,5]*Malaysia-Japan Int'l Institute of Technology (MJIIT)*
Universiti Teknologi Malaysia (UTM)
54100 Jalan Semarak, Kuala Lumpur, Malaysia
[1]bjlalitha2@live.utm.my
*Corresponding Author: [2]akmmislam@ic.utm.my

Yoshiaki Katayama[3]
[3]*Nagoya Institute of Technology (NITech)*
Gokiso-cho, Showa-ku, Nagoya,
Aichi, 466-8555 Japan
[3]katayama@nitech.ac.jp

Shozo Komaki[4] and S. Baharun[5]
[4]komaki@ic.utm.my
[5]drsabariah@ic.utm.my

***Abstract*— the long awaited Cloud computing concept is a reality now due to the advancement and transformation of computer generations. However, the implementation of this concept as a technology is still at infancy stage due to several issues such as policy, standards, users, security, etc. This paper features the basic concepts of cloud computing, security issues and proposes an integrated authentication mechanism called the Cloud Cognitive Authenticator (CCA). CCA is an API proposed for the cloud environment integrating bio-signals, one round Zero Knowledge Protocol (ZKP) for authentication and Rijndael algorithm in Advance Encryption Standard (AES). CCA is proposed to enhance the security in public cloud through four procedures providing two levels of authentication as well as encrypting/decrypting the user id. The novelty of CCA is that it uses Electro Dermal Responses (EDR) for the first level authentication. Furthermore, the proposed encryption in CCA provides concrete cryptography. Finally, this paper concludes with the future direction of this study.**

Keywords- Cloud Computing security, Integrated authentication mechanism, Cloud Cognitive Authenticator (CCA), API, One Round Zero Knowledge Protocol (ZKP), Advance Encryption Standard (AES) algorithms

I. INTRODUCTION

Computers were initially designed and developed for military purposes, and had advanced tremendously in changing human life in various applications. Rapid advancement and changes of computing device technologies and constant depreciating values of computing resources contribute to the need for technology transformations. Thus, it can be seen that the computing resources are moving towards web based utilization. Cloud computing is a paradigm shift against traditional IT resources setup which offers dynamically scalable resources provisioned as services over the internet [1, 3, 4]. It is believed that cloud computing offers tremendous economic benefits. In addition, cloud computing provides increased mobility, ease of use and portability of applications [2-5], which means users easily access information anywhere.

Cloud computing consists of three layers [1-6]. Infrastructure-as-a-Service (IaaS) [5-6] is the bottom most layer. It provides basic computing infrastructure components such as storage, CPU, memory offered by Citrix, 3tera and VMware who are among the IaaS vendors. These resources are offered to users over the internet on-demand and rental basis. The second layer which serves as a platform to deploy and dynamically scalable web applications such as Google App Engine is known as Platform-as-a-Service (PaaS) [6-7]. The top most layer is called as Software-as-a-Service (SaaS) [6-7]. It provides users with ready to use applications such as Zoho, Google Docs and Microsoft CRM. In addition these services are supported by two main technologies, web services and web browsers to access these services [2]. Web services are commonly used to provide access to IaaS services and Web Browsers are used to access SaaS applications. Both approaches can be found in PaaS.

Irrespective of the service mentioned above cloud computing is commonly deployed in four models [7] based upon customers' requirement. They are *Private Cloud, Community Cloud, Public Cloud,* and *Hybrid Cloud.* Public cloud computing model is adopted in this study because provide increased user mobility, mass energy reduction and cost saving. Public Cloud is a setup which is open for use by the general public [7]. This setup could be controlled, maintained and manipulated by different government organizations or corporate organizations or academic institutions, or any combination of them permitted by the Cloud Service Provider (CSP). On the other hand, public cloud exposes users, their assets in cloud and data to extreme danger since they can be publicly accessed through the internet. Due to these reasons, users and organizations are not confident in adapting to public cloud. This is why the other three models are more favorable to public cloud model. Integration of security, authentication and functionality is vital in maintaining an efficient and effective working environment for the business. One of the

This work is partially supported by grant GUP Tier-2, 2012-2013 with Vote No. 08J77 under Ministry of Higher Education (MoHE) and by MJIIT Research Grant of Universiti Teknologi Malaysia (UTM) Year 2012-2013 with Vote No. 4J044

978-1-4799-0400-6/13/$31.00 ©2013 IEEE

essential tasks in maintaining a secure environment is the control of user identities. Creating and deleting identities, monitoring them, enforcing password policies are routines that are important IT operational tasks. This does not change with the public cloud. Using strong passwords and changing them on regular basis are crucial in a public environment. Even though identity federation ensures these tasks but these identities may be easily stolen and imitated.

