Journal of Basrah Researches (Sciences) **52**(1), 224 (2026)
DOI: https://doi.org/10.56714/bjrs.52.1.16

Towards Secure End-To-End Communication using a Nonce Biometric Authentication Code, Based on Iris and Duplicate Steganography

Esraa Talab[1,*], Zaid Ameen Abduljabbar[1,2], Hamid Ali Abed AL-Asadi[1], Vincent Omollo Nyangaresi[3,4], Abdulla J. Y. Aldarwish[1,5]

[1] Department of Computer Science, College of Education for Pure Sciences, University of Basrah Basrah 61004, Iraq
[2] Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China
[3] Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya.
[4] Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamil Nadu, India.
[5]Department of Computer Sciences, Sciences, Gujarat University, Ahmedabad, 380009, Gujarat, India.

ARTICLE INFO

Received 29 March 2026
Revised 28 April 2026
Accepted 07 May 2026
Published 30 June 2026

Keywords:

Smart Devices; Iris; Duplicate Steganography; Nonce Biometric Key; Nonce MAC

Citation: E. Talab et al., J. Basrah Res. (Sci.) **52**(1), 224 (2026). DOI:https://doi.org/10.56714/bjrs.52.1.16

ABSTRACT

Cloud Computing is the next biggest revolution for research organizations and top-most companies in information technology. But it has run into several security challenges so far. Two main concerns in data security are authentication and integrity, and many interesting works have been proposed to detect or prevent tampering in information transactions between end-to-end smart devices in a cloud environment. This means a robust mechanism to ensure that data is not altered during transfer. We propose a unique Message Authentication Code MAC algorithm in this work, based on duplicate steganography using the discrete wavelet transform, as well as feature matching of the smart device users. The findings from this integration aim to maintain message integrity for all smart device users and protect them from attacks such as insider attacks, forgery, and replay attacks. Next, we describe the realizability of our method through security analysis and demonstrate that it satisfies decisive safety properties such as nonce biometric key management, a user's nonce biometric key, phase key agreement, message anonymity, resistance against chosen message attack (CMA), data integrity for a smart device user's message steganography, and a transient MAC session per user. Experimental results demonstrate that the proposed work achieves an execution time of 0.126 seconds that evaluated over 100 runs with 5000 users, and an accuracy 100% when tested on 10,000 users, confirming its efficiency and robustness. Finally, through security analysis and experimental results, we demonstrate and prove that the scheme cannot be compromised by common attacks.

[*]**Corresponding author email:** esraa.talab@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

1. Introduction

A large volume of data has been transferred over the Internet in recent years due to modern information digitization technologies, such as cloud computing [1], which has seen remarkable growth. With text data as one of the most critical and widely used channels, images/audio/video are also media for passing information. Cloud computing is considered the next generation's approach to realizing their computing infrastructure and a complementary way to provide users with access to a very large volume of resources, as well as offering an effective, on-demand service tailored to their needs [2]. Nonetheless, cloud computing suffers from numerous security issues, according to IDC statistics [3]. The successful application of this depends on the fundamental need for robust security safety techniques. When two parties exchange messages in the cloud, owing to the inherent need for message protection, there is a primary requirement for automatic methods that are efficient and robust enough to determine whether the content of these text messages requires validation. That is, providing messages that are vulnerable to malicious attacks, such as replay, forgery, and insider attacks, is one of the biggest challenges in cloud and green computing. But message authentication and integrity issues have been identified as major problems in the last few years, and several methodologies have been suggested [1, 4-10]. The use of cryptographic hash functions is the single most effective way to prevent a message from being forged by one party and sent to another [4-10].

There are, however, some disadvantages regarding MAC research, which will be described in more detail in the Related Works Section. The limitation of MAC is that it does not seem to guarantee the high security level needed when used standalone as a pure MAC. For this reason, the authors Zhenxing Liu et al. [9] combined the timestamp factor with the Message Authentication Code (MAC). In this way, the hash value can be updated only once per session, and each user's message can be used only once to thwart authentication attacks.

MAC is an efficient solution to the challenges mentioned above; however, stronger and more certain factors can give better assurance over MAC. Therefore, in this article, we have provided an efficient and secure scheme to protect the text against manipulation or tampering when transferring it between users of smart devices in a cloud environment. In this algorithm, secret key allocation is carried out using strong iris features extracted with a 2-D Gabor filter, after obtaining the common intersection of the sender's and receiver's iris images from smart devices, followed by double steganography and a nonce cryptographic hash function. These combine to keep the user’s message safe from tampering. Therefore, MAC is produced by combining these strong characteristics to be increasingly resistant to malicious attacks, such as insider attacks. Afterwards, a cover image is used to hide the nonce bio-hashed value using duplicate steganography. We demonstrate that our proposed scheme retains these characteristics during the generation of nonce bio-key management, duplicate steganography, and anonymity message code for messages exchanged between the sender and receiver. It is a well-planned procedure for various queries and requires periodic authentication to reduce the actual audit cost per audit phase. Furthermore, IDC’s statistics [3] show that high-ranking, high-pressure problems in cloud computing concern integrity, which is also addressed in our paper on security in the cloud.

More robust and sure factors can provide better assurance over MAC, which is an effective solution to the above problems. Hence, in this work, we have proposed a secure and low-complexity scheme to protect documents from manipulation or tampering during transfers between smart device users in a cloud environment. The scheme combines a biometric approach using extracted strong iris features, a two-dimensional Gabor filter applied to the intersection of the sender's and receiver's irises, encryption and hashing functionality, and double steganography. These combine to keep the user’s message safe from tampering. Therefore, MAC is produced by combining these strong characteristics to be increasingly resistant to malicious attacks, such as insider attacks. Afterwards, a cover image is used to hide the nonce biometric hashed value using duplicate steganography. We demonstrate that our proposed scheme retains these characteristics during the generation of a nonce bio-key, duplicate steganography, and an anonymity code for messages exchanged between the sender's and receivers smart devices. It is a well-planned procedure for various queries and requires periodic authentication to reduce the actual audit cost per verification phase. Furthermore, IDC’s statistics [3] show that high-ranking, high-pressure problems in cloud computing concern integrity, which is also addressed in our paper on security in the cloud.

More robust and sure factors can provide better assurance over MAC, which is an effective solution to the above problems. Hence, in this work, we have proposed a secure and low-complexity scheme to protect documents from manipulation or tampering during transfers between smart device users in a cloud environment. The scheme combines a biometric approach using extracted strong iris features, a two-dimensional Gabor filter applied to the intersection of the sender's and receiver's irises, encryption and hashing functionality, and double steganography. These combine to keep the user's message safe from tampering. Therefore, MAC is produced by combining these strong characteristics to be increasingly resistant to malicious attacks, such as insider attacks. Afterwards, a cover image is used to hide the nonce biometric hashed value using duplicate steganography. We demonstrate that our proposed scheme retains these characteristics during the generation of a nonce bio-key, duplicate steganography, and an anonymity code for messages exchanged between the sender's and receiver's smart devices. It is a well-planned procedure for various queries and requires periodic authentication to reduce the actual audit cost per verification phase. Furthermore, IDC's statistics [3] show that high-ranking, high-pressure problems in cloud computing concern integrity, which is also addressed in our paper on security in the cloud.

