Journal of Theoretical and Applied Information Technology
31st May 2018. Vol.96. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TOWARD FOR STRONG AUTHENTICATION CODE IN CLOUD OF INTERNET OF THINGS BASED ON DWT AND STEGANOGRAPHY

[1]ALI A. YASSIN , [2]ABDULLAH MOHAMMED RASHID , [1]ZAID AMEEN ABDULJABBAR , [1]HAMID ALI ABED ALASADI , [1]ABDULLA J. Y. ALDARWISH
1Computer Science Dept., Education College for Pure Science, Basra University/Iraq,
[2]Computer Science , Education College for Human Science, Basra University/Iraq,

ali.yassin@uobasrah.edu.iq , Abdullah.rashid@uobasrah.edu.iq , abdalla_rshd@yahoo.com

* Correspondence: AliAdel79yassin@gmail.com Tel.: +9647717542311

ABSTRACT

Now days, with the remarkable fast development of micro processing devices and communicating technologies, networks, computers, mobile devices and Internet have become very unavoidable, as a result led to the emergence and prevalence of the Internet of Things (IoT). The mobility devices in IoT have entered in all areas of life ranging from a smart home down to a smart city. Due to big storage systems are extremely needed for securing data in flexible processing. Especially, the two or more entities wish to exchange data in IoT. In this paper, we propose secure and scalable scheme to keep data against attacks during a communication channel in IoT environment when IoT's components want to exchange their data. This scheme work based on crypto hash function, and Discrete Wavelet Transform (DWT) that apply on sender's/receiver's message. Our proposed scheme distinguishes a good of security, scalability, and reliability in entities' data via IoT. Additionally, our work includes numerous security features like one time message code for each user's login request, user's message integrity, user's message anonymity, and session key agreement. Empirical results have explained the potential and profits of the proposed scheme as well as significant gains in performance.
Keywords: *IoT, MAC, Key Management, Inside Attack.*

1- INTRODUCTION

In information technology world today, the improvement of multicore processors leads to a significant increase in the amount of computational power on a single device.. In parallel and distributed system, the advancement of networking technologies has funded with the fast enlargement of web skills and service providers. Now, ‘‘Big Data’’ is a term for huge and budding sets of data. ‘‘How fast it is budding’’ and ‘‘how difficult it is’’ are the key anxieties. Project companies see that the data in their place is an excellent foundation of insights [1]. Due to a relatively current event of an upsurge in data exchanged among nodes in devices (computer, laptop, mobile, etc.) in the Internet of Things (IoT), exchanging data between two or more devices in IoT are also often needed for secured Big Data [2]. IoT refers a modern era of computing whereby every conceivable object is prepared with a smart device permitting data collection and communication via the Internet. The main challenges of IoT represented in the security in terms of the group and use of individuals’ special data. Continuously, the security of exchanging data in the IoT's environment and how to keep this data from adversaries is very important demand.

Obviously, the message that generated from a legal user is known as User Authentication and is supported by Message Authentication code (MAC) for ensuring from the integrity and authenticity of received message. MAC functions require possessing several security tools such as SHA-1.

For more security, a MAC function should be having ability to withstand famous malicious attacks like forgery and insider attacks. As a result, even if an adversary can be achieved an oracle which holds the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

shared key and produces MACs for messages of an adversary's selecting; an adversary cannot guess MAC for other messages without execution infeasible amounts of computation. The main components (sender and receiver) of MAC values are used the same secret key. This means that the components of a message should be agreed on the same key in the setup phase, as is the state with symmetric encryption. Additionally, any user has ability to verify a MAC is also capable of producing MACs for other messages [4, 5].

Constantly, MACs are very sensitive to any modification of the message. If one or more bits of user's message update, MAC changes about 50 percent of their bits and cause to be the message impractical. Furthermore, the successful verification of MACs demands equivalence of all of bits of the received sender's MAC with calculated receiver's MAC. Such a hard condition for the successful verification of messages protected by MACs is not suitable for some applications. There are numerous schemes in this topic that endured from various drawbacks such as reflection attacks, insider attacks, replay attacks, and guesting secret key between the sender and receiver [5-7].

In this paper, we propose a good message authentication scheme for IoT based cloud environment that divides into two phases—setup and verification. Furthermore, our proposed scheme enables authentication and integrity protection of messages exchanged over a secure communication channel between entities that based on shared secret key and steganography. Where, the sender and receiver have been agreed to the shared secret key at setup phase. The construction of our proposed scheme enables a sender to encode any message as a first step while the second step hides this code inside image based on discrete wavelet transformation. In the other side, the receiver has ability to detect the validity of sender's MAC that he uses the same secret keys to complete the integrity of message at verification phase. Additionally, we also present a regular procedure with reverence to probabilistic queries and orderly verification to reduce the cost of auditing through verification phase.

The motivation and contributions of our proposed scheme as follows: (1) we present an effective scheme to reduce the computational cost of cloud audit services by selecting the best parameters between components; (2) our work does not need high cost, easy of compatibility with available infrastructure, and simple to manage and deploy; (3) our scheme has ability to withstand several malicious attacks such as reflection attacks, forgery attacks, replay attacks, Man-In-The-Middle attacks, parallel-session attacks, and insider attacks; (4) cloud service provider and legal user can fulfill valid session keys; (5) our proposed scheme provides one time message code for each user's login request, user's message integrity, user's message anonymity, and session key agreement; (6) the proposed work aims to achieve a high balance between the complexity of security and high performance.

Our work has distinctive properties as follows: (1) we present an effective scheme to reduce the computational cost of cloud audit services by selecting the best parameters between components; (2) it does not need high cost, easy of compatibility with available infrastructure, and simple to manage and deploy; (3) Our scheme has ability to withstand several malicious attacks such as reflection attacks, forgery attacks, replay attacks, Man-In-The-Middle attacks, parallel-session attacks, and insider attacks; (4) cloud service provider and legal user can fulfill valid session keys.

The organization of this paper is arranged as follows. The important tools of our scheme are existed in Section 2. Sequentially, a review of previous works is presented in Section 3. Section 4 displays the proposed scheme. We present the security analysis and experimental results in Section 5, and Section 6 refers to conclusion of this paper.