In this paper, a Cognitive Cloud Authenticator (CCA) is proposed. The novelty of CCA is that it integrates biometrics, encryption and authentication to ensure durable user id and integrity to public cloud authentication scheme. Cognitive biometrics deploys bio-signals such as EEG, ECG, and EDR as the input to an authentication system which can be used individually or in a multi-mode biometric system. Cognitive biometrics can record both the cognitive and emotional state of an individual which are difficult to forge, and certainly cannot be lost. Typically, the required amount of data can be acquired within 1 minute and is painless.

The AES is proposed, so that the cryptographic deployed in CCA is able to overcome the limitations of XML Encryption which is extensively applied in the current public cloud environment. In addition, this cryptography is proposed in CCA since it is able to withstand Linear Cryptanalysis (LC) and Differential Cryptanalysis (DC).

This mechanism is expected to provide a more accurate user authentication as it is not only relying on the user identity but with the EDR information obtained even the mental state of the user is determined. CCA is able to authenticate users with both valid id and valid intentions and by doing so it addresses the security issues in cloud computing security as discussed below.

WS-Security is an essential specification addressing security for Web Services [9]. Provision of integrity, confidentiality and authentication of Simple Object Access Protocol (SOAP) messages is provided by WS-Security. It defines how existing XML security standards like XML signature and XML Encryption can be applied to SOAP messages. XML signatures allow XML fragments to be digitally signed to ensure integrity while the XML Encryption allows XML fragments to be encrypted to ensure data confidentiality [9-10]. In order to make the encryption possible, XML Encryption defines an Encrypted Key element for key transportation purposes. XML fragment is encrypted with randomly generated symmetric key, which itself is encrypted using the public key of the message recipient. In addition to encryption and signatures, WS-Security defines security tokens suitable for transportation of digital identities e.g. X.509 certificates. XML signatures suffer from "Wrapper attack", where the attacker is able to inject duplicated fragment of XML while adding additional code leading the computer to do additional unwanted tasks [11].

In a cloud environment, browsers are generally used for retrieving and interfacing application. The common defence for browsers is for the server to monitor the original location of these browsers. Whenever a request is made by the browsers, it can only be accepted if the request comes from the same location [10]. This defence is proven to be insufficient form of security. Browsers are not able to utilize the benefits of XML Signature or XML encryption [10]. Therefore, browsers rely on Transport Layer Security (TLS) or Secure Sockets Layer (SSL) security [10]. TLS is the most significant cryptographic protocol as it is implemented in every web browser [9]. The SSL consists two main parts which is the Record Layer that is responsible to encrypt or decrypt Transmission Control Protocol (TCP) data streams using algorithms and keys. These keys are produced in the TLS Handshake [9-10], the second part of TLS which is used to authenticate the server and optionally the client. The key back draw with TLS is "phishing" where users are tricked by malicious websites or individuals to gain users login information [9-10]. Once the attacker obtains the information, TLS become obsolete in protecting data. In this technique, the server is required to have digital certificate and not all pages are secured. Furthermore, the expiration of certificates has to be considered.