1.1. Motivation

A plethora of protocols have been proposed for smart device networks to maintain their security posture. However, all these solutions rely on classical cryptographic primitives such as blockchains, public-key infrastructure, physically unclonable functions (PUFs), and bilinear pairings. All these methods have many security, performance, or privacy issues and are therefore not appropriate for resource-limited smart devices. To prevent attacks that negatively interfere with the reliability of smart devices, such as desynchronization, impersonation, privacy leaks, replay attacks, and DoS, should be prevented. Thus, it needs a security scheme for end-to-end communication in smart devices that is effective, efficient, and robust.

1.2. Threat Model

In this section, we present an attack model against our scheme based on the Dolev–Yao (DY) and Canetti–Krawczyk models, which are widely used to model protocol security. In these threat models, attacker Ä can do the following, resulting in the compromise of private keys for smart services and service providers.

- Changing and removing the content of intercepted messages;
- Creating and sending out false messages to vulnerable parties;
- Physiological capture and compromise of network elements such as smart devices;
- Extracting sensitive security keys from the smart meter's memory;
- Utilizing extracted memory content of smart meters to perform attacks;
- Capture of derived session keys and other session state parameters.

1.3. Contributions

Thus, several protocols have been proposed for smart device networks to safeguard their security posture. But these solutions rely on classical cryptographic systems such as blockchain, public-key infrastructure (PKI), physically unclonable functions (PUFs), and bilinear pairings. Since all these techniques face several security, performance, or privacy challenges, they are not applicable to resource-constrained smart devices. It should also prevent attacks such as desynchronization, impersonation, privacy leaks, replay attacks, and DoS, which negatively affect the reliability of smart devices. Hence, a proper, secure scheme that is efficient and robust for end-to-end smart devices is needed.

Our scheme proposes to cloud environment, as a general entity and to the message authentication and integrity in particular have three main contributions: (1) In this paper, we proposed new robust message authentication algorithm which combines shared biometric information of iris for feature extraction process, cryptography one way hash function implementation and generated duplicate steganographic representation of our input stream/message in order to structure integrity

authentication for it. (2) Strong authenticated phase keys can be obtained for both service providers and smart device users. (3) It is not only computationally efficient, but also allows for easy integration into the existing infrastructure. (4) Our scheme is realistic in the defense against various attacks like replay attack, insider attack, and reflection attack. (5) To reduce computational costs in cloud auditing facilities, the core concept of our efficient scheme has focused on determining the optimal choice of parameter value.
The remainder of this manuscript is organized as follows. Section II presents the various forms of text authentication solutions, outlining their details, identifying the most significant and widely used ones, along with a comparative analysis to identify our scheme. Section III presents the review of preliminary concepts that underlie our proposed scheme. In Section IV, we discuss the proposed scheme in terms of both configuration and authentication phases. A security analysis against the known attacks is shown in Section V. Section VI explains the implementation and performance. Finally, Section VII closes the presentation.

2. Related Works

Earlier work has introduced different authors' propositional message authentication code (MAC) schemes to guarantee the authenticity and integrity of sent messages. S. Wang et al. [4] have recently introduced the concept of message anonymity and proposed a protocol for MAC-based vehicle-to-vehicle message authentication as a means of anonymity, authentication, and message integrity. To generate the anonymous message authentication code, Hash MAC anonymity relies on a specific timestamp as a one-off factor. The authors show that MAC takes less time to process than a digital signature. But this scheme incurs extra cost in that each vehicle needs a separate hardware component, which would have to be a tamper-proof hardware device storing its ID and the shared symmetric secret. Furthermore, the proposed protocol has not undergone a security analysis, and does the author’s work provide enough detail to prevent attacks against authentication and integrity?
Here, we propose a robust scheme to resolve these issues in a cloud environment using iris biometrics. In our work, we used a phase key agreement established between users of smart devices; a biometric nonce key was also used to provide robust message anonymity for end-to-end smart devices. Furthermore, it does not have to use additional devices for a tamper-free, where the iris is increasingly revealing (every user has each particular eye), and also more secure (eg. much more difficult to steal) whenever you perform steganographic duplicates for hiding bio-MAC.
Then, three years later, the identical item was proposed by Zhenxing Liu et al. [5], proposed a hash-based secure interface between two (or more) published entities over the Internet based on a nonce shared private key, a timestamp, a public hash function, and the validity time of messages for nonce message anonymity. It is even unclear what kind of attacker it might protect against. In Ref. [10], Zi-ming Zhao et al. introduced the fusion of smart card functionality with a one-way hash function. The authors in [6] I. S. envisioned a peer-to-peer world and proposed an efficient, end-to-end secure authentication scheme. While they used a public key infrastructure, the authors did not use a smart card; instead, they used a one-way hash function for computation and proposed another method that is very efficient and has low computational cost. The disadvantage of a smart card is that it is, by definition, a more complex device, and that the additional infrastructure in the form of a card reader would need to be installed at some expense. Additionally, it requires extensive middleware implementation to standardize smart cards and communication standards. This drawback can be overcome through iris biometric features, in which the user's iris information is captured only once and reused for subsequent valid user login. Further, the smart card may be either lost or stolen, and in our proposed scheme, nobody can guess or steal anybody's iris, i.e., the sender cannot predict the receiver's iris and vice versa, because we have used a bio-shared image, which is calculated from the intersection of a sender's iris and a receiver's iris.
The nonce key idea based on non-reusability was introduced by F. Zhang et al. [7] which use an authentication protocol consisting of two cryptographically secure building blocks, run between two endpoints, an authenticated key exchange, and a keyed Hash Message Authentication Code (HMAC) is adopted to secure authentication. This allows endpoints to authenticate each other in a transparent two-way manner. Key Setup, Key Scheduling and Key Update operations are carried out independently on both ends. Thus, this method has the disadvantage of its complexity to demand

additional operations (Key Setup, Key Scheduling and Key Update). Our proposed work uses a nonce key and random numbers; a nonce-based authentication protocol; and a MAC that is valid only once per user login, balancing simplicity & security. Moreover, the proposed scheme is low-complexity and more secure because it uses an iris biometric key to generate the secret value using a keyed hash function, thereby ensuring message anonymity.

