Journal of Engineering and Applied Sciences 13 (19): 8027-8033, 2018
ISSN: 1816-949X

Towards One-Time Biometric-Message Authentication Code in Cloud Computing

[1]Zainab Amin Abduljabbar, [2]Zaid Ameen Abduljabbar and [2]Rana Jassim Mohammed
[1]College of Science
[2]College for Pure Sciences, University of Basra, Basra, Iraq

Abstract: Cloud Computing (CC) security is a significant area of concern. Thus, far a number of authentication and integrity schemes have been proposed to recognize or protect any modification with exchanges of message between two smart devices users within a cloud environment. However, suggested schemes did not give off an impression of being adequately designed as a secure scheme to prevent common forms of attack. In the research we design a lightweight Message Authentication Code (MAC) in light of the characteristic of manually signature applying a local binary pattern in order to guarantee the trustworthiness of the IoT client's message. Characteristics are extricated from the client's biometric-signature to produce a message code for every client's login and to disallow malignant assaults, for example, forgery, replay and insider adversary. The scheme plot significant many security characteristics, for example, strong MAC anonymity, stage biometric-key management and agreement, a client's message integrity, a client's once biometric-key and once MACLESS code for every client's session. At long last, the security investigation and test comes about show and demonstrate the insusceptibility and proficiency of the research.

Key words: Cloud computing, characteristics extraction, manually signature, once biometric-key, once MAC, code

INTRODUCTION

In the present data age, transmitted data has profoundly developed and has been appropriated exponentially (TamilSelvan *et al*., 2009). CC is by and large viewed as the processing framework of the people to come it is a viable methods for empowering clients to use expansive volumes of assets and in addition to give an effective and promptly accessible on-request service (Dinh *et al*., 2013). However, cloud computing faces many challenges as seen in the IDCs statistics (Velte *et al*., 2009).

Its effective organization relies upon the presence of solid security systems. Because of the fundamental requirement for message security when two IoT clients are transmitting inside CC, proficient and strong programmed strategies are required to distinguish and approve the messages content. For instance, the assurance of messages against adversary and attacks, for example, replay, forgery and insider attack is a standout amongst the most vital security issues in fields, for example, CC and green computing. Nonetheless, the issues of message validation and authentication and integrity have been tended to as pressing issues and numerous accomplishments have been displayed by specialists as of late (Wegman and Carter, 1981; Xu *et al*., 2006; Zhao *et al*., 2008; Rabadi and Mahmud, 2008; Liu *et al*., 2011; Castiglione *et al*., 2014; Shen and Liu, 2014).

The best approach to preventing the manipulation of messages during transmission between two smart devices users is cryptography of one-way hash functions (Wegman and Carter, 1981; Xu *et al*., 2006; Zhao *et al*., 2008; Rabadi and Mahmud, 2008; Liu *et al*., 2011; Castiglione *et al*., 2014; Shen and Liu, 2014).

The aim of applying the MAC is to authenticate both the sender of a message and its integrity. Unfortunately, there are some problems related to MAC research can be shown more detailed in the related research. However, MAC has several disadvantages including the risk that an eavesdropper may discover that important sensitive data are being transmitted. An eavesdropper may use a cryptanalysis technique to extract the hashed key; clearly, many types of attacks can still occur when only MAC is used to secure data integrity (Liu *et al*., 2011). For this reason, the researchers (Liu *et al*., 2011) have integrated the MAC with the timestamp factor. This allows the hashed value to be changed once and every user's message to be used onetime.

This study focuses on overcoming all the aforementioned drawbacks by combining powerful assurance factors with MAC. In this way, a productive and secure scheme is intended to shield message from being controlled or altered amid transmission between clients in a cloud system over an unsecure channel. The procedure integrates a biometric mechanism that includes

Corresponding Author: Zainab Amin Abduljabbar, College of Science, University of Basra, Basra, Iraq

the utilization of the powerful features extricated by the Local Binary Pattern (LBP) after combining the handwritten signature of the sender, the handwritten signature of the receiver and the summation of a cryptographic hashed value called MACLESS. We prove that our proposed scheme keeps these properties based on the generation of once biometric-key management assumption and the anonymity bio-MAC with regard to messages in the interchange amongst sender client and receiver client.