APIs have the ability to enhance the cloud experience and provide cross cloud compatibility [10-12]. It allows CSP to integrate applications and other workloads into the cloud. Today, almost every CSP publishes their API's to users for exposing the available features of cloud components to their customers [11] and to facilitate customers to formulate their deployment re-architecture for better mutual benefits [11]. Most CSPs offer generic HTTP and HTTPS API integration to allow their customers greater cloud versatility [10-12]. Furthermore, it is through the cross-platform APIs, cloud tenants have access to the resources not only from their primary cloud provider, but also from others. This saves a lot of time and development energy since organizations can now access the resources and workloads of different cloud providers and platforms. Though CSPs' API's are exceptionally useful to users with regards to the understanding of CSPs components and functions, it also invites attackers' attention to be familiar with the architecture of the CSP and internal design details [11]. Hence, insecure APIs may lead to major security concerns for CSP as well as customers, for examples cyber-attacks and illegitimate control over user accounts [11-12]. At any point-of-time, CSP's cannot eliminate their API's announcement due to the strong influence of web services and XML-blend with respect to cloud computing [11-12]. Lastly, cryptography and key management issues are not something unique to cloud computing. Like any other traditional system, this becomes the most critical requirement also in cloud computing. This, in turn, reflects in the high security risk possibilities. In fact, the need for appropriate, up-to-date cryptographic systems with efficient key management will be the pertinent subject for any CSP with highly sensitive customer information [8-10]. As compared to traditional systems, the huge amount of

business data in the cloud attracts the attention of attackers who constantly eye private information. As the current generation hacking techniques advance to an entirely new level, many of the traditional cryptographic algorithms and mechanisms do not suit the cloud computing trends of today's businesses [8-10].

This paper is organized as follows. In the next section, we provide related works reviewed to achieve the proposed mechanism. In Section 3, we present the proposed integrated authentication mechanism. Then, an analysis of the proposed scheme is provided in comparison with the existing authentication schemes in Section 4. Finally the paper is concluded in Section 5, together with future research directions based on the proposed mechanism.

II. Related Works

In this paper [6], a survey on cloud computing, highlighting its key concepts, architectural principles, and state-of-the-art implementation as well as research challenges are presented. It aims to provide a better understanding of the design challenges of cloud computing and identify important research directions in cloud computing. The next analyzed article [8] includes the current security challenges in a cloud computing environment based on state-of-the-art cloud computing security taxonomies in technological and process-related aspects.

Biometrics is a measure where features of individuals are captured to uniquely characterize the individuality of a person. It involves the collection and digitization of vectored data from the authentication apparatus. It is then sent to a computer with a signal processing algorithm to extract characteristic features which are the biological signature of the person [13]. These features are stored in a database and they are compared with newly extracted features to authenticate a person's ID [13-14]. Such features are extracted from fingerprints, iris of the eye, voice, signature, facial characteristics, walking patterns, typing patterns, and DNA [13-14]. Extensive research has deduced that certain patterns of fingerprint, iris minutiae, voice spectrum are unique to a person [14]. However, fingerprinting has been shown not to be foolproof as the fingerprint of a person may be lifted from a drinking-glass and then used by an impostor [14]. The iris identification devices may also be fooled. As for the voice identification, technology advancement has shown that with proper frequency synthesizers one's voice can be modified to emulate another person's voice [14]. A person's signature has been used as an identifier for centuries. However, a large number of forged signatures have shown that the signature itself is a weak method to prove one's identity [14]. Even the facial and anatomical characteristics which are unique to a person have been shown that they can be temporary or permanently altered to imitate someone else's characteristics [14]. Walking habits may be used to identify a person. However, good imitators mimic one's walking habits [14]. Author in [14] reviews the history of designs of a particular branch of effective technologies that acquire electro dermal response readings from human subjects. Electro dermal response meters have gone through continual improvements to better measure these nervous responses in this article. Electro dermal response traditionally has been labour intensive. Protocols and transcription of subject responses were recorded on separate documents, forcing constant shifts of attention between scripts, electro dermal measuring devices and of observations and subject responses. These problems can be resolved by collecting more information and integrating it in a computer interface that is, by adding relevant sensors in addition to the basic electro dermal resistance reading to untangle body resistance, skin resistance, grip movements; other factors affecting the neural processing for regulation of the body. A discussion whether electro dermal response data streams can be enriched through the use of added sensors and a digital acquisition and processing of information, which should further experimentation and use of the technology. This paper [14] highlights the deployment of bio-signals as the basis for a novel approach to biometrics, termed 'cognitive biometrics.' Cognitive biometrics deploys bio-signals such as EEG, ECG, and EDR as the input to an authentication system which can be used individually or in a multi-modal biometric system. These signals can be acquired using a single technology, electrodes placed in the appropriate place on the body surface (head and arms). Typically, the required amount of data can be acquired typically within 1 minute and is painless. User acceptance issues may need to be addressed but scalp based EEG electrodes, which typically require the use of conductive gels are being replaced through dry-electrodes, which do not require conductive gels, and are therefore easier to apply. Cognitive biometrics can record both the cognitive and emotional state of an individual which are difficult to forge, and certainly cannot be lost. They can be deployed for both static and continuous based biometrics, and can certainly be applied in conjunction with behavioural biometrics such as keystroke dynamics. These are issues that need to be addressed by the biometrics community at large. On the other hand, different systems may require different types of credentials to determine user identity where credential is the evidence or documentation provided by a user in the process of user authentication, in this paper [17-18] an integrated authentication mechanism using the Zero Knowledge Proof (ZPK) and the Rijndael algorithm in Advance Encryption Standard (AES) has been proposed for a dynamic wireless sensor network. The Zero Knowledge Proof (ZKP) protocol is a powerful cryptographic system that can be applied in many cryptographic applications and operations such as identification, authentication and key exchange is elaborated in [17-18]. The uniqueness of ZKP is that the claimant protects the confidentiality of the secret at any cost by not revealing anything. The framework of ZKP is described in