2. BASIC TOOLS

For more details, we view briefly some of the cryptographic tools which are used during our work.

2.1 Hash Functions

The hash function considers a one way encryption, it is a well-defined mathematical method that consists of a set of bits which is produced from a large size file, the result of hash function can be knew hashes. Using cryptographic hash functions in the message authentication code has become a standard scheme in several applications, particularly in the internet security procedures. Both of authentication and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

integrity considered as major issues in the information security; where the hash code can be added to the message. After that, at any time the authenticated users have ability to check the verification and integrity of the receiving messages. Then, users compute hash function on these message and compare the result with the senders' hash-codes, if so, that is mean the message derived from the sender without changing because if there is any altered has been added to the data will lead to change the hash code at the receiver side[5, 8].

2.2 Discrete Wavelet Transform (DWT)

Wavelet transform Is a useful computational tool for various images, signal processing uses, and video processing . The result of applying DWT on digital image which is decomposed into four levels as follows: (1) low-frequency approximation level; (2) low-frequency horizontal level; (3) low frequency vertical level; (4) high-frequency diagonal level. When applied it on digital image, the distribution of data based on the degree of significance. As a result, the data region is existed in the first level (approximation level) which named the low- low (LL) sub-band; It is the important data area. The remaining areas are called as the detail. The present levels are as follows: low-low (LL), high-low (HL), low- high (LH), and high-high (HH). These levels are identified as DWT [9].

2.3 Problem Definitions

Least significant bit (LSB) considers one of the most famous methods used is to hide data. In general, there are many hurdles associated with this method. It is very subtle to any type of filtering or processing of the hidden image. Rotation, scaling, removing, cropping, updating, insertion of noise, or loss compression to the hidden image will abolish the message. Alternatively, for the hiding ability, the information size to be hidden comparatively determines on the size of the cover-image. The message size should be smaller than the input image (cover image). A large ability permits the use of the smaller input image for the message of fixed size, and thus reductions the bandwidth needed to transfer the hidden image [6, 10]. Additionally, there is weakness based on an adversary that can easily damage the message by eliminating or zeroing the complete LSB plane with very little modification in the cognitive value of the updated hidden image. Consequently, if this scheme causes someone to doubtful something embedded in the hidden image, and then leads that this scheme is not effective and cannot be relied upon in modern applications.

Our work focuses on overcoming the aforementioned problems based on discrete wavelet transform. Thus, we design an efficient and secure scheme to transfer message securely between two or more entities in IoT. In the setup phase, both of sender and receiver aggress with secure key SK. In the verification phase, the sender converts his message (msg) from plain text to mac base on crypto-hash function MD5 and secret key. Then, he divides his msg in to four parts. After that, sender applies DWT on image and hides each part in the four layer's image that has been produced from DWT for increasing the security and conquers all above drawbacks of LSB's scheme. Furthermore, he converts his image from wavelet domain to special domain by using inverse discrete wavelet transformation (Covimage). Then, sender sends Covimage and mac to the receiver. Upon receiving the sender's message (cover-image, mac) by receiver, he retrieves message msg that embedded inside Covimage. Then, he computes mac′ by using hash function and secret key. Then, he mac′ with mac′. If so, receiver verifies the sender's message. Otherwise, he detects the illegal message. Figure 1 explains the methodology of our proposed scheme.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

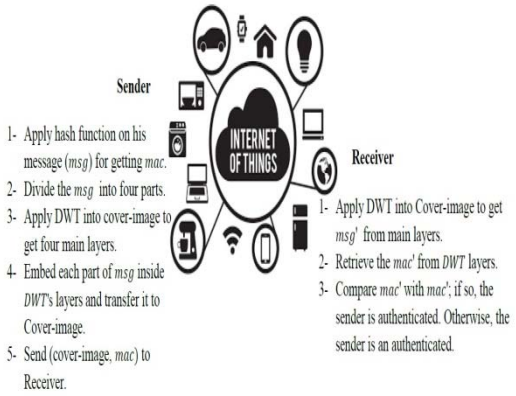


Figure 1. The Verification Phase Of Our Proposed Scheme

3. RELATED WORK

Recently, there are many authors that have proposed different authentication, authorization, and data integrity schemes based on cryptographic hash function (one way function) to produce a sturdy hashed value and exchanged it securely through communication channels. Jain et al. [10] proposed an adjusted least significant bit spatial domain embedding scheme. This scheme splits an image pixels ranges (0-255) and generates key which is called a stego-key. This key consists of five gray-level ranges of image and each range refers to update fixed number of bits to add in least significant bits of image. The restriction of their scheme is to hide extra bits of signature with hidden message for its integrity aim. Additionally, their scheme focus on the blue channel in color image to hide information.

In [11] authors have introduced an adaptive LSB substitution depended on data hiding scheme for input image. To perform improved visual quality of hidden image it takes care of noise sensitive area for embedding. This scheme focus to analyze the brightness, darkness , edges, and texture masking of the high at non-importance area of image and Leading to isolate and identify of sensitive areas in color image that called r's region. The LSB's (r) for embedding is calculated by the high-ranking bits of the image. Additionally, it also uses the pixel adjustment scheme for enhanced hidden image visual quality through LSB substitution scheme. The experiential results view a good ability to hide information., but dataset for results are restricted; There are no images that do not contain many edges with noise such as 'Baboon.tif'.

Fridrich and Goljan [12] proposed a scheme for self-embedding an image as a way of keeping the main elements of image against operations such as cropped, or updated, rotation which affect the retrieval of data from the hidden image. The major principle of this scheme is to embed a compressed version of the image inside the LSB of image's pixels. The main drawback of this scheme by mechanism of embedding information which shows the affected of data retrieved from the hidden image.

In [13] Ashwin Swaminathan et al. have enhanced an algorithm for creating hashed image, applying Fourier-Mellin transform characteristics which are fixed by two-dimensional affine transformations. The method also contains key-dependent randomization into the Fourier-Mellin transform constructions a secure and robust hashed image.