Another biometric key proposal by Al-Assam etal.[8] ingeniously combined steganography and biometric cryptosystems to provide strong mutual authentication wirelessly between the two entities, as well as keying material for nonce stego-keys. It's a concealed one-shot bio-key transferred through an untrusted pathway, valid while checking but not applicable for replay attacks on individual identities. However, the downside of this approach is its higher computational cost. Our scheme addresses this problem by transferring only the starting point and endpoint of the given iris feature vector between the sender/receptor instead of sending an explicit key, thereby rendering steganography unnecessary. So, the biometric shared between the sender and receiver of our design is a bio-shared image of their irises, which provides mutual authentication and trust between them. This is how the user will know which message to expect from a starving user. Recently, Z. A. Abduljabbar [9] developed the first nonce-biometric MAC based on a new mechanism that uses an offline signature to produce a nonce-biometric key. Unlike most others, we have generated a nonce biometric key that embeds unique iris properties, much stronger than a manual signature. Moreover, nonce bio-key and bio-MAC have been hidden in duplicate order with DWT.

In [10], R. Hossam et al. introduced the One-Key Galois Message Authentication Code (OGMAC) as an efficient extension of the classical One-Key Carter-Wegman MAC. The construction that we use has single-key entries and a universal hash function, not two keys. In addition, simplicity and security are ensured by embedding iris features into a cryptographic one-way hash function and by utilizing duplicate steganography.

However, as we have seen, most of the schemes above suffer from several disadvantages. We introduce a new text authentication system based on a stable hash function that relies on biometric image features shared by the sender's and receiver's irises in our identity design. 2. How to extract representation: Bio-shared image applies a 2D Gabor filter for a wide range of 1024-D feature vector construction. Second, the bio-key: a nonce bio-key and a cryptographic hash function are combined to securely produce a biometric nonce message code. Third, this bio-MAC is secure with double steganography. Ultimately, the message integrity is achieved at the receiver or authentication phase. Moreover, we present the combination of multiple security aspects for our scheme such as extraction of user's iris features, generation of nonce bio-key for every user's login which extracted from a large volume of other iris features, robust secrecy via message anonymity due to the use of a salt-key and various random numbers, phase key agreement with an individual nonce message key used only for every user file sign-in. These features can help prevent messages from being altered. We show that our scheme is robust, secure and efficient in terms of low time processing for generating and verifying MACs from security analysis and experimental results. Security features are illustrated in Table 1, and a comparison of security properties is given in Table 2.

Table 1. Security Features

Feature	Definition
C1	Nonce key is generated once when the valid user wants to submit a message.
C2	Bio-key is extracted from iris features by using 2-D Gabor filter.
C3	The MAC of user's message is secure when he wants to perform login phase for sending message to another user, where the acting MAC is unknown by using random numbers and nonce biometric key.
C4	Phase key agreement has been established between sender and receiver via CSP and ECC techniques. They can use this key in the following user's logins.

C5	Sender and receiver can authenticate each other by using bio-shared image which is contains shared information of sender's iris and receiver's iris.
C6	Nonce bio-key extracted from Shared bio-image for transmitting message between sender and receiver.
C7	ECC asymmetric encryption/decryption approach provides a secure channel through configuration phase.
C8	Message transmitted between sender and receiver over cloud environment.
C9	Using duplicate steganography to hide nonce biometric MAC

C1: Nonce key; C2: Biomtric key; C3: nonce message anonymity; C4: Session key agreement; C5: Mutual authentication between two parties; C6: Biometrics key management; C7 Secure channel; C8: Cloud environment; C9: Duplicate Steganography

Table 2. Comparison of Authentication Schemes

Feature	Our Scheme	S. Wang et al. [4]	Zhenxing Liu et. al. [5]	Zi-ming Zhao et. al.[6]	F. Zhang et al. [7]	Abduljabbar Z. A [9]	R. Hossam et al.[10]
C1	√	×	√	×	√	√	×
C2	√	√	√	×	√	√	√
C3	√	×	√	×	×	√	×
C4	√	√	√	√	√	√	√
C5	√	√	×	√	√	√	√
C6	√	√	×	×	√	√	√
C7	√	√	×	×	√	√	√
C8	√	×	×	×	√	√	√
C9	√	×	×	×	√	×	√

3. Preliminaries And Requirements

3.1. ECC

Elliptic Curve Cryptography (ECC) is a power to define a public key cryptography with an algebraic closure of a finite field based on Elliptic Curves. Provides higher security with much smaller key sizes than RSA (e.g., 256-bit ECC, 3072-bit RSA, and is more efficient (in short: faster computations, less power use). ECC depends on the hard problem of elliptic curve discrete logarithms. So, it requires significantly less bandwidth and memory, making it suitable for resource-constrained devices such as smartcards, smartphones, and IoT devices, and is widely used in SSL/TLS certificates, Digital Signature using ECDSA, and cryptocurrencies like Bitcoin. The only advantage of ECC over RSA is that ECC offers higher security per bit, while the key generation and signature verification are also very fast [11].

3.2. Features extraction of iris

Of these approaches, iris recognition is among the most promising due to patterns exclusive to the eye-to-eye or individual-to-individual level, which could lead to unique features alongside stability and noninvasiveness [12]. But the bio-key in our proposed scheme is generated from iris features. A 2-D Gabor filter has been used in our scheme to extract features from normalized irises to build a bio-key for message-authentication key generation. Numerous researchers have proposed and implemented various approaches to extract significant features from normalized iris images. An often-used Gabor filter is extracted for iris recognition [12]. Daugman [13] uses a 2D Gabor filter, while S. Hariprasath [14] adopts a 2D Gabor filter in his work. However, the Gabor Filters have a Gaussian

shape in both the spatial and frequency domains. This makes them stable under various transformations like translation, rotation and scaling. They are also very good with noise. Their robustness makes Gabor filters attractive for object recognition; hence, they are widely used to detect particles in iris images in iris recognition systems [14].
In this context, we have employed a Gabor filter in our scheme to extract samples from the normalized iris data and have applied the preprocessing technique described in [14] for iris localization and normalization. Additionally, we define the same as a region of interest (ROI) [15]. Then the ROI is normalized to a rectangular block of 256 × 64 pixels (see Figure 1).