[17-18] where the claimant is responsible to proof she knows a secret, without revealing it to the verifier.

The Rijndael algorithm in Advance Encryption Standard (AES) is a symmetric scheme which appears as a better option as it offers better computational efficiency by computing extremely fast due to the application of simple operations and efficient executions. This scheme provides a considerably smaller and very secure key size, 128-bit keys [18] besides requiring inexpensive hardware as it performs simple algorithms. The Rijndael symmetric keying scheme algorithm is further studied to determine the applicability in this research. Rijndeal algorithm is an iterative block cipher, which means that the initial input block and cipher key undergo multiple transformation cycles before producing the final output [18]. The algorithm can operate over a variable-length block using variable length keys. A 128, 192, and 256 bits long, and all nine combinations of key and block length are possible. The algorithm is written so that block length and key length can easily be extended in multiples of 32 bits, and the system is specifically designed for efficient implementation in hardware or software on a range of processors [18]. The Rijndeal algorithm offers a combination of security, performance, efficiency, ease of implementation and flexibility [18]. The Rijndeal algorithm appears to be consistently a very good performer when implemented in both hardware and software across a wide range of computing environments.

III. CLOUD COGNITIVE AUTHENTICATOR (CCA)

Cloud Cognitive Authenticator (CCA) is a cloud utility provider API proposed to provide a cognitive authentication mechanism. CCA uses data captured from an EDR biometric scanner when the users request to establish connection with the hypervisor to access the cloud services. EDR is the skin conductance of the user consisting user behavioural or mental state information. CCA will authenticate the skin conductance level, and then merge this detail together with other user details namely device and network information as the user id, which will then be encrypted and decrypted for further authentication and access to the cloud services as illustrated in Figure 1. By adopting CCA, not only users with valid id but also with valid intentions are distinguished in prior to allow accessibility to resources. This is achieved from the electro dermal or skin conductance responses obtained from skin conductance meter. The conductance may vary by micro-siemens as the skin and muscle tissue response to external and internal stimuli. When the device is correctly calibrated, it measures these minute differences. The Skin Conductance Response (SCR) is highly sensitive to emotions in some people such as fear, anger, startle response, orienting response and sexual feelings which may produce similar skin conductance responses [16]. These reactions are utilized as part of the polygraph or lie detector.