In 2008, Rabadi and Mahmud [14] presented the understandable of message anonymity. This scheme, the message authentication protocol usages message authentication code (MAC) from vehicle to vehicle to support authenticity, anonymity, and message integrity. The perception of MAC anonymity relies on a timestamp, which is a one-time factor to produce an anonymous message. Conversely, this scheme entailed extra costs because an additional hardware device to save the ID and shared symmetric secret was needed on each vehicle. Besides, the security analysis of the presented scheme was not discussed. Later in 2010, Jamil and Aziz [15] presented the idea of permutation key to the transformed image. The authors proposed a secure hashing scheme between two components to overcome the issue of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security over communication. They used a permutation key for each block of the separated image to make the hashed value much harder to be guessed by an adversary. The shortcomings of this scheme is that the permutation key is calculated based on feature extraction to produce hashed image. Thus, an adversary might identify this and recalculated the permutation key to redevelop the hashed value. In 2011, the idea of message anonymity has resumed again by Liu et al. [16], they recommended a hash-based secure interface between two components over the Internet. A one-time shared private key, a timestamp, a public hash function, and a validity period were exploited to generate one-time message anonymity. On an ongoing basis, Naqvi and Akram [17] proposed an idea of increasing the sturdiness of the key based hash message authentication code (HMAC-MD5). They presented to apply MD6 compression function to produce a strong key to compute HMAC. The key was made based on MD6 maintained randomization and was hard for adversaries to guess. Nevertheless, the security analysis of their scheme was not discussed extensively and was restricted to birthday and detailed key search attacks.

In 2015, Zaid et al. [18] presented a good scheme depended on biometric key, discrete wavelet transformation, and crpto-hash function. In their work, the authentication code is hidden in the image document and then uses it in verification phase to ensure from validity of legal user and integrity of data in the same time .

Freshly, Castiglione et al. [19] suggested a good authentication approach between two entities based on crypto hash function HMAC-SHA-512 and an authenticated key exchange. These authors allege that their proposed scheme is well-organized; however, the computational cost of HMAC considers very high. Consequently, we prove this scheme is not efficient in terms of performance, as discussed in Table 1 and Section 4.

In this paper, we propose a robust message authentication scheme based on cryptographic tool, DWT, and simple steganography (LSB) in the environment of internet of things. Our proposed scheme is supplied by a strong security aspect, can resist well-known attacks, and works a good performance compared with the MACs' schemes. Our proposed scheme based on data hiding technique of image is proposed. This scheme is embedded the bits of message based on discrete wavelet transformation to conquer all drawbacks of LSB's scheme. Moreover, our scheme comprises several security features such as user's message anonymity, session key agreement, data integrity and authority for user's message, and once message code for each user's login request. The investigational results show the efficiency, flexibility, and hardiness of our proposed scheme. Furthermore, the proposed scheme has novelty and distinguished from the previous works because it relies on hiding the text message in the image after it is folded into four parts by using DWT. Then, a key is used to generate a one-time message that is already agreed between parties in the setup phase. Our proposed work balances the complexity of security and high performance. Finally, the comparisons security a property is explained in Table 1 between our proposed scheme and related authentication schemes.

Table 1. Comparison With Related Works

Feature	Proposed Scheme	[14]	[15]	[16]	[17]	[18]	[19]	[20]
C1	Yes	No	Yes	No	No	Yes	Yes	No
C2	Yes	Yes	Yes	No	No	Yes	No	No
C3	Yes	Yes	No	No	No	Yes	Yes	Yes
C4	Yes	No	No	No	No	Yes	Yes	Yes
C5	Yes	No	No	No	No	No	No	No
C6	Yes	No	No	No	Yes	Yes	No	No
C7	Yes	No	No	No	No	Yes	No	No
C1: One-time key; C2: One-time key; C3: Key agreement; C4: Secure channel; C5: Cloud & IoT environment; C6: Using authentication code with steganography; C7:Using DWT								

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

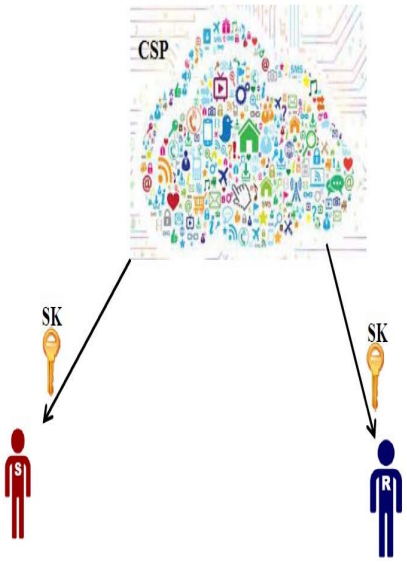


Figure 2. Setup Phase Of The Proposed Scheme

3. Our Proposed Scheme

In this section, we propose a good message authentication code scheme for IoT's environment. The following symbolizations in Table 2 will be used during our scheme.

Our scheme consists of three main parts, Cloud Service Provider (CSP), Sender side (S), and Receiver side (R) in IoT's environment. Our work divides into two phases— Setup and Verification. Setup phase is executed only once while the verification phase is implemented whenever a sender/receiver wants to submitted his message.

In the setup phase, both of sender and receiver register in CSP that supports theme by secret-shared key SK (see Figure 2). The central elements $(\mathrm{CSP}, \mathrm{Sender}, \mathrm{Reciver})$ also practices a cryptographic hash functionh(.), symmetric key, CSP sets up $n = p * q$; where both p and q are two large primes and secret key is $SK \in Z_n$. The both sender (S) and receiver (R) register their identities to the CSP over a secure channel.

In the verification phase, the sender wants to send his message to receiver. He computes the following steps (see Figure 3):

1- He converts his message (msg) from plain text to mac base on crypto-hash function MD5; where $\mathrm{mac} = \mathrm{h}(\mathrm{msg} \parallel \mathrm{SK})$. So, SK is used for generating one time hash message to prevent sniffing and Man-In-The-Middle (MITM) attacks (see Table 3).

2- After that, he computes a new secret key $SK = SK \oplus \sum_{i=1}^{n} \mathrm{Ascii}(\mathrm{mac})$; where n represents the length of mac's string. This step considers one of the advantages of proposed scheme for computing a new key for each verification phase (see Table 2).