The main contributions of our scheme to the cloud environment, message authentication and integrity are as follows. First, the research addresses every single past shortcoming and in this manner displays another hearty message verification and authentication technique that utilizes strong characteristics extraction from shared biometric manually written signature data and cryptography as a restricted and strong hash function to ensure a integrity and authentication message. That is this scheme provides end-to-end robust integrity during the transmission of message within a cloud environment. Second, in this scheme, mutual authentication between 2 parties is based on biometric-shared information from the combination of the handwritten signatures of the sender and receiver in a cloud environment. Thus, both parties (smart devices users) have a shared biometric reason to believe anything between them. Third, both service providers and smart devices users can achieve authenticated phase keys. The proposed research is exceptionally powerful against many assaults for example, replay assaults, insider assaults and reflection assaults. Fourth, the principle thought behind our effective research has been to locate the best decision of parameter incentive to diminish the computing cost of cloud audit services. Sixth it is important to point out that the iterative nature of the MAC computation (80 rounds) is designed to generate a once hashed value for each message to distinguish it from others, even the smallest variation has happened. So, the main aim of integrating MAC with other factors such as a biometric handwritten signature is to make the reverse computation much harder. Finally, a once bio-key is secretly and anonymously transmitted amongst the IoT sender and IoT beneficiary. Along these lines, getting the key is troublesome for attackers and this key ends up noticeably invalid when a client logs off the framework. The proposed scheme provides a robust approach for preventing the key from being envisaged by attackers.

Literature review: Various researchers have previously proposed different MAC schemes to provide authentication and integrity to transmitted messages or documents. The concept of message anonymity was presented by Rabadi and Mahmud (2008) who proposed a message authentication protocol using message authentication code from vehicle to vehicle to give obscurity and anonymity, authentication and integrity for a message uprightness. The idea of hash MAC obscurity relies upon a timestamp which is a once parameter used to produce a mysterious message. The researchers demonstrated that the execution time for message authentication code is not as much as that for a digital signature. Be that as it may, this method acquires extra expenses in light of the fact that additional equipment is required on every vehicle. This device should be tamper-resistant to save the ID and shared symmetric secret. Moreover, the security analysis of the proposed protocol was not discussed that is the research of the researchers was unclear regarding the capability of the proposed approach to reinforce authentication and maintain integrity against various attacks.

The current study presents a robust scheme to overcome the aforementioned problems via the cloud environment and digital signature biometrics. CSP and ECC are utilized to establish a robust and secure phase key agreement among users. Additionally, the configuration phase is used only once and then discarded. Therefore, time is limited.

A similar idea was exhibited 3 years ago by Liu *et al.* (2011) who proposed a hash-based secure interface between two elements over the web where in a once shared private key, a public one-way hash, a timestamp and a legitimacy period are used to produce once message obscurity. The shortcoming of their research is that the creators just quickly talked about security examination. The sorts of assault that this research can withstand us genuine so not elucidated.

The concept of integrating a smart card with a one-way hash function was presented by Zhao *et al.* (2008) who proposed the formation of a productive client to-client verification scheme in a shared situation. Despite utilizing an public key framework, the authors principally utilized a restricted hash and a smart card to build up a plan with solid security and insignificant computational cost. The disadvantage of this method is the many-sided quality of the gadget and the way that the extra card reader required will bring about additional expenses. Using smart cards, also, requires additional middleware applications to match a smart card with communication standards.