The authentication mechanism in CCA is proposed to have four procedures where procedure one (P1) and

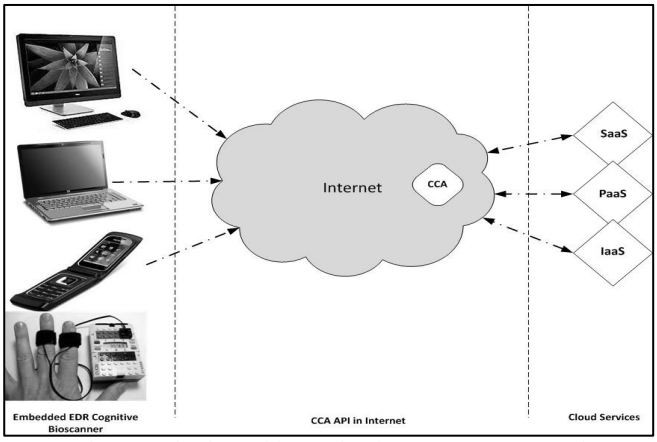

Figure 1: Cloud Cognitive Authenticator (CCA) Framework

procedure four (P4) provides two different levels of authentication whereas procedure two (P2) and three (P3) is suggested in conducting the cryptography tasks. These procedures are shown in Figure 2, where the first procedure is P1, called Electro Dermal Response (EDR) Authenticator. Here, the captured EDR reading of the skin conductance meter [17] is converted, and then this skin electrical conductance [17] is verified to determine the users' emotional and physiological arousal. If this procedure validates the users' skin conductance responses as normal, then it proceeds to P2, the User Id Generator or Encryptor procedure which is responsible to generate the user id by merging *EDR reading, IP address, device details* and *hypervisor connection start time* and encrypt this id using the Rijndael Algorithm [17-18]. Once the user id is encrypted it is transmitted to the third procedure of CCA, P3 that is the User Id Decryptor. At this procedure the user id is decrypted using Rijndael Algorithm. Upon successful decryption P3 requests the next procedure P4, ZKP Authenticator to establish connection with the hypervisor. Following this, ZKP Authenticator responds to the request by providing a randomly generated variable *c* [17-18] based on One Round Zero Knowledge Protocol (ZKP), to authenticate the authenticity of the hypervisor connection

P1	**ELECTRO DERMAL RESPONSE (EDR) AUTHENTICATOR**
P2	**USER ID GENERATOR/ENCRYPTOR**
P3	**USER ID DECRYPTOR**
P4	**ZKP AUTHENTICATOR**

Figure 2: Cloud Cognitive Authenticator (CCA) Procedures

request earlier. EDR Authenticator procedure then responds to the challenge by computing the secret, *r* [17-18] using *c*. Finally, the ZKP Authenticator procedure validates *r* to ensure the validity of the secret. CCA uses the integrated authentication and encryption mechanism suggested in [18-

19]. The uniqueness of this scheme is that it combines the techniques of biometrics, AES and One round ZKP. This scheme offers a consistent performance when implemented in both hardware and software across a wide range of computing environments. This integration is not only providing a flexible and ease of implementation, but it also delivers a robust security scheme without acquiring large storage devices and processing power allowing the cloud environment to achieve the green computing objective. When this scheme is integrated with the cognitive biometric device, it will provide a solitary user identity as it is unique to every user. In addition, CCA algorithm semantics are also illustrated in Figure 3 below.

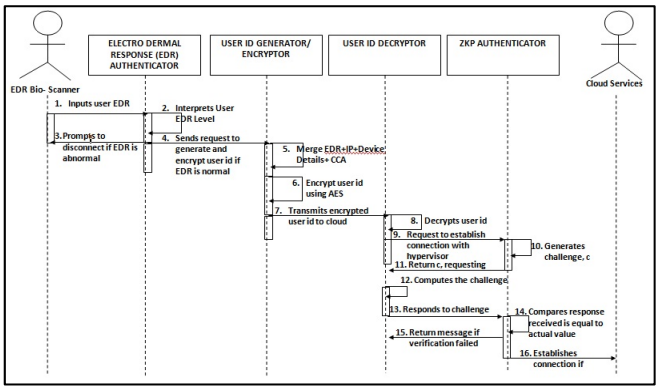

Figure 3: Cloud Cognitive Authenticator (CCA) Algorithm Semantics

The operational semantics of *CCA Algorithm* are provided below:

% When a user is requesting to connect to the cloud to access his resources

Let *c* = challenge generated by ZKP Authenticator, r = response computed by EDR Authenticator