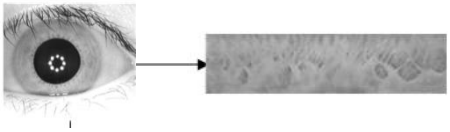

Fig. 1. Preprocessing of iris

A set of 2-D real Gabor filters with various orientations $\theta = 0^{\circ}, 45^{\circ}, 90^{\circ}\ and\ 135^{\circ}$) are used to filter the normalized iris image. Some examples of the filtered image are shown in figure 2. Each filtered image is then equally divided into 16×16 blocks, while the mean of each block is computed. Thus, we can obtain 16×16×4 = 1024 values from an iris image. After normalizing each value to an integer in the range [0, 1024], the outcome is a 1024-D feature vector:

$$V = (X_1, X_2, X_3, X_4, \ldots\ldots, X_{1024})$$

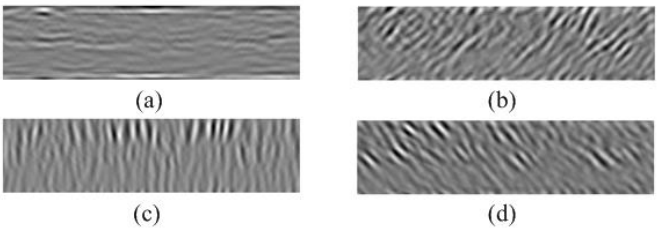

Fig. 2. Filtered images by2-D real Gabor filter

3.3. Hash Functions

Secure Hash Algorithms (SHA) were issued by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). SHA-0: The first version of the 160-bit hash was released in 1993 under the name 'SHA'. It was succeeded soon after by the minorly improved SHA-1. It was released in 1995 by the National Institute of Standards and Technology (NIST) as a new, stronger function for use in cryptographic applications as a Federal Information Processing Standard [20]. MD5 used the same design as SHA-1. IT operates on 512 bite blocks and produces 160 (20-byte) digests. Many governments use SHA-1 to set security standards across industries. It is much more resilient to malicious attacks [33, 34]. NSA offered a second family of hash functions. These include two locked hash functions, SHA-256 and SHA-512, which differ in block size. Additionally, the word size differs: SHA-256 uses 32-bit words, while SHA-512 uses 64-bit words. There exist shortened versions of each standard as well - SHA-224 and SHA-384 [16, 17, 18].

4. The Proposed Model

The suggested solution comprises two phases: the Configuration phase and the Authentication phase. The Configuration phase is done only once to generate the important parameters for the authentication process. Both end-to-end smart devices receive a biometric shared image and share a key. Each time a smart device user wishes to send an authenticated message to another smart device user, the Authentication phase is invoked. The first step is also using ECC, a cryptographic hash

function and a symmetric key encryption/decryption $Enc(.)/Dec\ (.)$. during the configuration phase (Cloud Service Provider *CSP*, Smart Device Sender *SDS*, Smart Device Receiver *SDR*). Next, they are only required to perform an ECC for secure transmission of data between over an unsecured channel. Thus, this operation is required only during the configuration phase, not in subsequent phases. Hence, CSP is not necessary at runtime and during authentication. The following steps illustrate the configuration:

- The ECC key generation is performed by (*CSP*, *SDS*, and *SDR*) to create a private key and public key, this pair will be utilized to encrypt irises sending from *SDS* as well as *SDR* to *CSP* for security purposes. The (*CSP*) then transmits the public key PU_{CSP} to both SDS and SDR allows them to encrypt their respective irises (IR_{SDS}, IR_{SDR}) which are sent back to the (*CSP*), as shown in Figure 2.
- When the *CSP* obtains (IR_{SDS}, IR_{SDR}) in encrypted form, it decrypts the irises using its private key PR_{CSP} and stores (IR_{SDS}, IR_{SDR}). Then it generates a shared image biometric by performing an intersection operation ($Shbio$ = $\mathrm{IR_{SDS}} \cap \mathrm{IR_{SDR}}$) and calculating a common key $Biok = \mathrm{Bio} - \mathrm{FX}(Shbio)$, as illustrated in figure 1 where $\mathrm{Bio} - \mathrm{FX}$ is a function to extract features. A 2-D Gabor filter was used for this purpose to compute features based on the normalized data of iris. Usually, having done this step *CSP* encrypt ($Shbio, Biok$) by use of (PR_{SDS}, PR_{SDR}) and sends both to the *SDS* and *SDR* as appropriate. The *SDS* and *SDR* finally decrypt the received ($Shbio, Biok$) using (PR_{SDS}, PR_{SDR}) as their private key. Once the configuration phase is done, *SDS/SDR* uses his/her biometric shared image to extract biometric features. Then it used such bio-features to generate a nonce anonymous key along with nonce biometric key for the authentication phase, as shown in Figure 2.

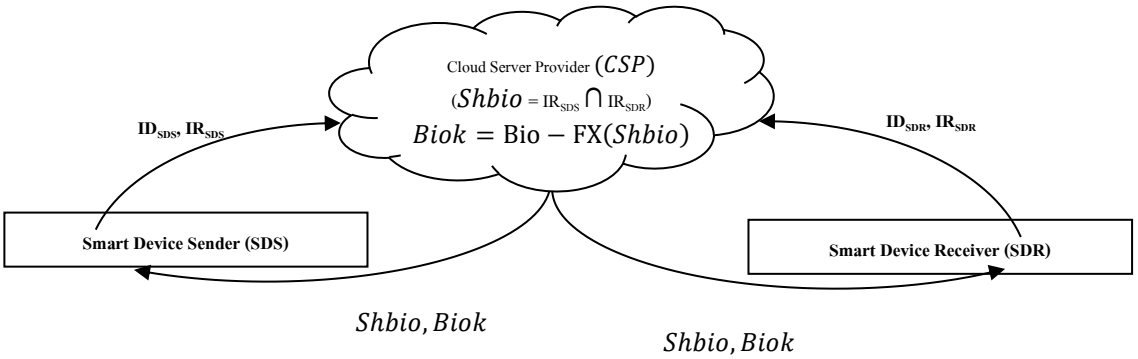

Fig. 3. Configuration phase diagram.

The Algorithm 1is summarized as follows.

Algorithm 1: Configuration Phase
Input: Iris images of sender (IRSDS) and receiver (IRSDR)
Output: Shared biometric key and system parameters

Begin
1: CSP generates ECC public/private key pairs.
2: SDS and SDR encrypt the iris images using CSP's public key.
3: Sends the encrypted iris images to CSP.
4: CSP decrypts the IRSDS and IRSDR using their private keys.
5: Calculates the shared biometric image: IB = IRSDS ∩ IRSDR.
6: Extracts iris features using a 2D Gabor filter.
7: Generates a shared biometric key from the extracted features.
8: Encrypts the shared data and sends it to SDS and SDR.
9: SDS and SDR decrypt and store the shared biometric data.
End

The authentication phase is summarized as follows.