Xu *et al.* (2006) presented an efficient one-key Carter-Wegman MAC called one-key Galois MAC. This scheme employs a key and a universal hash function instead of the two keys used by Wegman and Carter

(1981). Meanwhile, the presented scheme in the currentsstudy is made more robust by embedding hand written signature features with a cryptographic one-way hash function to provide simplicity and security.

Another idea for a one-time key was introduced by Castiglione *et al*. (2014) who proposed a robust one-time authentication protocol, based on two cryptographically strong building blocks an authenticated key exchange and a keyed Hash Message Authentication Code (HMAC) between two endpoints. This enables transparent mutual authentication between two endpoints. Moreover, key setup, key scheduling and key update operations are accomplished independently by both endpoints. Therefore, this scheme suffers from drawback in the form of complexity in which more operations are required (key setup, key scheduling and key update).

MATERIALS AND METHODS

Perposed scheme: The common notations listed in Table 1 are utilized throughout this study. The proposed method is made out of two stages in particular, configuration and verification. The first one is performed just once; both S and R get biometric-shared manually signature (Prabhakar *et al*., 2003; Impedovo and Pirlo, 2008) and shared keys. Then, the last will be summoned each time a client wishes to send a validated and authenticated message to another client. In the configuration stage, the fundamental parts (the cloud service provider or CSP, the sender or S and the receiver or R) also, use ECC (Miller, 1986; Handschuh, 2011; Stallings, 2013) cryptographic hash function (.) (Miller, 1986) and symmetric key encryption/decryption Enc (.)/Dec (.). These parts can just run ECC when transmitting secure information among CSP, S and R over an entrusted channel. Along these lines, this operation is essential for the setup stage and not for the following ones. CSP isn't needed in the real execution-time. The accompanying advances are performed amid the configuration stage.

Configuration stage: S, R and CSP, utilizes ECC to produce private and public keys which will be utilized to secure handwritten signature transmittal from both S and R to CSP. Later, CSP sends the public key PU_{CSP} to both S and R in order to encrypt handwritten signatures of S and R (HS_s and HS_r, consecutively) and return them.

Upon receiving the encrypted HS_s and HS_r, CSP decrypts the received handwritten signatures using the private key PR_{CSP}, saves Hs_s and Hs_r and generates a biometric-shared handwritten signature by combining them ($SHS = HS_s \cup HS_r$) to get the Random features Vector RV = Fx (SHS) and the shared key Shk = Fx (SHS). Hence, FX denotes to a function which extracts features and employs an LBP filter to extract features from the normalized biometric-shared handwritten signature data. Afterward, CSP encrypts RV and Shk using PU_S and PU_R and transmits them to S and R, respectively. At long last, S and R decrypt they got Rv and Shk utilizing their private bio-keys (PR_S and PR_R, successively). After the configuration phase, S/R can use his/her random vector of features to generate a one-time key or an anonymous key, a summation of message authentication code (MACless). This process completes the verification phase as shown in Fig. 1.

Table 1: Notations used in the proposed scheme

Symbol	Definition
h(.)	One-way hash function
CSP	Cloud Service Provider
Enc (.)/Dec (.)	Encryption/Decryption function for symmetric key
S, R	Sender and Receiver smart devices users, respectively
PU_{CSP}, PR_{CSP}	Public and Private keys of the from ECC
PU_S, PR_S	Public and Private keys of from ECC
PU_R, PR_R	Public and Private keys of generates by ECC
HS_S, HS_r	Handwritten Signatures of S and R, consecutively
SHS	Biometric-Shared Handwritten Signature computation depend on the union of
FX	Function to extract a random feature vector of from a biometric-shared signature
RV	Random feature vector extracted from a biometric-shared handwritten signature by employing an LBP filter
Shk	Shared key
SK	Salt-Key computation based on the starting and end points from a random vector of features (Rv)
E, E', E''	Random number that denotes the end point from a Random Vector of features (RV) this number is used to generate a one-time salt-key
I_i, I_i', I_i''	Random number that denotes the starting point from a Random Vector of features (RV) this number is used to generate a one-time salt-key
M	Message to be authenticated
M'	S sends the summation of MAC (MACless) to R
M''	R re-computes the summation of MAC (MACless)
||	Concatenation function