1. **Start**
2. Input : = Skin Conductance Response, IP, device details, request initiation time;

% EDR Authenticator interprets the input

3. **If** User EDR level: = 1
   User id: = merge (*EDR reading + IP+device details + request initiation time)*;
   Else
   Message is sent to the user *"Your SCR is not normal, please try again later"*;
   End If
4. User id is encrypted using AES block cipher;
5. Encrypted user id is received by ID Decryptor;
6. ID Decryptor requests to establish a Connection with hypervisor;
7. ZKP Authenticator generates variable := c [17-18] and transmits to EDR Authenticator;
8. EDR Authenticator computes variable := r [17-18] as respond to the challenge;

% ZKP Authenticator authenticates

9. **If** r: = True
   Connection between user and hypervisor is established;
   Else
   Message is sent to user *"Your access is denied"*;
   End If
10. **End**

IV. CCA And Existing Schemes Analysis

Presently, most authentication schemes are based on user ids, either the biometric ids such as fingerprints, iris, voice or the traditional id such as passwords. Based on the existing security schemes for cloud computing such as the WS-Security and TLS/SSL, Table 1 is derived by comparing and analyzing the authentication techniques enabled in each security scheme. Through the analysis it is discovered that these schemes become obsolete once the user ids are stolen or imitated. Besides, this comparison enables to determine the authentication techniques which may be integrated in the proposed scheme. Therefore the analysis, in proposing CCA enabling existing authentication techniques to be employed such a password and location based, in addition it also considers the EDR information which obtains and determines even the mental state of the user. Through this technique, anyone accessing cloud resources with malicious intentions will be denied of access, even though the user id is stolen or imitated. By employing One Round Zero Knowledge Protocol in CCA, it provides the ability of the claimant to protect the confidentiality of the secret. Here, both claimant and verifier are unable to cheat each other and the verifier is not able to learn anything from the protocol. Consequently, the verifier cannot pretend to be the claimant to a third party. Finally, using AES cryptography for encryption and decryption as compared to the XML encryption eliminates the possibility of weak, semi weak keys and equivalent keys. Table 2, tabulates the possible attacks in WS-Security and TLS/SSL. These schemes are vulnerable against wrapper attack, Man-in-the-Middle (MITM) attack and Cross Site Scripting (XSS) attacks. Based on this analysis CCA is proposed to integrate the Rijndael Algorithm in AES to solve the vulnerability of cloud computing against the similar attacks.

Table I: Comparison between Existing Cloud Authentication and CCA

Cloud Utility Provider Security	**ATTACKS**					
	Wrapper	MIMT	XSS	SQL Injection	Phishing	Square Attack
WS-Security	×	×	×	×	×	✓
TLS/SSL	×	×	×	×	×	✓
CCA	✓	✓	✓	✓	✓	×
LEGEND: ✓ Protected			× Not Protected			

TABLE II: COMPARISON BETWEEN EXISTING CLOUD SECURITY AND CCA ATTACK DEFENCE STRENGTH

Cloud Utility Provider Security	AUTHENTICATION						ENCRYPTION	
	Phase 1					Phase 2		
	Password	Digi-Cert	Biometrics	Location	EDR	One Round ZKP	XML	AES
WS-Security	✓	✓	✓	✓	×	×	✓	×
TLS/SSL	✓	✓	✓	✓	×	×	✓	×
CCA	✓	×	✓	✓	✓	✓	×	✓
LEGEND: ✓ Fulfilled × Not Fulfilled								

Unlike the existing schemes, CCA will be insusceptible against these attacks based on Table 2. In addition by adopting AES encryption over the communal XML encryption, CCA protects packets against SQL injection and "phishing".

V. CONCLUSION AND FUTURE WORK

In this study, behavioral biometrics, AES cryptography and One Round Zero Knowledge Protocol has successfully integrated in public cloud computing model. It is shown to be a unique authentication mechanism in providing a more accurate user authentication for it is not only relying on the user identity but also is attack proof. The main superiority aspect of CCA compared to the existing models is the coverage of the two levels of authentication together with robustness of the encryption algorithm.