1. $SDS \rightarrow SDR: T, T', SP_i', EP', Pos$. S execute the steps below:

- Assume SDS's text message is *T*.
- Generate nonce salt-key $Shbiok = \text{Bio} - \text{FX}\ (Shbio) \rightarrow SP_i, EP$: Where Bio-FX is a function of biometric feature extraction, SP_i and *EP* are start point and end point of extracted biometric features. SP_i and *EP* are drawn at random once. The value of *EP* parameter should be less than the length of the biometric feature vector that is 1024.
- Output biometric random number $rbio_i \in FX(Shbio) = FX\big(Sh(SP_i, EP)\big) \rightarrow Pos$ to get nonce anonymous message_code (On resending the same message by SDS to SDR or vice- versa), $T' = h(T||Shbiok||rbio_i)$.
- Compute $SP_i' = SP_i \oplus Biok$ and $EP' = EP \oplus SP_i$
- SP_i' and EP' can be embedded individually in the cover image.
- Use a duplicate steganography mechanism [19] to embed the (T') in the cover-image.
- Transmit *T* and the cover-image, which is composed of (T', SP'_i, and EP'), to SDR.

2.SDR verifies the integrity of SDR's message as follows:

- From the cover-image SP'_i, EP' can be extracted.
- Calculate $SP_i'' = SP_i' \oplus Biok$ and $EP'' = EP' \oplus SP_i''$
- Regenerate $Shbiok' = \text{Bio} - \text{FX}\ (Sh(I_i'', EP)$ depending on the position of biometric features extracted (SP_i'') and the end point of extracted biometric features (EP''). Extract biometric random number $rbio_{i_i}' = FX(Shbio(Pos \in (SP_i'', EP'')))$. Then, SDR computes $T'' = h(T'||Shbiok'||rbio_{i_i}')$ Then if $T''= T'$, it proves the integrity of *T* sent by SDS. Otherwise, the authentication phase is halted.

  The Algorithm 2 is summarized as follows.

Algorithm 2: Authentication Phase
Inputs: Message T, shared biometric features
Outputs: Authentication result

Begin
1: Generate two random start and end points, SPi and EP.
2: Extract biometric features using the Bio-FX function.
3: Generate a random biometric key (nonce).
4: Calculate the MAC address using a hash function.
5: Include (T', SPi, EP) using data hiding techniques.
6: Send the hidden image and message to the receiver.
Receiver side:
7: Extract SPi and EP from the hidden image
8: Recalculate the biometric features and the random key (nonce).
9: Recalculate the MAC address.
10: Compare the received MAC address with the calculated MAC address.
11: If they are equal → Accept the message.
12: Else: Reject the message.
End

5. Security Analysis

We demonstrate that the scheme can resist well-known security attacks, including replay and insider attack. We propose a scheme that has the following advantages, nonce-based biometric key, nonce-anonymous message code, an agreement on keys and duplicate steganography.

Theorem 1. The proposed solution supports robust anonymity for user messages.

Proof. We assume that a SDS/SDR tries to send the same message already sent before, so if an adversary intends to eavesdrop (T, T', SP_i', EP', Pos) as sender login request, he cannot use the same

thing's anonymous and biometric nonce message authentication code of the SDS $T' = h(T||Shbiok||rbio_i)$. Since each time is generated once for every request of the SDS ($rbio_i$ and $Shbiok$) [9,13]. Hence, from the intersection of SDR's iris and the SDS's iris, we extracted $rbio_i \in FX(Shbio) = \text{Bio} - \text{FX}\left(Sh(SP_i, EP)\right) \rightarrow Pos;\ \ Shbiok = FX(Shbio) \rightarrow SL_i, EO;\ \ (Shbio = \text{IR}_{\text{SDS}} \cap \text{IR}_{\text{SDR}})$. Bio- $\text{Bio} - \text{FX}$ is a function that needs to be computed for feature extraction. Ii and E are the initial and end inputs of extracted features, respectively. SP_i, EP is selected randomly once. In addition, one of the critical keys ($Shbio, SP_i, EP, Pos$) required for the adversary to compute the crypto hash function T' is not possessed. As a result, it is much more difficult for an enemy to reveal SDS's message authentication code. It is clear that our scheme can provide anonymity for smart users' messages (please refer to Table 3).

Table 3. Explain message anonymity

Message	MAC
computer science	'f95005ea64b1dd74aac6d6b27c31fad9590481a2'
computer science	'd60222b5f1defcb40f3d0012d87bc975389c2651'
computer science	'ad9bd2fef9c33b7997b752d1bc1d0bcafc8ef46c'
computer science	'2a7044a82f48473eb1ff17fabe693374d601eff1'
computer science	'72422def276b53f05bfb7ddffa035d145c7f8f28'
computer science	'd40b5b2fa21148a563a464d8c1fcdd4f53e55430'
computer science	'dbec4b6f4ea02b382bf0ec2bc331540a038daca9'
computer science	'c7b52b7f7b2d53a0d9a828f7f2a498ca738e77e8'
computer science	'182b7fb419e6ee4e7f09d996e33424157c3d99a6'
computer science	'f10ff6139995d067489df0ccbddf0c7033afa858'

Theorem 2. The proposed solution can offer strong authentication code based on biometric features.

Proof. The biometric operator is a specific piece of equipment that can identify a person in the form of certain physiological characteristics e.g. iris recognition. Iris is the best security type in biometric plans and can be overcome by well-known attacks. *SDS* and *SDR* send their irises (IR_{SDS}, IR_{SDR}) to the CSP through a secure channel in the configuration phase. The CSP then stores (IR_{SDS}, IR_{SDR}), creates a bio-shared image ($Shbio = IR_{SDS} \cap IR_{SDR}$) and sends $Shbio$ to the *SDS* and *SDR*. At the authentication stage, where either user can send a message to another, a biometric-message authentication code $T' = h(T||Shbiok||rbio_i)$ needs to be computed that bases on biometric salt-key $Shbiok = \text{Bio} - \text{FX}\ (Shbio) \rightarrow SP_i, EP$ and biometric random number $rbio_i \in \text{Bio} - \text{FX}\ (Shbio) = FX\left(Sh(SP_i, EP)\right) \rightarrow Pos$ as shown in the following clearly our proposed approach is compatible with biometric message authentication codes.

Theorem 3. The proposed solution supports biometric key management.

Proof. In the proposed work, whenever a SDS sends the text message (T) to a SDR, or vice versa, the secret and nonce biometric salt-key $Shbiok = FX(Shbio) \rightarrow SP_i, EP$ is used to compute ($T' = h(T||Shbiok||rbio_i)$. Moreover, the calculation mechanism of nonce biometric shared keys $Shbiok$ is based on (SP_i, EP), where $SP_i$is the start point of extracted biometric features and EP is the end point of extracted features. SP_i, EP are chosen nonce randomly and hidden in the cover image using duplicate sreganography. Hence, the attacker still cannot obtain the nonce biometric session keys, which means they cannot determine from where the main operators ($Shbiok, Shbio$) are at the configuration stage via *CSP*, or the (SP_i, EP, Pos) generated by the SDS in the authentication phase. Hence, our work enables biometric-key management

Theorem 4. The proposed solution is resistant to replay attacks.