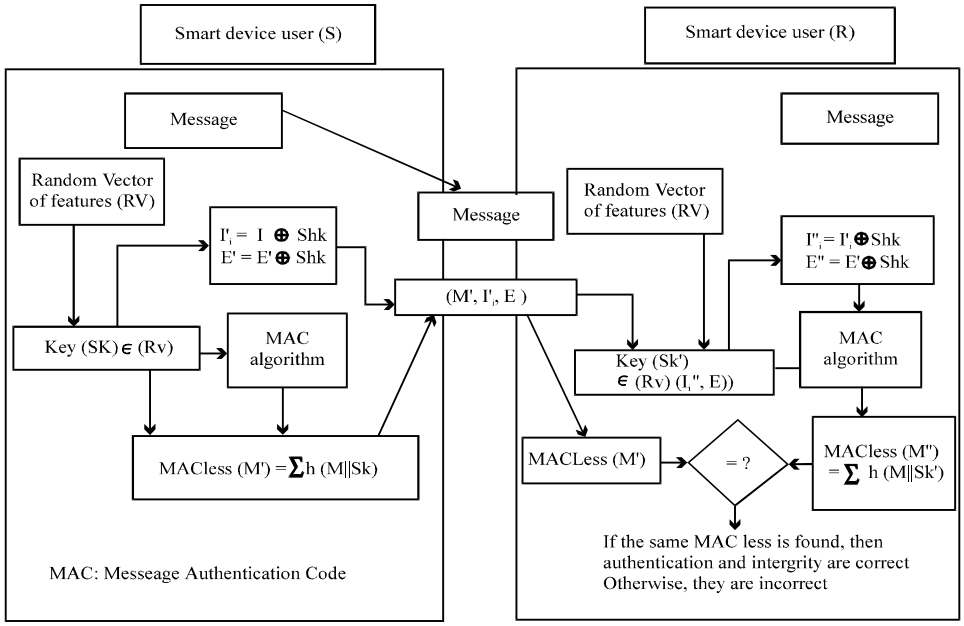

Fig.1: Diagram of the proposed scheme diagram

Verification phase: S→R: M, M', I_i, E'.S achieves the following steps:

- Assume that the message of the sender is M
- Generate a one-time Salt-Key (SK)∈(RV)→I_i, E where I_i and E are the starting and end points, respectively, from the random extracted vector features (Rv). I_i and E are randomly selected .The E parameter should not exceed the length of the feature vector which is 3060
- Compute MACless (M′) = ∑ h (M||Sk)
- Compute $I_i' = I_i \oplus Shk$
- Compute $E' = E \oplus Shk$
- Send message (M) and the parameters (M', I'_i, E') to R

R examines the message integrity using following steps:

- Compute $I_i'' = I_i' \oplus Shk$
- Compute $E'' = E' \oplus Shk$
- Regenerate Salt-key (Sk') ∈ (RV(I_i'', E'')) depending on the starting point (I_i'') and end point (E'') of the Random vector extracted features (Rv).
- Compute MACless (M'') = ∑h (M||Sk'). If M'' matches M', then R ensures the integrity of the message that S has submitted. Otherwise, the verification phase is terminated.

Security analysis: We contend that the research can resist many dangers to security, including replay, forgery, parallel session, MITM, insider, reflection, off-line guessing and DOS. The proposed research has various aspects and comprises of a once biometric key, once unknown and anonymous bio-MAC, one-time MACless anonymity and biometric key management. This scheme does not attract the attention of eaves droppers and thus provides biometric mutual authentication.