3- He selects his image (img) and applies DWT , and divides his msg in to four parts and hides each part of message text in the four layer images that have been produced from DWT for increase the security. Also, this step considers very important to conquer all drawbacks of LSB's scheme. Continuously, he transforms img from wavelet domain to special domain for producing cover-image (Covimg) based on inverse discrete wavelet transform (IDWT).

4- Then, sender sends $(\mathrm{Covimg}, \mathrm{mac})$ to the receiver.

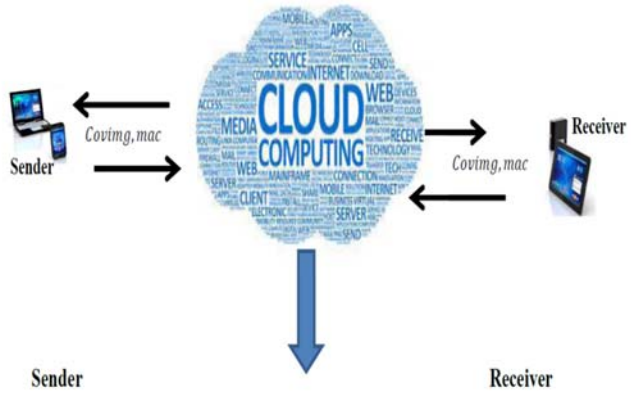
5- Upon receiving the sender's message $(\mathrm{Covimg}, \mathrm{mac})$ by receiver, he retrieves sender's message (msg') that embedded inside Covimg. Then, he computes mac' by applying crypto hash function $\mathrm{mac}' = \mathrm{h}(\mathrm{msg} \parallel \mathrm{SK})$. Then, compares mac' with mac. If so, receiver verifies the sender's message and computes a new secret key $= SK \oplus \sum_{i=1}^{n} \mathrm{Ascii}(\mathrm{mac}')$. Otherwise, he detects the illegal message from an authenticated user. Figure 3 explains the methodology of our proposed scheme in verification phase.

Table 2. Symbolizations Of Our Proposed Scheme

Symbol	Definition
h(.)	A cryptographic hash function.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CSP	Cloud Service Provider.
SK	Secret shared key.
msg	Sender's message.
mac	Message authentication code of sender.
DWT	Discrete Wavelet Transformation.
IDWT	Inverse Discrete Wavelet Transformation.
img	Sender's original image.
Covimg	Steganography image.
Ascii	ASCII function.
mac'	Message authentication code of Receiver.
msg′	Receiver's message.



Sender **Receiver**

1- Divide msg into four parts (p_1, p_2, p_3, p_4).
2- Convert img into (LL, HL, LH, HH).
3- Compute $mac = h(msg, SK)$ and $SK = SK \oplus \sum_{i=1}^{n} Ascii(mac)$.
4- Embed p_1, p_2, p_3, p_4 inside (LL, HL, LH, HH), respectively.
5- Generate $Covimg$.
6- Send $Covimg, mac$.

$Covimg, mac$ →

1- Retrieve msg' from $Covimg$.
2- Compute $mac' = h(msg, SK)$.
3- Compares mac' with mac. If so, receiver verifies the sender's message.
4- Compute $SK = SK \oplus \sum_{i=1}^{n} Ascii(mac)$.

Figure 3. Verification Phase Of Our Proposed Scheme

Table 3: Explain One Time Mac For Each Verification Phase And Mechanism Of Generating SK

	Message	Message Authentication Code	Ascii Code	SK
1	Basra	9c59b55a530e18407064e7749fb5329895353997	4231	2341
2	Basra	AB9b56trDUe18407064e7749fKL988765fdgfj7	5821	6781
3	Basra	Ty676883297890ftfhvbghjfdfdjl4556ewsfvn345	9102	9021

4. EXPERIMENTAL RESULTS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In this section, we support the security analysis of our proposed scheme and performance investigation.

4.1 Security Analysis

We demonstrate that our scheme can resist many malicious attacks such as insider attack, reflection attack, replay attack, forgery attack, MITM attack, and provides several merits such as once anonymous message code and session key agreement.

Theorem 1. Our scheme can provide known-key security.

Proof. When the sender wants to send message (msg) to the receiver, he generates a new key SK that used once time for each verification phase based on the following equation 1:

$$SK = SK \oplus \sum_{i=1}^{n} Ascii(mac) \dots (1)$$

By the way, in the receiver side the event has been repeated when the receiver checks the verification of sender's message and computes a new shared key that he uses to send message to sender or verification a new sender's message. So, the receiver based on the equation2 as follows:

$$SK = SK \oplus \sum_{i=1}^{n} Ascii(mac') \dots (2)$$

So, an attacker fails to achieve the new session key.

Theorem 2. Our proposed scheme can provide strong user message anonymity.

Proof. Assuming one of the main entities in IoT's environment (sender/receiver) tries to resend the same message which has been sent previously, if an attacker tries to listen on the sender's/ receiver's request $(Covimg, mac)$ during login phase, he fails to apply the same sender's login request $mac = h(msg, SK)$ because the sender disables his login requesting when he logout the system based on equation 1. Also, an attacker cannot access to the key SK for computing the message authentication code mac'. Therefore, there are many difficulties faced an attacker to reveal the sender's message authentication code. Evidently, our proposed scheme can provide users' message anonymity.

Theorem 3. Our scheme can prevent a replay attack.

Proof. An attacker executes a replay attack by snooping the login message which sent by a legal sender to the receiver. At that time, an attacker try to use sender's message to impersonate the valid sender/ receiver when he login out of the system. In our work, each a new sender's/ receiver's requesting should be matching with $CSP's$ key (SK) . Consequently, an attacker fails to authorization any replayed message to the $reciever's$ verification. Besides, our work can resist this attack without having to rely on synchronization clocks. So, our scheme depends on generated once shared key SK instead of timestamp and the secret parameters (mac/mac') are used once for each sender's/receiver's login message request. Therefore, an attacker fails to use this type of attack.

Theorem 4. Our scheme can resist the forgery attack and parallel-session attack.

Proof. If any attacker attempts to impersonate legal user, he should be retrieved user's session message $(msg, mac , covimg)$ by using secret shared key (SK). An attacker does not possess any idea about (Sk) to compute (mac/mac', covimg). Thus, our proposed scheme prevents the forgery attack.