Proof. An adversary can replay attacks by snooping the login message sent by the rightful *SDS* to the *SDR*. After the sender-receiver exchange has ended, an attacker uses this message to spoof the legitimate smart device user when the user logs off the system. The longing request of each new sender in our scheme must be identical with the keys $Biok, Shbio$, IR_{SDS}, IR_{SDR} generated by CSP. Consequently, no authenticated message replayed to the receiver can be valid to an adversary. Hence, this type of attack is not applied to an adversary, and the replay attack in our suggested protocol becomes significantly more difficult.

Theorem 5. The scheme prevents a parallel-session attack or forgery attack.

Proof. In case of impersonation by the valid session message (T, T', SP_i', EP', Pos) can be utilized using secret parameters $Shbiok, Shbio$, IR_{SDS}, IR_{SDR} to re-compute because an adversary has no idea about $Biok, Shbio$, $, SP_i', EP', Pos$ to compute$(T', SP_i', EP', Pos, rbio, Shbiok, biok)$. Finally, an adversary will not be able to construct a valid session message and thus cannot apply forgery attack. Thus, the proposed work can defend against forgery attack.

Theorem 6. The proposed scheme makes hidden biometric authentication code difficult to recover.

Proof. To enhance the security of the hidden nonce biometric authentication code $(T' = h(T||Shbiok||rbio_i)$, the proposed work used a duplicate steganography mechanism [19] to embed in in the cover-image. Although a third party or attacker could detect whether the bits of $T'$are an integral part of a cover image, the attacker will have difficulty restoring such data because an integral part of the bits of $T'$is in a duplicate steganography mechanism. Moreover, each one of the four bytes (MACLESS) has been embedded in a sub cover image through DWT. A misleading steganalysis process can make the recovery of nonce biometric authentication code T' very difficult. Hence, disclosing the $T'$of *SDS* is difficult for an eavesdropper. The proposed scheme can obviously support the difficult recovery of T'.

Theorem 7. Steganography is used by the proposed scheme to avoid attracting an impersonator's attention.

Proof. The benefit of information concealment using only cryptography is that the yet-deciphered bit serial is not cause for interest during transfer of data between *SDS* and *SDR*, but encrypted messages are visible as a form of communication and thus can also attract attraction. However, encrypted messages are visible and can thus attract attraction. In contrast, steganography conceals the fact that a secret message is being sent and even hides its contents. It hides sensitive data ($T^{'}$) in a duplicate steganography mechanism. So this scheme will not draw attention from any eavesdropper, and the messages are unknown to potential attackers. Additionally, $T^{'}$ is difficult to extract from the stego-image and data are generated and used for a single time only. Hence, without attracting eavesdroppers' attention to the proposed scheme, it remains secure.

Theorem 8. The proposed scheme can maintain biometric iris features in the configuration phase.

Proof. In nearly all cases, the stealing phase is where the attacker attempts to steal sensitive data for use in the authentication stage. In the proposed scheme, each of *CSP*, *SDS*, and *SDR* uses a strong asymmetric cryptographic method, namely ECC, to generate a private key and public key. These keys are adopted to encrypt the IR_{SDS}, IR_{SDR} irises data sent from *SDS* and *SDR* to *CSP*, as well as the bio-shared data and biometric key ($Shbio, Biok$) that will be transmitted from *CSP* to *SDS* and *SDR*. Thus, it would not make sense for an attacker to know iris ' dataand main keys ($Biok$) without obtaining the decryption keys (PR_{SDS}, PR_{SDR}) using ECC technology. Clearly, this scheme provides a high level of protection during the configuration phase.

Theorem 9. The proposed scheme is resistant to MITM attacks.

Proof. For example, in this attack, the intruder can block the message from *SDS* to *SDR*. When a user logs out of *CSP*, they can reuse that message/image document. In the proposed solution where all parameters were securely encrypted with $Biok$, and anonymous message_code $T' = h(T||Shbiok||rbio_i)$ is generated based on shared biometric features and nonce biometric random number. In addition, the scheme hides in T' in a duplicate steganography manner. Moreover, SDS generates a temporary bio-salt key one time by producing sensitive data $Shbiok = \text{Bio} - \text{FX}\ (Shbio) \rightarrow SP_i, EP$ as a session request towards *SDR*. As (T', SP_i', EP') become useless when *SDS/SDR* logs off from *CSP*. If an attacker listens to the transmission between *SDS* and *SDR* and finds that the key is used only once. Hence, computing T' is difficult. We will show that the proposed scheme overcomes an MITM attack.

6. Implementation And Results

To assess the efficiency and accuracy of our proposed scheme, we have conducted a number of experiments. The experiments were executed in a simulated environment for evaluate the performance of the proposed system. The implementation was executed on a 4.7 GHz Intel Core i7-1255U machine equipped with 8GB RAM and used Python to implement the proposed work.
For evaluation purposes, biometric iris data was collected and then processed using feature extraction via a two-dimensional Gabor filter, producing a 1024-dimensional feature vector. The proposed work was tested using 5,000 users for execution time analysis and 10,000 users for accuracy assessment, each experiment was replicated 100 times to ensure consistency and reliability of the results. The first figure, 3, demonstrates the running time for the authentication phase. For denoting the best solution of our proposed, each user has equal time for authentication phase of our scheme which is 0.126 seconds. Moreover, the evaluation metrics are presented in Table 4. Table 5 presents the time requirement for our proposed scheme. Secondly, regarding system efficiency, we address the accuracy of the proposed work. In practice, as illustrated in Figure 4, we get all the top results accurate (100%).

Table 4. Evaluation parameters

Symbol	***Definition***
TM_{RSA}	Running time of ECC.
TM_h	Running time of a hash function.
TM_{Xor}	Running time of Xor function.
TM_{Opr}	Running time of mathematical operations such as multiplication, addition and subtraction.
TM_{ST}	Running time of duplicate steganography.