Table 2: Message anonymity explanation

Variables	Message explanation
Basrah	d40b5b2fa21148a563a464d8c1fcdd4f53e55430
Basrah	dbec4b6f4ea02b382bf0ec2bc331540a038daca9
Basrah	c7b52b7f7b2d53a0d9a828f7f2a498ca738e77e8
Basrah	182b7fb419e6ee4e7f09d996e33424157c3d99a6
Basrah	f10ff6139995d067489df0ccbddf0c7033afa858

Theorem 1: Our scheme plan can give vigorous client message secrecy and anonymity.

Proof. Assume that S/R attempts to resend a similar message. On the off chance that an attacker endeavors to listen in on the sign-in demand of the S (M, M', I'i, E') at that point the attacker can't utilize the same MAC ((M') = h(M||Sk)) utilized by S on the grounds that the S creates just a once MAC for every S ask for (SK).Thus, SK extracts a feature vector by combining the handwritten signatures of R and S (RV = Fx (SHS)); (SK)∈(RV)→I_i, E; (SHS = $HS_s \cup HS_r$). Both I_i and E are selected randomly.

Likewise, the eavesdropper does not have the primary biometric-key and parameters (SHS, I_i and E) to process the one-way hash function M'. Subsequently, disclosing the MAC of S is difficult for an eavesdropper. The proposed scheme can obviously support the anonymity of user message (Table 2).

Theorem 2: The proposed scheme can provide a biometric MAC.

Proof: The biometric operator identifies a person based on particular physiological features such as his/her handwritten signature. A handwritten signature is one of the most commonly used security measures in biometric topics it has ability to resist familiar adversary and attacks. During the configuration stage, both S and R transmit their Handwritten Signatures (HS_S and HS_r) to CSP through a secure transmittal using applied ECC. Afterward, CSP saves HS_S and Hs_r, generates biometric-shared Handwritten Signatures ($SHS = HS_s \cup HS_r$) and extracts a vector of features (RV = FX (SHS)). RV is then sent to both S and R. During the verification phase, S or R should generate a biometric-MAC ($M^{'}$) = h (M||Sk) based on Salt-Key $(SK) \in (RV) \neg I_i$, E whenever S and R intend to transmit a message on each other. Our method can unmistakably bolster biometric MAC.

Theorem 3: Our scheme can provide biometric key management.

Proof: In our research, S utilizes a secret Salt-Key [$(Sk) \in (RV) \neg I_i$, E); (RV = Fx (SHS)); ($SHS = HS_s \cup HS_r$)] to compute ($M^{'}$) = h(M||Sk) when S transmits M to receive r (R) or vice versa. In addition, the mechanism for computing Sk is based on (I_i, E) where I_i is the starting point of the feature extraction from the user signature and E is the endpoint of the extracted features. Both I_i, E are selected randomly. Subsequently, an attacker can't get to the session biometric-keys and can't get the primary parameters and bio-keys (SK, SHS) that are created amid the configuration stage through CSP. SK depends on the extracted features of the combined biometric-shared image of the handwritten signatures of S and R ($SHS = HS_s \cup HS_r$) and the one-time random positions generated by S (I_i, E) during the verification phase. Thus, the research bolsters bio-keys management.

Theorem 4: The research can keep a replay attack.

Proof: An attacker plays out a replay assault by listening stealthily at the sign-in message which is sent by the legitimate smart device S-R. After the trade amongst S and R, the assailant reuses this message to mimic the substantial client when he/she logs off the framework. In the research, the sign in demand of each new sender ought to be indistinguishable with the CSP keys RV, Shk, SHS, HS_s and HS_r. Along these lines an assailant can't pass any replayed message for the check of R. Therefore, the assailant neglects to play out this kind of assault in light of the fact that our work has redirected it.

Theorem 5: The research is unacceptable to be focused by DOS attack.