Theorem 5. Our scheme can resist an insider attack.

Proof. In the proposed scheme, when any user wants to register with CSP for remote-access services, he needs to send his identities information to CSP. Due to the utilization of secret key (SK) and crypto-hash function h, they are represented basically impossible for CSP to obtain the user's msg from the cover image (covimg). Furthermore, the main values $(mac/mac', covimg, SK)$ are produced once time for each user's login request. Obviously, our scheme can preclude the insider attack and Cloud service provider impersonation attack.

Theorem 6. An attacker fails to use a reflection and MITM attacks.

Proof. This type of attack is occur, when a legal user (sender/receiver) sends his login message to the authenticated receiver, an attacker attempts to catch user's message and submits it back to the same sender in IoT's environment. In the proposed work, an attacker fails to fraud the sender/receiver since he cannot

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

use the main values (mac/mac', covimg) that sent from the sender to the receiver vice versa. An adversary fails to use these values again because generate once time for each sender's/ receiver's login request. Hence, our proposed scheme avoids MITM and reflection attack.

Theorem 7. Our scheme can provide integrity of sender's/receiver's message.

Proof. Assuming, if an adversary attempts to extract/ change the message (msg) that has been embedded inside image (Covimg) and then he sends it again to receiver. An adversary fails to apply his attack because the receivers will check the integrity of sender's message by computing (mac′) and compare with mac; if the result is not matching, the receiver will confirm the message is not integrated. Obviously, our proposed scheme can support's message integrity (see Figure 4).

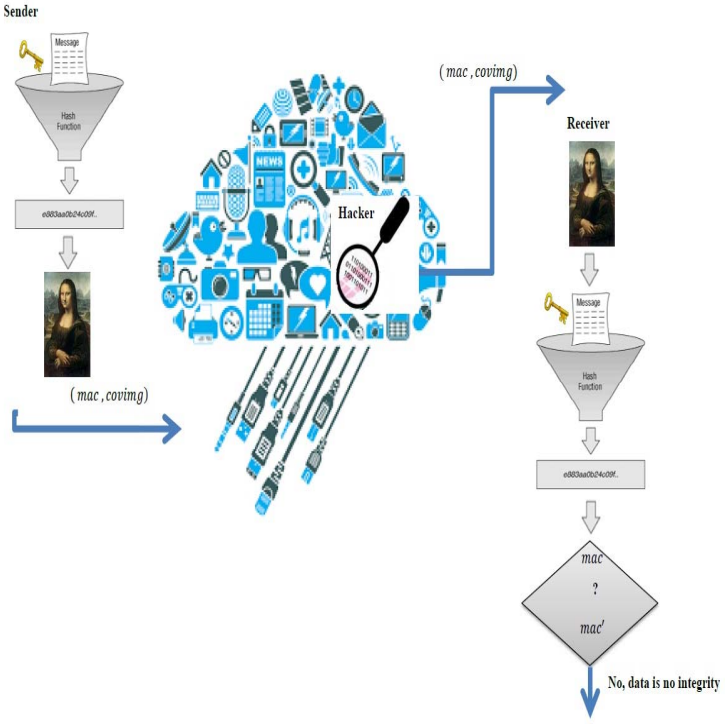


Figure 4. Data Integrity Of Our Proposed Scheme

4.2 Investigation Performance

In this section, We conduct numerous experiments to measure the efficiency and flexibility of our proposed scheme. The experiments have completed based on 3000 users that are used with images 512×512 pixels to conceal user's message over verification phase. Figure 5 views performance of verification phase. Conversely, any sender wants to exchange message with the receiver needed 0.0582 seconds as average. This result refers the high speed of our work in verification phase. Furthermore, the estimation parameters are confirmed in Table 4. Furthermore, Table 5 explains the time requirement of our scheme. We have registered through our experiments 3000 users. Moreover, our scheme supports high good results in PSNR as shown in Table 6; we used the first fifth users. Thus, our work can strongly battle visual attack. Additionally, the computing time for proposed work is short; the average time of the verification phase of each entity, containing the sender and receiver entities in IoT's environment, was equal to 0.0582 compared with Castiglione et. al's scheme that has been equaled 0.2754 (see Figure 6). Furthermore, Figures 7, 8, and 9 describe histogram of original and cover images that applied on message and MAC in the Table 6.

Table 4. Estimation Parameters

Symbol	Definition
T_h	Time processing of a hash function.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

T_{Xor}	Time processing of Xor function.
T_{Opr}	Time processing of mathematical operations such as multiplication, addition, subtraction, summation, DWT, and IDWT.
$T_{\|\|}$	Time processing of concatenation function.

Table 5. Performance Of Our Proposed Scheme

Phase	CSP	Sender	Receiver
Setting	$2T_{OPr}$	-------	-------
Verification	-------	$T_h + 3T_{Opr} + T_{\|\|} + T_{Xor}$	$T_h + 2T_{Opr} + T_{\|\|} + T_{Xor}$
Total	$2T_{OPr}$	$T_h + 3T_{Opr} + T_{\|\|} + T_{Xor}$	$T_h + 2T_{Opr} + T_{\|\|} + T_{Xor}$

Table 6. PSNR Of Proposed Scheme

Message	mac	Measures	Covimg
Bird	ba8b339e339fbf0027d8a4f38360905463534c91	PSNR	82.789
Basra	9c59b55a530e18407064e7749fb5329895353997	PSNR	83.006
Iraq	f76eea34fbe10f941f729241abc540d934b97cc0	PSNR	81.764

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

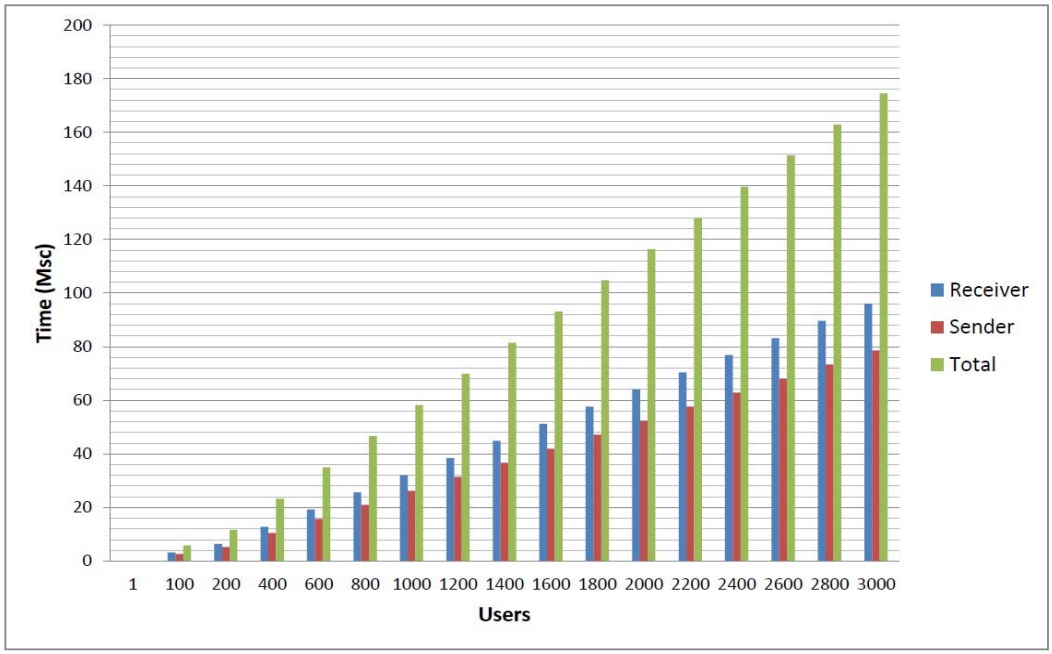


Figure 5. Views The Performance Of Our Proposed Scheme

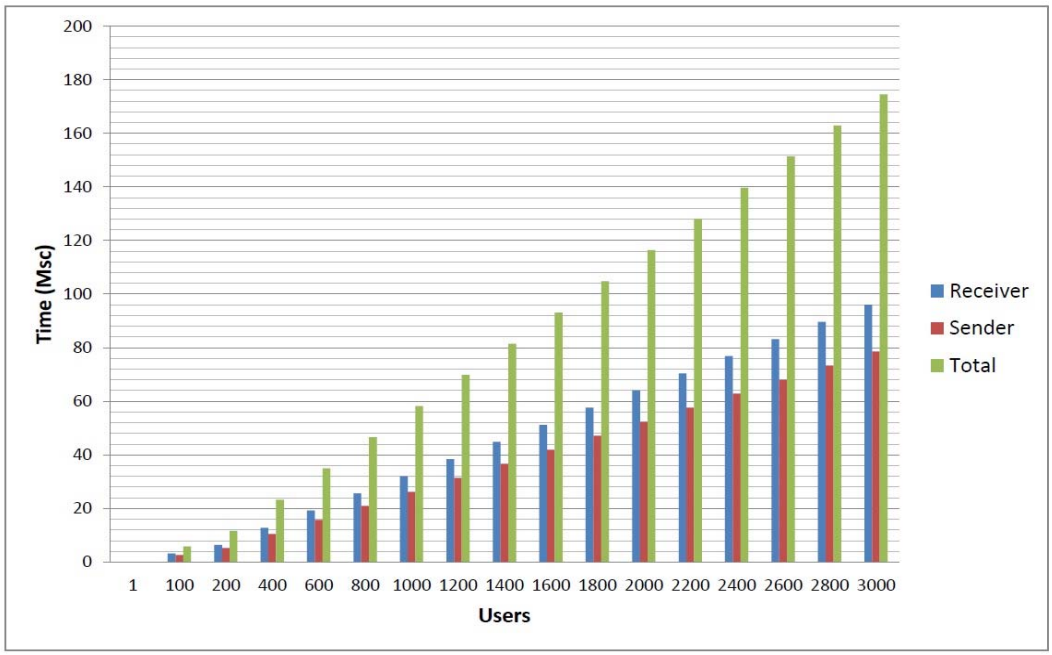


Figure 6. Views The Performance Castiglione Et. Al's Scheme

Journal of Theoretical and Applied Information Technology
31st May 2018. Vol.96. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

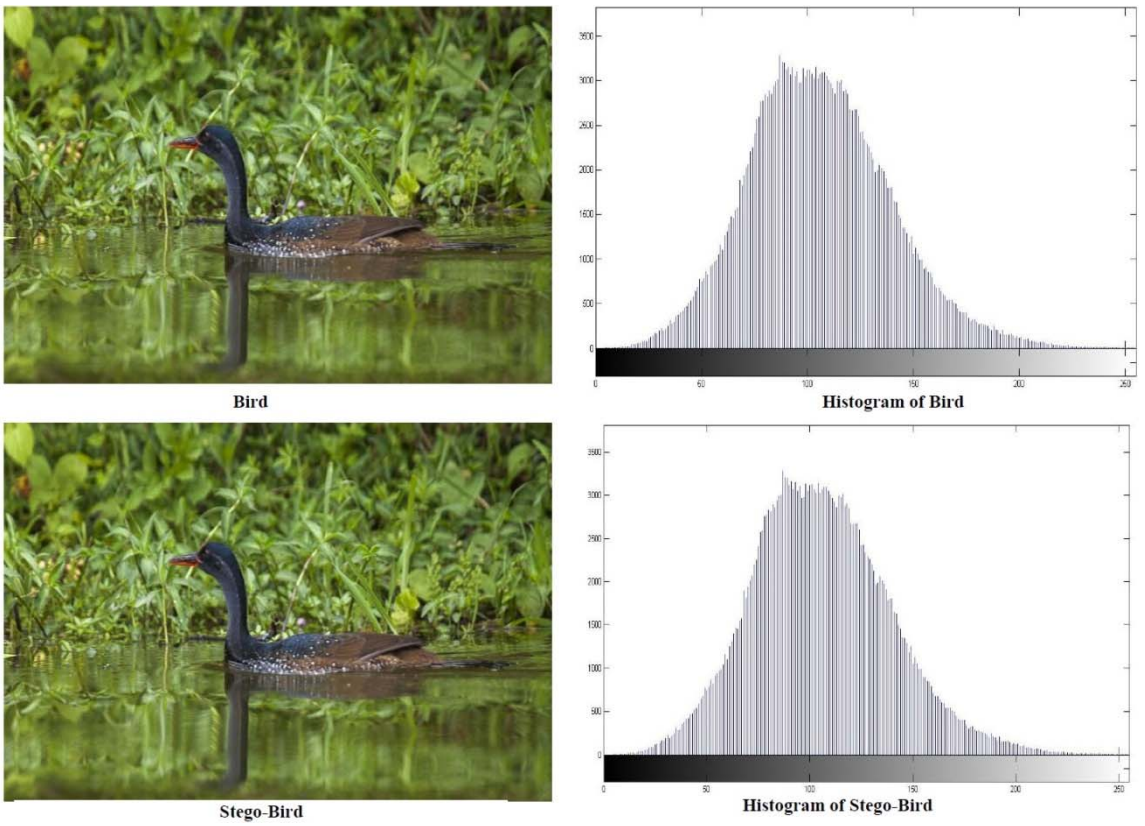


Figure 7 .views the histogram of Bird's image

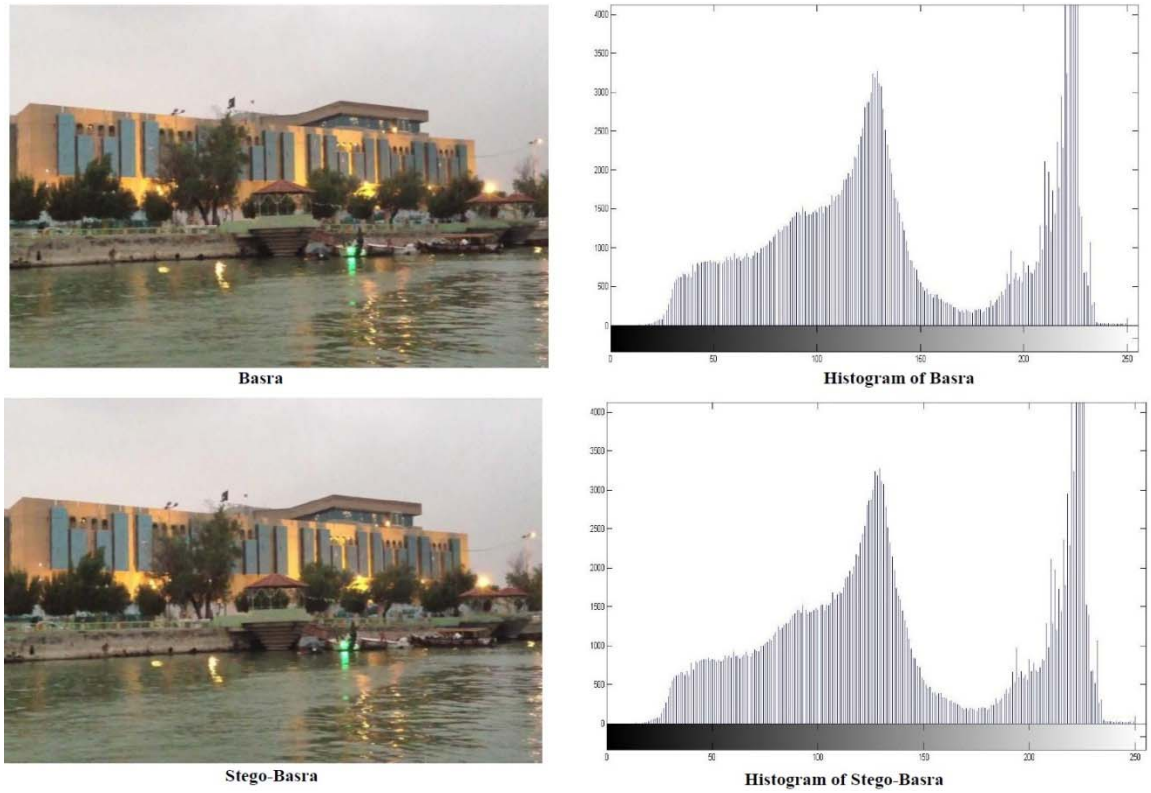


Figure 8. Views The Histogram Of Basra's Image

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

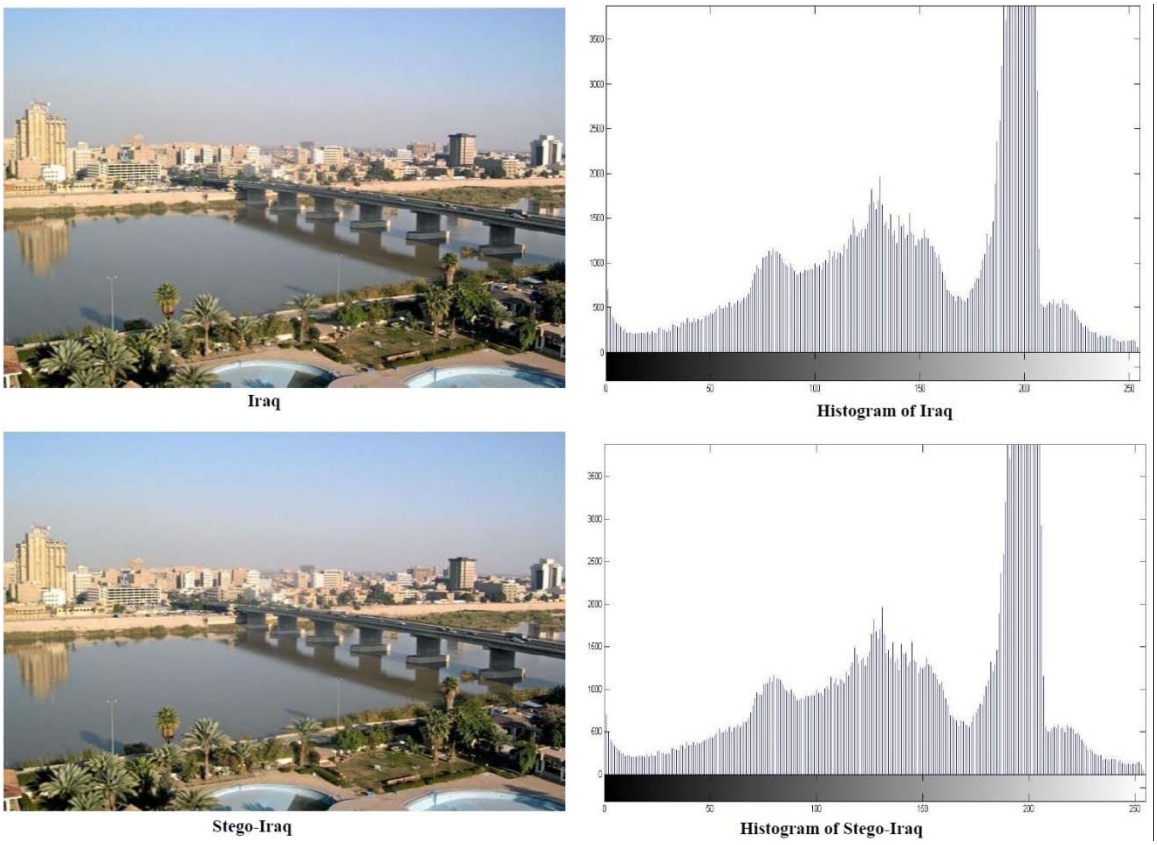


Figure 9. Views The Histogram Of Basra's Image

5. CONCLUSION

This paper proposed a confident and accessible IoT authentication system with concern of security, efficiency, scalability, elasticity and trustworthiness to meet the necessities of computing, and communication. The main essential advantages of our scheme include (1) our proposed scheme preserves a secret MAC between the sender and receiver in IoT's envroment; (2) it supports one-time message anonymity; (3) generating one key for each sender's/ receiver's login request ; (4) our proposed scheme uses DWT to hide message with crypto-hash function that makes the task of an adversary more hardly; (5) our work supports authentication and integrity of message between parties in IoT environment based on generating once key and message by using crypto-hash function, DWT, and steganography functions which are making the our work highly suitable for each exchange messages between IoT's entities. Additionally, our scheme can resist a familiar attacks such as replay attacks, MITM attacks, insider attacks, and forgery attacks. The results showed that the proposed scheme has a very good hidden invisibility, good security and robustness for a lot of MAC attacks. The proposed scheme is better in security and capacity as shown experimentally than existing schemes.

REFERENCES

[1] H. Jiang, F. Shena, S. Chena, K.-C. Li , Y.-S. Jeong, A secure and scalable storage system for aggregate data in IoT, Future Generation Computer Systems, 49 (2015), 133-141.

[2] J. Shu, Z. Shen, W. Xue, Shield: a stackable secure storage system for file sharing in public storage, J. Parallel Distrib. Comput. 74 (9) (2014).

[3] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34(1) (2011)1-11.

[4] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems 28 (2012) 583-592.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[5] Md. T. Khorshed, A.B.M. S. Ali, S. A. Wasimi, A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing, Future Generation Computer Systems 28 (2012) 833-851.

[6] Ali A. Yassin, Mushtaq A. Hasson, Hesham Saleh Ridha, A New Message Authentication Code Scheme Based on Feature Extraction of Fingerprint in Cloud Computing, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 11, pp. 1711-1716, 2014.

[7] R.L. Rivest. "The MD message digest algorithm", In S. Vanstone, editor, Advances in Cryptology - CRYPTO' 0, LNCS 5 , pp. 0 - 11, 2011.

[8] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit Algorithm For Image Steganography". IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

[9] W. Wei, F.-L. Liu, X. Ge, and Y. You, "Color image encryption algorithm based on hyper chaos," in Proceedings of the 2nd International Conference on Information Management and Engineering (ICIME'10), April, pp. 271-274. 2010.

[10] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[11] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.

[12] J. Fridrich and M. Goljan, Protection of Digital Images Self Embedding, Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, New York, NJ, USA, 1999.

[13] A. Swaminathan, Y. and M. Wu, "Robust and secure image hashing," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 215-229, 2006.

[14] N. Rabadi and S. Mahmud, "Drivers' anonymity with a short message length for vehicle-to-vehicle communications network," Proceedings of the Fifth IEEE Consumer Communications and Networking Conference (CCNC'08), Las Vegas, NV, USA, IEEE, pp. 132-133, Jan. 2008.

[15] N. Jamil and A. Aziz, "A Unified Approach to Secure and Robust Hashing Scheme for Image and Video Authentication," Proceedings of Third IEEE International Congress on Image and Signal Processing (CISP), Yantai, China, pp. 274-278, 2010.

[16] Z. Liu, H. S. Lallie, L. Liu, Y. Zhan, and K. Wu, "A hash-based secure interface on plain connection," Proceedings of the sixth International Conference on Communications and Networking in China (ChinaCom'11), Harbin, China, IEEE, pp. 1236-1239, 2011.

[17] S. I. Naqvi and A. Akram, "Pseudo-random key generation for secure HMAC-MD5," Proceedings of the Third IEEE International Conference on Communication Software and Networks (ICCSN), Xi'an, China, pp. 573-577, May, 2011.

[18] Zaid Ameen Abduljabbar, Hai Jin, Zaid Alaa Hussien, Ali A. Yassin, Mohammed Abdulridha Hussain, Salah H. Abbdal, Deqing Zou, Robust Image Document Authentication Code with Autonomous Biometric Key Generation, Selection, and Updating in Cloud Environment, Proceedings of the International Conference on Information Assurance and Security (IAS'15), Marrakesh, Morocco, IEEE, pp. 60-65, Dec. 2015.

[19] A. Castiglione, A. De Santis, A. Castiglione, and F. Palmieri, "An efficient and transparent one-time authentication protocol with noninteractive key scheduling and update," Proceedings of 28th International Conference on Advanced Information Networking and Applications (AINA'14), Canada, IEEE, pp. 351–358, May 2014.

[20] A. K. Das, A. Goswami, A robust anonymous biometric-based remote user authentication scheme using smart cards. J King Saud Univ-Comput Inf Sci, Vol. 27(2), pp. 193–210, 2015.