Table 5. Performance of our proposed scheme

Phase	***CSP***	***Sender***	***Receiver***
Configuration	$TM_{ECC} + T_{Opr}$	TM_{ECC}	TM_{ECC}
Authentication		$4TM_{Opr} + 1TM_h + T_{Xor} + T_{MST}$	$2TM_{Opr} + T_{Mh} + TM_{Xor} + T_{MST}$
Total	$TM_{ECC} + TM_{Opr}$	$TM_{ECC} + 4TM_{Opr} + 1TM_h + TM_{Xor} + TM_{ST}$	$TM_{ECC} + 2TM_{Opr} + TM_h + TM_{Xor} + TM_{ST}$

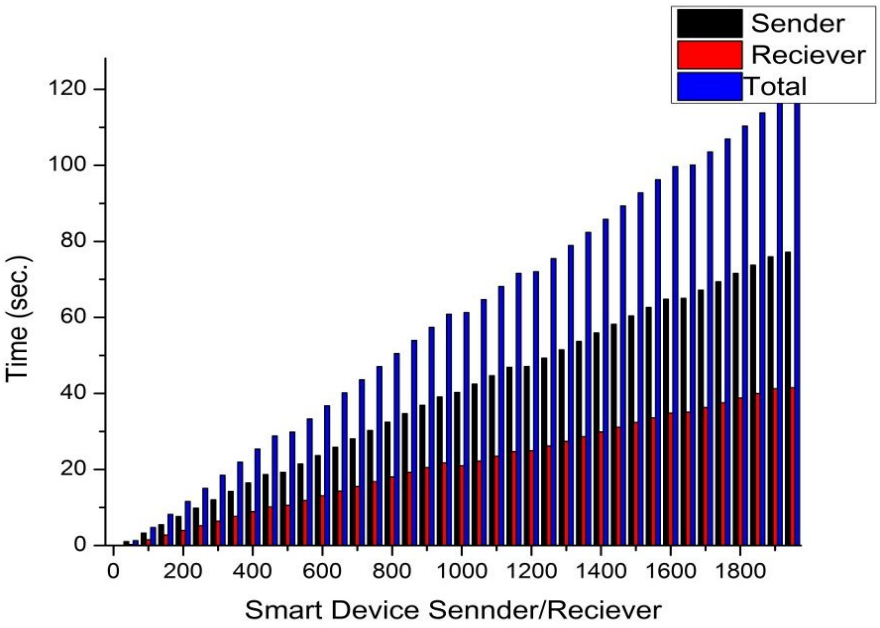

Fig. 4. shows the performance of our proposed scheme

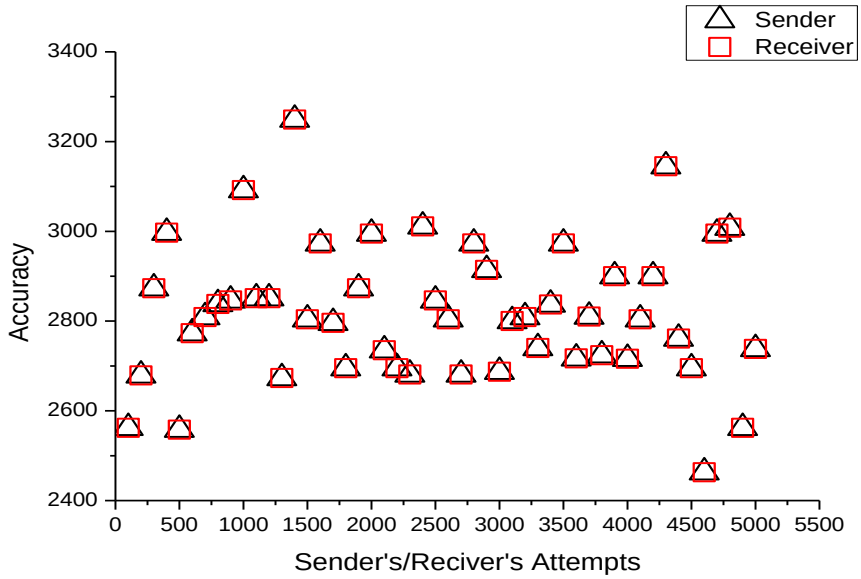

Fig. 5. shows the accuracy result of our proposed scheme

7. Conclusion

First, as previously stated, our paper is basically a literature survey on the strengths and weaknesses of integrity and authenticity in the past few years. This paper proposes a new identity-based efficient biometric nonce message authentication code for end-to-end smart devices users in the cloud computing environment. It proved to be a very good method for symmetric biometric key generation using iris biometric feature extraction. This scheme is intended to expand the roles while limiting previously known attacks. However, the tremendous advantage of this first technique is that no single opponent gets the keys due to iris feature removal, and if the *SDS*'s and *SDR*'s irises are closely positioned in front of each other, the bearer may not obtain a biometrically shared image. Third, it issues a nonce biometric key, thereby resulting in nonce message anonymity. Fourth, it addresses biometric key management. The fifth factor is that authentication is linked to an individual's biometrics. Furthermore, the security analysis section proves that the proposed scheme is resistant to

both replay attacks and forgery attacks. The proposed scheme has a very strong security proof and low time and computational costs, which are comparable to those of similar previous schemes. From the figure above, we can infer that this shared iris biometric feature, derived from a one-way hash function between two endpoints with duplicate steganography, is secure enough against message passing. This technique can also be combined to authenticate the transmitted message, verify its integrity, and prove the sender's identity. In conclusion, our scheme provides both usability and security.

References

[1] T. Rethika, I. Prathap, R. Anitha, and S. V. Raghavan, "A novel approach to watermark text documents based on eigen values," in Proc. 9th Int. Conf. Network and Service Security (N2S), Paris, France, Jun. 2009, pp. 1–5.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013, DOI: 10.1002/wcm.1203.

[3] A. T. Velte, T. J. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach. New York, NY, USA: McGraw-Hill, 2010, p. 35.

[4] S. Wang, Z. Fan, Y. Su, B. Zheng, Z. Liu, and Y. Dai, "A Lightweight , Efficient , and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks," 2024. DOI: doi.org/10.3390/electronics13081418.

[5] Z. Liu, H. S. Lallie, L. Liu, Y. Zhan, and K. Wu, "A hash-based secure interface on plain connection," in Proc. 6th Int. ICST Conf. Communications and Networking in China (CHINACOM), Harbin, China, Aug. 2011, pp. 1236–1239, DOI: 10.1109/ChinaCom.2011.6158347.

[6] Z.-M. Zhao, Y.-F. Liu, H. Li, and Y.-X. Yang, "An efficient user-to-user authentication scheme in peer-to-peer system," in Proc. 1st Int. Conf. Intelligent Networks and Intelligent Systems (ICINIS), Wuhan, China, Nov. 2008, pp. 263–266, DOI: 10.1109/ICINIS.2008.142.

[7] F. Zhang, X. Huang, B. Chen, Y. Huo, and Z. Liu, "Research on the Machinability of Micro-Tapered Hole Group in Piezoelectric Atomizer and the Improvement Method," 2022, DOI: doi.org/10.3390/s22207891.

[8] H. Al-Assam, R. Rashid, and S. Jassim, "Combining steganography and biometric cryptosystems for secure mutual authentication and key exchange," in Proc. 8th Int. Conf. Internet Technology and Secured Transactions (ICITST), London, U.K., Dec. 2013, pp. 369–374, DOI: 10.1109/ICITST.2013.6750224.

[9] Z. A. Abduljabbar, Z. A. Abduljabbar, and R. J. Mohammed, "Towards nonce biometric-message authentication code in cloud computing," Journal of Engineering and Applied Sciences, vol. 13, no. 19, 2019.