There are still several areas that are not addressed in this paper, such as the interoperability of CCA as well as the compatibility of AES encryption. These areas can be ventured in further works of this research. The load balancing algorithms for CCA or CSP APIs in order to handle multiple users accessing the browser without jeopardizing the reliability and performance of the browser are the other future research direction in this line. The periodical ERD level authentication that is having access to the users EDR level throughout his activity and the connection to the hypervisor is determined by this monitored information could also be the other possible direction of work.

ACKNOWLEDGEMENT

This work is partially supported by grant GUP Tier-2, 2012-2013 with Vote No. 08J77 under Ministry of Higher Education (MoHE) and by MJIIT Research Grant of Universiti Teknologi Malaysia (UTM) Year 2012-2013 with Vote No. 4J044.

REFERENCES

[1] F.A. Alvi, B. C. (2013). A review on cloud computing security issues & challanges. International Journal of Cloud Computing and Services Science(IJ- CLOSER) , 2 (1).

[2] Doina Bein, W. B. (2009). The Impact of Cloud Computing on Web 2.0. Economy Informatics Journal , 9 (1), 5-12.

[3] Kuyoro S.O, I. F. (2011). Cloud Computing Security Issues and Challanges. International Journal of Computer Networks (IJCN) , 3 (5), 247-255.

[4] Madhan Kumar Srinivasan, K. S. (2012). State- of- the -art Cloud Computing Security Taxonomies- A classification of security challenges in the present cloud computing environment. International Conference on Advances in Computing, Communications and Informatics (ICAACI-2012) (pp. 470-476). Chennai: ACM.

[5] Swarnpreet Singh, R. B. (2012). Architecture of Mobile Application,Security Issues and services involved in Mobile Cloud Computing Environment. International Journal of Computer & Electronics Research , 1 (2), 58-67.

[6] Kevin Hamlen, M. K. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy , 4 (2), 39-51.

[7] Rohit Bhadauria, R. C. (2012). A Survey on Security Issues in Cloud Computing. International Journal of Computer Applications , 47 (18), 47-66.

[8] Allan A.Friedman, D. M. (2010, October). Privacy and Security in Cloud Computing. Issues in Technology Innovation , pp. 1-13.

[9] Jenson Meiko, J. S. (2009). On Technical Security Issues in Cloud Computing. International Conference on Cloud Computin. 2, pp. 109-116. IEEE.

[10] John C.Roberts II, W. A.-H. (2011). Who Can You Trust in the Cloud?A Review of Security Issues Within Cloud Computing. Information Security Curriculum Development Conference (pp. 15-19). Kennesaw, GA, USA: ACM.

[11] Soren Bleikertz, M. S. (2010). Security Audits of Multi- tier Virtual Infrastructures in Public Infrastructure Clouds. ACM , 93-102.

[12] Sven Bugiel, S. N.-R. (2011, October 17-21). AmazonIA:When Elasticity Snaps Back. (ACM, Ed.) ACM , 389- 400.

[13] W.Webb, K. (2004). Biometric Security Solution. In Biometrics for Network Security (p. 376). IEEE computer society.

[14] Wu, Z. (2008). Biometrics Authentication System on Open Network and Security Analysis. International Symposium on Electronic Commerce and Security.

[15] Westland, C. (2011). Electrodermal Response in Gaming. Journal of Computer Networks and Communication , 2011, 2-14.

[16] Yasuaki Ohtaki, A. S. (2009). Integration of Psycho- physiological and behavioural indicators with Ambulatory Tracking for Momentum Indoor Activity Assessment. ICROS-SICE International Joint Conference 2009. Fukuoka.

[17] Lalitha Bhavani Jivanadham et.al, "A Secured Dynamic Cluster-Based Wireless Sensor Network", Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN 2012), IEEE Thailand Section, July 2012, Phuket, Thailand.

[18] Lalitha Bhavani Jivanadham et.al, "Construction and Maintenance of a Secured Dynamic Cluster- Based Wireless Sensor" MJIIT-JUC Joint Symposium (MJJS 2012), November 2012, Kuala Lumpur, Malaysia