Proof: This attack for the most part endeavors to briefly or inconclusively counteract or hinder administrations of correspondence offices and assets. For this situation, the authentication framework enables a rightful client to change his or her secret key. Such method is appropriate to be focused by a DOS assault. In the research, the once bio-key (key refresh) $(SK) \in (RV) \neg I_i$, E is processed freely amongst S and R and does not need any fascination between them. Likewise, our scheme does not utilize a central part. However in the configuration phase; it uses CSP only once and then later discards it. The present scheme works with endpoint-to-endpoint method. Thus, the research is hard to be targeted by DOS attacks.

Theorem 6: The research can resist parallel-session and attacks.

Proof: Such type of attack, the adversary attempts to personate a legitimate client by creating a valid log-in message by accessing a valid session message. In the proposed scheme if an attacker attempts to impersonate, then he/she can access a valid session message (M, $M^{'}$, $I^{'}_i$, $E^{'}$) utilizing the secret parameters RV, SK, Shk, I_i and E. The attacker does not have any information on RV, Shk, SHS, HS_s and HS_r to compute ($M^{'}$, $I^{'}$, $_i E^{'}$) and impersonate the valid user S/R. Finally, the attacker will neglect to fashion a legitimate session message. Hence, he/she ca't play out a fraud attack. Our work can keep a fraud attack.

RESULTS AND DISCUSSION

To assess the proficiency and exactness of the research, we have executed many analyses. Initially Fig. 2 demonstrates the run-time of the verification stage. The average time for the verification period of the research is equivalent to 0.026 sec for every client who indicates the exceeding expectations arrangement of our scheme. This average time has been gotten from 500 keeps running of our scheme with each run comprising of 10000 clients. Besides, concerning framework proficiency, we think about the exactness of our work. In down to earth terms, Fig. 3 demonstrates that we get 100% precise outcomes from 10,000 clients in our analysis. For more noteworthy perceive ability, we utilize 5,000 clients in Fig. 2 and 3.

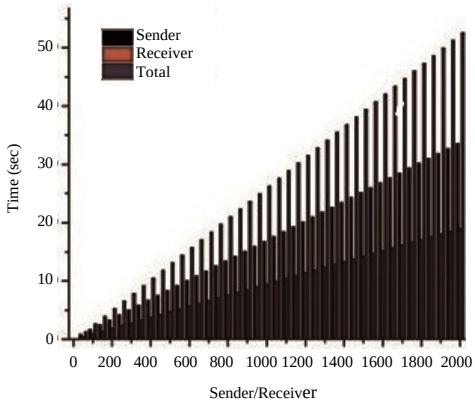

Fig. 2: The performance of our proposed scheme

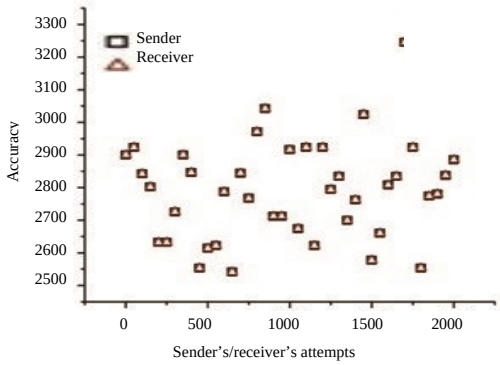

Fig. 3: shows the accuracy result of our proposed scheme

CONCLUSION

This study includes a literature review of the strengths and weaknesses of data integrity and authentication in recent years. It presents new and efficient MACless anonymity among smart devices users in a cloud computing environment. A robust method was developed by extracting handwritten signature features to generate a symmetric one-time biometric key.

The research expects to give extra parts and counteract known attacks to ensure message. The generous favorable circumstances are as per the following. Initial, an attacker may neglect to acquire the keys considering that they rely upon written by hand signature feature extraction. Second, an attacker may not acquire the biometric-shared data, since, it relies upon the joined manually written signatures of both the sender and receiver and is ensured by ECC in the configuration stage. Third, a once bio-key that prompts once message obscurity and anonymity is given. Fourth, the hashed value is encoded into a new form called MACless where in MAC is reduced and modulated to 4 bytes by summing it. Overall, the scheme is efficient and sufficiently secure to provide a good starting point for the maintenance of message between users in mobile cloud computing.

REFERENCES

Castiglione, A., A. De Santis, A. Castiglione and F. Palmieri, 2014. An efficient and transparent one-time authentication protocol with non-interactive key scheduling and update. Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA'14), May 13-16, 2014, IEEE, Victoria, British Columbia Canada, ISBN:978-1-4799-3629-8, pp: 351-358.

Dinh, H.T., C. Lee, D. Niyato and P. Wang, 2013. A survey of mobile cloud computing: architecture, applications and approaches. Wirel. Commun. Mob. Comput., 13: 1587-1611.

Handschuh, H., 2011. Sha-0, Sha-1, Sha-2 (Secure Hash Algorithm). In: Encyclopedia of Cryptography and Security, Tilborg, H.C.A.V. and S. Jajodia (Eds.). Springer, Boston, Massachusetts, ISBN:978-1-4419-5905-8, pp: 1190-1193.

Impedovo, D. and G. Pirlo, 2008. Automatic signature verification: The state of the art. IEEE. Trans. Syst. Man Cybern. Part C. Appl. Rev., 38: 609-635.

Liu, Z., H.S. Lallie, L. Liu, Y. Zhan and K. Wu, 2011. A hash-based secure interface on plain connection. Proceedings of the 6th International ICST Conference on Communications and Networking in China (CHINACOM'11), August 17-19, 2011, IEEE, Harbin, China, ISBN:978-1-4577-0100-9, pp: 1236-1239.

Miller, V.S., 1986. Advances in Cryptology-CRYPTO'85 Proceedings. Springer, Berlin, Germany,.

Prabhakar, S., S. Pankanti and A.K. Jain, 2003. Biometric recognition: Security and privacy concerns. IEEE Secur. Priv., 1: 33-42.

Rabadi, N.M. and S.M. Mahmud, 2008. Drivers anonymity with a short message length for vehicle-to-vehicle communications network. Proceedings of the 5th IEEE Conference on Consumer Communications and Networking (CCNC'08), January10-12, 2008, IEEE, Las Vegas, Nevada, ISBN:978-1-4244-1456-7, pp: 132-133.

Shen, J.J. and K.T. Liu, 2014. A novel approach by applying image authentication technique on a digital document. Proceedings of the 2014 International Symposium on Computer, Consumer and Control (IS3C'14), June 10-12, 2014, IEEE, Taichung, Taiwan, ISBN:978-1-4799-5277-9, pp: 119-122.

Stallings, W., 2013. Digital signature algorithms. Cryptologia, 37: 311-327.

TamilSelvan, R., I. Prathap, A. Ramalingam and S. Raghavan, 2009. A novel approach to watermark text documents based on Eigen values. Proceedings of the 2009 International Conference on Network and Service Security (N2S'09), June 24-26, 2009, IEEE, Paris, France, ISBN:978-2-9532-4431-1, pp: 1-5.

Velte, T., A. Velte and R. Elsenpeter, 2009. Cloud Computing: A Practical Approach. McGraw-Hill, New York, USA.,.

Wegman, M. and J. Carter, 1981. New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci., 22: 265-279.

Xu, J., D. Wang, D. Lin and W. Wu, 2006. An efficient one-key carter-wegman message authentication code. Proceedings of the 2006 International Conference on Computational Intelligence and Security Vol. 2, November 3-6, 2006, IEEE, Guangzhou, China, ISBN:1-4244-0604-8, pp: 1331-1334.

Zhao, Z.M., Y.F. Liu, H. Li and Y.X. Yang, 2008. An efficient user-to-user authentication scheme in peer-to-peer system. Proceedings of the 1st International Conference on Intelligent Networks and Intelligent Systems (ICINIS'08), November 1-3, 2008, IEEE, Wuhan, China, ISBN:978-0-7695-3391-9, pp: 263-266.