[10] R. Hossam, F. Heba, M. Yasser, and M. A. El, "A Proposed Biometric Technique for Improving Iris Recognition," *Int. J. Comput. Intell. Syst.*, pp. 1–11, 2022, DOI: 10.1007/s44196-022-00135-z.

[11] V. S. Miller, "Use of elliptic curves in cryptography," in Advances in Cryptology—CRYPTO '85, Lecture Notes in Computer Science, vol. 218, Berlin, Germany: Springer, 1986, pp. 417–426, DOI: 10.1007/3-540-39799-X_31.

[12] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security & Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003, DOI: 10.1109/MSECP.2003.1193209.

[13] J. Daugman, "How iris recognition works," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, Jan. 2004, DOI: 10.1109/TCSVT.2003.818350.

[14] S. Hariprasath and V. Mohan, "Biometric personal identification based on iris recognition using complex wavelet transformations," in Proc. Int. Conf. Computing, Communication and Networking, St. Thomas, VI, USA, Dec. 2008, pp. 1–5, DOI: 10.1109/ICCCNET.2008.4787736.

[15] L. Yu, D. Zhang, and K. Wang, "The relative distance of key point based iris recognition," Pattern Recognition, vol. 40, no. 2, pp. 423–430, Feb. 2007, DOI: 10.1016/j.patcog.2006.03.008.

[16] R. L. Rivest, “The MD4 message digest algorithm,” in Advances in Cryptology—CRYPTO ’90, Lecture Notes in Computer Science, vol. 537, Berlin, Germany: Springer, 1991, pp. 303–311.

[17] Z. A. Abduljabbar et al., “A robust and efficient authentication protocol for intelligent systems in smart healthcare IoMT,” in 2025 IEEE 24th Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), Guiyang, China, 2025, pp. 1357–1364, DOI: 10.1109/Trustcom66490.2025.00157.

[18] I. F. Khazal et al., “Towards secure QR-based message for E2E communication in IoT-cloud,” in Software Engineering: Emerging Trends and Practices in System Development, R. Silhavy and P. Silhavy, Eds., CSOC 2025, Lecture Notes in Networks and Systems, vol. 1560. Cham, Switzerland: Springer, 2025, DOI: 10.1007/978-3-032-00239-6_15.

[19] P. V. Nadiya and B. M. Imran, “Image steganography in DWT domain using double-stegging with RSA encryption,” in Proc. Int. Conf. Signal Processing, Image Processing & Pattern Recognition (ICSIPR), Coimbatore, India, Feb. 2013, pp. 283–287, DOI: 10.1109/ICSIPR.2013.6497941.

Journal of Basrah Researches (Sciences) **52**(1), 224 (2026)
DOI: https://doi.org/10.56714/bjrs.52.1.16

نحو اتصال آمن من طرف إلى طرف باستخدام رمز مصادقة بيومتري عشوائي، يعتمد على قزحية العين وتقنية إخفاء البيانات المكررة

إسراء طالب[1،*] ، زيد أمين عبد الجبار[1,2]، *حامد علي عبد الأسدي[1]* ، فينسنت أومولو نيانغاريسي[3,4]، عبد الله جاسم ياسين [1،5]

[1] قسم علوم الحاسوب، كلية التربية للعلوم الصرفة، جامعة البصرة، البصرة 61004، العراق.
[2] معهد شنتشن، جامعة هوا تشونغ للعلوم والتكنولوجيا، شنتشن 518000، الصين
[3] قسم علوم الحاسوب وهندسة البرمجيات، جامعة جاراموجي أوغينغا أودينغا للعلوم والتكنولوجيا، بوندو 40601، كينيا.
[4] قسم الإلكترونيات التطبيقية، كلية سافيثا للهندسة، معهد سافيثا للعلوم الطبية والتقنية، تشيناي 602105، تاميل نادو، الهند.
[5] قسم علوم الحاسوب، كلية العلوم، جامعة غوجارات، أحمد آباد، 380009، غوجارات، الهند.

معلومات البحث

الاستلام 29 اذار 2026
المراجعة 28نيسان 2026
القبول 07 أيار 2026
النشر 30 حزيران 2026

الكلمات المفتاحية

الأجهزة الذكية، قزحية العين، إخفاء مكرر، مفتاح بيومتري عشوائي، رمز مصادقة الرسائل العشوائي

Citation: E. Talab et al., J. Basrah Res. (Sci.) **52**(1), 224 (2026).
DOI:https://doi.org/10.56714/bjrs.52.1.16

الملخص

تُعدّ الحوسبة السحابية الثورة الأبرز القادمة لمؤسسات البحث العلمي وكبرى شركات تكنولوجيا المعلومات، إلا أنها واجهت حتى الآن العديد من التحديات الأمنية. يتمثل أحد أهمّ هذه التحديات في أمن البيانات في المصادقة وسلامة البيانات، وقد طُرحت العديد من الدراسات المهمة لكشف ومنع التلاعب في عمليات تبادل المعلومات بين الأجهزة الذكية في بيئة سحابية. لهذا السبب، لا تُجدي العديد من الطرق المُستخدمة حاليًا في إيقاف التلاعب والهجمات المُعادية على مجموعة البيانات. لذا، تبرز الحاجة إلى آلية قوية لضمان عدم تغيير البيانات أثناء نقلها. في هذه الدراسة، نقترح خوارزمية فريدة لرمز مصادقة الرسائل (MAC)، تعتمد على إخفاء البيانات المُكررة باستخدام تحويل المويجات المنفصلة، بالإضافة إلى مطابقة خصائص مُستخدم الجهاز الذكي. تهدف نتائج هذا التكامل إلى الحفاظ على سلامة الرسائل لجميع مُستخدمي الأجهزة الذكية وحمايتهم من هجمات مثل هجمات المُتسللين، والتزوير، وإعادة الإرسال. بعد ذلك، نصف إمكانية تطبيق طريقتنا من خلال تحليل أمني، ونُبين أنها تستوفي خصائص أمان حاسمة، مثل إدارة مفتاح القياسات الحيوية العشوائي، ومفتاح القياسات الحيوية العشوائي الخاص بالمستخدم، واتفاقية مفتاح الطور، وإخفاء هوية الرسائل، ومقاومة هجوم الرسالة المختارة (CMA)، وسلامة البيانات لإخفاء معلومات الرسائل الخاصة بمستخدم الجهاز الذكي، وجلسة MAC مؤقتة لكل مستخدم. وأخيرًا، من خلال التحليل الأمني والنتائج التجريبية، نُثبت ونُبرهن على أن هذه الطريقة لا يمكن اختراقها بواسطة الهجمات الشائعة.

***Corresponding author email:** esraa.talab@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq