Towards Secure QR-Based Message for E2E Communication in IoT- Cloud

Iman Fareed khazal[1], Hend Muslim Jasim[2], Mushtaq A. Hasson[2], Zaid Ameen Abduljabbar[2,3(✉)], Vincent Omollo Nyangaresi[4,5], Abdulla J. Y. Aldarwish[2], and Husam A. Neamah[6]

[1] Department of Management Information Systems, College of Administration and Economics, University of Basrah, Basrah 61004, Iraq
eman.fare@uobasrah.edu.iq

[2] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
{hend.jasim,mushtaq.husson,zaid.ameen, abdullajas}@uobasrah.edu.iq

[3] Department of Business Management, A-Imam University College, Balad 34011, Iraq

[4] Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya
vnyangaresi@jooust.ac.ke

[5] Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamil Nadu, India

[6] Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Debrecen 4028, Hungary
husam@eng.unideb.hu

Abstract. The contribution of smart mobility devices to the Internet of Things (IoT) has transformed everyday life, offering the ability to access and manage vast quantities of data in a revolution that continues to sweep the world. However, this incredible progress has led to the development of new challenges. The most significant of which is the continuing requirement for up-to-date security measures. Conventional solutions have tended to require heavier hardware while remaining vulnerable to new attack strategies; therefore, they are inappropriate for end-to-end SDs within the IoT-cloud. To overcome this problem, we propose a secure and lightweight solution that offers the combined security benefits of resistance data against attack and maintenance of privacy in communications for end-to-end E2E SDs. The strategy proposed is based on the least significant bit, cryptographic hash function randomization, with quick response (QR) message application. The proposed scheme offers many advantages, including user anonymity and message privacy, data integrity, key agreement, and one-time message code for each user session. The scheme also has additional commercial benefits given that QR code reading and generation does not result in additional costs. The results demonstrate the potential wide-ranging benefits, applications, and performance improvements.

Keywords: Communication system security · IoT-cloud · key management · lightweight one-time MAC · quick response

R. Silhavy and P. Silhavy (Eds.): CSOC 2025, LNNS 1560, pp. 218–236, 2025.
https://doi.org/10.1007/978-3-032-00239-6_15

1 Introduction

The Internet of things (IoT) excites and holds much promise and attention for data management throughout all technological disciplines including areas as varied as oil and gas exploration and mining operations in the field to academic research in any subject in addition to online social networks (such as Facebook, Viber, and WhatsApp) and all forms of multimedia data. To manage the enormous quantities of data generated from data collection devices and stored on rapidly advancing storage devices, solutions are now sought to enable effective and professional total data analysis and management.

The use and integration of SDs (SDs) has led to the development of the IoT, in which any data generator can be linked to the Internet to store data and communicate. The main challenge then becomes the security of this data within the IoT [1–4].

The growing market for SDs was estimated at 1.2 billion people globally in 2014 [5]. SDs offers the facility for easy and rapid Internet access with concomitant communication capabilities across devices, particularly with the third and fourth generations of cellular systems. This means that SDs are critical in communication within the IoT. However, despite the much recent technological advancement in device interaction capabilities, the security of communications remains a weak point of the IoT.

As SDs become integrated progressively further into daily life, the cross-communication between devices is increasingly necessary. Although *end-to-end* (E2E) is predicted to confer enormous benefits in facilitating communication [6], it also inevitably leads to one of the most significant security issues for the IoT, that is, E2E interaction between devices [6].

Furthermore, while the processing capability of SDs is constantly improving, it is still unable to match that of personal computers. As the dependence on inter-communication between SDs for the IoT increases, it's crucial to recognize the existing drawbacks in this field, such as replay attack and reflection attack, as well as guessing of S and R secret keys [7, 8]. These issues currently prevent the provision of sufficient or real simple utility security to maintain E2E message security and privacy. In this context, the need for a better, more efficient security provision is urgent to counteract security threats [9, 10].

Some additional security problems are also observed in the communication between two entities, which is not the case in the IoT-cloud environment. Thus, a robust, but lightweight security solution for the IoT-cloud environment is required to ensure data authentication, integrity, and privacy. These issues represent the most crucial security concerns [1–4, 11–13]. Despite this situation, the availability of appropriate security solutions between E2E SDs for the IoT-cloud environment remains a significant issue.

Conventionally, three standard approaches are used to prevent message manipulation during transmission between E2E users. The first is cryptography of one-way hash functions; second is watermarking; and third is application of digital signatures. However, in spite of the achievements of the existing approaches in message authentication and integrity, several obstacles exist. For example, watermarking approaches are expensive [1] because they require additional processing time for message authentication to embed and extract watermark information. Similarly, the utilization of digital signatures is also expensive [6]. *Message authentication code* (MAC) is to authenticate both the S of a message and its integrity. Cryptography one-way hash function has the advantage of being quicker to authenticate than a digital signature and watermarking [3].

To secure E2E message delivery, we propose an approach that utilizes MAC and cryptography one-way hash function. This approach categorizes the message sent by a legitimate user via a smart device. The authenticity and integrity of the received message are then protected by the key function of MAC-validation. Several tools and applications, including the secure hash function (SHA-1), use MAC functions.

Furthermore, MAC functions should demonstrate functionality in resisting standard attacks and adversary strategies such as forgery, replay, modification, and insider. This means that even if an adversary or attacker could access sensitive data that holds the shared key and generate MACs for selected messages, the MAC for other messages remains safe and inscrutable without excessive additional work implications. The S and R, as the main components of a MAC strategy, efficiently use the same secret key, simplifying the process. Therefore, in the setup phase, using the same key in a similar way to symmetric encryption, the message components should agree. Additionally, MAC could be generated for other messages by any user who provides the appropriate initial authentication [7, 8, 14, 15].

MAC is extremely responsive to any changes within the message. Any updates of a user's message results in the MAC transforming around 50% of their bits to manipulate the transformed message [16, 17]. For MAC validation to be successful, all of the bits of the MAC received by the S must match those calculated by the R's MAC. This authentication condition is incontrovertible for MAC-protected user's communications. Therefore, this approach is inappropriate for situations such as e-banking transactions.

This paper presents a novel lightweight, high integrity MAC strategy for smart device communication in the IoT-cloud environment, which consists of a two-stage (setup and authentication) process. The strategy presented offers the advantages of authentication, integrity protection, and privacy preservation for E2E messages delivered over an unsecure communication channel.

The proposed strategy involves a shared secret key, MAC, quick response (QR) code, and steganography between the S and R corresponding SDs. The reliability of this strategy is anchored in the shared secret key, a robust element agreed upon by the S and R in the setup phase. In the first authentication step, the S randomly scatters the characters of the message and then encodes the scattered message into a QR code to guarantee message privacy; in the second step, based on the least significant bit (LSB), a MAC of the message is concealed inside an image to ensure integrity. Thus, inside the S's image, the S's MAC is concealed. The S's image is then used as the cover image forwarded to the R. Simultaneously, by utilizing the same secret keys, the R can determine the legitimacy of the S's MAC in order to complete message integrity during the authentication phase. In addition, the R can read that QR code using a decoder to obtain the message embedded in the code. To minimize audit costs during this authentication phase, the procedure is formally structured with regard to authentication mechanisms and probability analysis. The scheme presented in this paper has five distinct benefits:

1. Secure key exchange with authenticated session keys between paired SDs in the IoT-cloud can be attained by users and service providers via means, which is particularly appropriate, for energy-limited SDs;
2. Simple integration utilizing available infrastructure, with easy deployment and management results in a low-cost solution;

3. Fundamental security requirements for secure communication between E2E SDs in the IoT-cloud are met with additional provision for resistance to a wide range of attack strategies, such as forgery replay, insider, reflection, *man-in-the-middle* (MITM), offline guessing, *denial of service* (DOS), online key-guessing, and message privacy attacks;
4. Increased message security and privacy are ensured by utilizing randomization with QR code mechanism;
5. Processing costs of cloud audit services are minimized by the effective use of optimum processing parameters.

In the remainder of this paper, a summary of other relevant issues is presented in Sect. 2. The fundamental requirements of the suggested security strategy are presented in Sect. 3. The suggested work is discussed in Sect. 4 in detail. Details of implementation results and security analysis are indicated in Sect. 5, and the paper concluded in Section.

2 Related Work

Various authentication and integrity methodologies based on cryptographic hash function have been proposed by various authors over the last few years to secure the generation and transfer of a robust hash value between different entities. Many of these schemes have pitfalls. With this in mind, recent developments in secure messaging using MACs will be presented along with their disadvantages; the situation from an IoT perspective will also be discussed.

In 2006, Swaminathan et al. [18] employed Fourier–Mellin transform features to enhance an algorithm for an image hash, resulting in stable 2D affine transformations. To ensure a robust image hash, this process also incorporated the outputs of the Fourier–Mellin transform with key-dependent randomization. This scheme with limitations, even though it was successful in identifying the locus of malicious manipulations, the wrap-around effect of the Fourier–Mellin transform led to errors in pinpointing the exact location of these manipulations. However, the potential impact of this research on the field of image hashing is significant, making it a topic of great relevance.

The message anonymity approach was demonstrated in 2008 by Rabadi and Mahmud [19]. To engender message anonymity, authentication, and integrity, this strategy involved the utilization of MAC between vehicles. To produce an anonymous message, this approach of MAC anonymity relied on a timestamp (i.e., a one-time factor). However, to ensure the ID and shared symmetric secret could be saved, additional hardware should be installed in each vehicle, which obviously results in requirements for further expenditure. Furthermore, their work did not provide detailed security analyses.

To produce a transformed image, the concept of a permutation key was introduced later in 2010 by Jamil and Aziz [20]. This approach to ensure security during communication involved a secure hashing scheme between two entities. The key role of the permutation key is to deter an attacker from guessing the hashed value, as it is employed for each block of the divided image. However, this methodology has a drawback-feature extraction is used to generate the image hash and the permutation key. Therefore, any adversary familiar with this weakness may utilize the relationship between the permutation key and hashed value.

Liu et al. [21] reevaluated the approach of message anonymity in 2011 by developing a hash-based secure interface between two entities over the Internet. This approach, which utilized a one-time shared private key, a public hash function, a timestamp, and a validity period, has the potential to produce nonce message anonymity. The attacks that this proposed method can combat are not explicitly explained.

Naqvi and Akram [22] introduced an approach in the same year that is crucial for strengthening the robustness of the key-based hash MAC (HMAC-MD5). They devised a robust key using an MD6 compression function, which was then used to compute the HMAC. The use of MD6-maintained randomization to generate the key made it challenging for an attacker to predict the key. However, the discussion on the security implications of this approach was somewhat limited, primarily focusing on exhaustive key search and birthday attacks.

To encrypt and protect the hashed value MAC-MD5 by utilizing a data encryption standard (DES), Chaisri and Amornraksa [23] presented the idea of preserving the integrity of a faxed document in 2012. In this approach, the secret key of DES is added by the S to the faxed document before sending it to the R, representing a significant drawback to this method. Therefore, it is possible for an attacker or adversary to extract and reuse the secret key to decrypt the MAC. Additionally, an adversary can generate a fake faxed document by reusing the key to produce it, and the R would be unaware of its illegitimate origin.

In 2012, Singh et al. [24] revisited the concept of conserving image content based on self-embedding strategy. This strategy permitted the partial repair of the image segments that were manipulated, cropped, or changed. Embed a compressed version of the image within the LSB of the image's pixels, representing the main underlying strategy for this approach. The principal drawback of this approach is the inherent weakness of the embedded information.

In 2014, Maleki et al. [25] presented a protocol based on an adjusted LSB spatial domain-embedding scheme. This involved the creation of a stego key to partition an image within a pixel range (0–255). The scheme, which updates a fixed number of bits inserted in the LSBs of the image, features five variant gray-level ranges of an image, each with a unique relationship. However, the scheme's potential is somewhat limited by its inability to conceal additional signature bits along with the hidden message for integrity purposes.

Castiglione et al. [26] formulated the cryptographic hash function HMAC-SHA-512 and an authenticated key exchange to propose a valuable authentication approach between two entities in the same year. Despite the well-structured methodology claimed, the processing cost of HMAC remains very high and, therefore, inefficient with respect to processing time, as illustrated in Subsect. 5.2. Combining a biometric key with a cryptographic hash function to formulate a good one-time message/image document authentication scheme was proposed in 2016 by Abduljabbar et al. [27]. This work resulted in a one-time authentication code. The cover image-based steganography anonymity is used to conceal the summation of the MACLESS code. One-time random pixel sequences generated by Rivest Cipher 4 and a one-time bio-key to generate MACLESS anonymity are merged to secure the concealing process. However, the susceptibility of this approach to malicious manipulation was not clarified, and whether this could be reliably

detected within a message/image document. For secure (M2M) communication within the IoT with a secure E2E M2M message delivery function, Chen et al. [8] outlined a methodology in the same year. However, the high symmetric key cryptographic negotiation function overhead problem is known to increase processing cost. In addition, issues with key exchange generation function are likely to require addressing. Furthermore, this approach does not assist with authentication code for SDs in the IoT-cloud.

In 2018, Lulian et al. [28] proposed a QR-based low-complexity protocol for lightweight authentication. Unfortunately, this method requires a secure channel to always transmit the authentication code, which is TLS. The difficulty of providing this secure channel in real-world applications is a significant challenge. Also, the method of generating the random number used with the QR code to generate the authentication has not been disclosed. Perhaps the attacker was able to generate the same number and thus generate the same authentication code.

In 2021, Mittal et al. [29] proposed secure techniques based on steganography to secure the sensitive data of bank clients. These techniques hide messages encrypted by a homomorphic cryptographic algorithm while QR is used as a cover image. This method cannot be used with constrained resource devices, as it uses an encryption algorithm with a very high computational cost. In addition, the size of the banking data to be encrypted may be large and require a long time to hide it.

In 2023, Devi et al. [30], to the problem of the production and distribution of goods and their counterfeit by many people and to distinguish between original and imitation goods, the authors proposed a method to verify the legitimacy of the products by mobile of the customer via scan QR code. QR code is generated from the hashing of the product and manufacturing address. The limitations of this method are that the address can be known, and the same hash can be used to generate the same QR code and deceiving the consumer in a simple way.

In 2024, Elizabeth et al. [31] proposed a two-factor authentication code based on QR and RSA a method known for its robust security. The data of the user is encrypted using RSA and a QR code is then generated from this cipher data. However, this method, while secure comes with a significant computational cost, primarily due to the use of RSA which may limit its application on light devices.

Most significantly, none of the approaches detailed above have addressed the requirement for a secure MAC mechanism for SDs in the IoT-cloud, and the privacy of messages is unprotected when transmitted between the S and R corresponding to SDs. The solution proposed in this paper constitutes a secure lightweight approach that could be implemented as part of a cloud-based MAC within the IoT-cloud environment for SDs using simple cryptographic primitives and QR coding. This approach enables the IoT-cloud to be considered a newer, more flexible and efficient version of the IT cloud. The scheme proposed in this paper has high-level security, and it could prevail against malicious attacks without entailing the additional costs associated with other MAC schemes. The approach relies on the strategy of hiding data in images: MAC bits are embedded with the LSB to ensure integrity, whereas the message is randomly scattered and encoded into a QR code image called QR_Image to maintain privacy. User message anonymity, secure session key agreement, one-time message code for each user's login, data integrity and

preservation of privacy of the user's message, representing many security benefits conferred by this scheme. Conducted results obtained clearly demonstrate that this approach is efficient, lightweight, and sturdy. The security parameters of the work suggested in this study is contrasted with those of six other comparable schemes in Table 1 below.

Table 1. Comparison of Authentication Schemes

Feature	Our Scheme	[20]	[21]	[22]	[23]	[26]	[27]	[28]	[29]	[30]	[31]
C1	√	√	×	×	×	√	√	×	×	×	√
C2	√	√	×	×	√	×	√	√	√	√	√
C3	√	×	×	×	√	√	√	×	√	×	√
C4	√	×	×	×	×	√	√	√	×	×	×
C5	√	×	×	×	×	×	×	×	×	×	×
C6	√	×	×	√	×	×	×	×	√	×	×
C7	√	×	×	×	×	×	×	√	√	√	√
C8	√	×	×	×	×	×	×	×	√	×	√
C9	√	×	×	×	×	×	√	×	×	√	×

C1: Nonce key; C2: Nonce message; C3: Key agreement; C4: Secure channel; C5: IoT-cloud; C6: Use of steganography with authentication code; C7: QR code; C8: Protecting the privacy of messages; Low-complexity.

3 Primitives and Requirements

During our approach's construction, significant cryptographic primitives are briefly outlined for transparency.

3.1 LSB

The LSB strategy is one of the most basic strategies influencing safe data transmission. This strategy relies on exchanging the LSB of the binary series of each digitized audio/text/image file sample with the binary relating to the user's secret message [7, 20, 32].

3.2 Hash Functions

The SHA family is a group of cryptographic hash functions outlined by the National Institute of Standards and Technology (NIST). SHA-0, published in 1993, is the first member of SHA. SHA-1, published in 1995, is a modified version of SHA-0. To ensure a slightly altered message and enhanced output ranges, the next four irregular models, i.e., SHA-22, SHA-256, SHA-384, and SHA-512, were issued by NIST. However, SHA-1 remains recalcitrant to malicious attacks, even if it runs on digital message blocks constituting n-bits for a 160-bit digest [33, 34].

3.3 QR Code

A QR code is a category of the 2D array barcode, which could be read much more rapidly than old-style Universal Product Code barcodes. As the latest trend, QR codes are currently an extremely fashionable technology. The codes are becoming increasingly ubiquitous with their wide application throughout e-business promotions, such as discount coupons, announcements, and resource chain management, and in areas far outside their original intended use states, such as tracking automobile portions in the auto/industrial industry.

QR codes enable a low cost, basic, easy, and safe technique to transfer data in a "push" design to individuals with suitable QR code-reading devices. Open-source libraries generate QR codes from various data sources with the only constraint being that the data is appropriate to a stable number of letters (alphanumeric strings) according to the review version of the QR code. Therefore, if a program can read any particular adaptation of the QR code data, then the individual program or app may also detect how the information is held after it is removed from the QR code. Such a scenario basically facilitates a smartphone application to analyze the received data and then to use this information in any method required by the programmer.

Given that each code modification has its own standards for data integrity, authority, idleness, and availability, the codes applicable to any smartphone operating system can function as the encode/decode public library provided the reconsiderations given by the application [34]. In addition, the advantages of the QR code can be summarized as follows [34]:

- Large capacity for data storage;
- Wide variety of data type for encoding;
- Strong error correction capability, in which even if it is part of the corrupted the QR code, then content is still obtained with a decoder.
- 360° readability, in which smart device users are enabled to read the QR image patterns from different angles to obtain data;
- Hypervelocity writing and reading, wherein SDs users can use the QR decoder to obtain the data embedded in the QR code. Such mechanism is faster compared with the traditional means of manually writing data.

4 Proposed Scheme

The S (S), R (R), and the cloud service provider (CSP) are the components of our proposed scheme. We employ a one-time configuration phase when applying the proposed method. However, the subsequent authentication phase is ongoing, allowing the S/R to actively participate whenever they wish to transmit a message via a smart device. Secure messaging with lightweight MAC for SDs in the IoT-cloud are detailed below.

4.1 Configuration Phase

This phase provides the cover image (Im) and the secret key Sk to the S's and R's SDs via the secure channel; both S and R register their identities in the CSP in the initial

configuration phase. The symmetric key *Sk* is employed by the main components (CSP, S, and R) for the cryptographic hash function h(.). The CSP uses two large primes p and q to sets up the secret key $Sk \in Zn$, where $n = p \times q$.

Subsequently, the CSP sends the crucial covert information (*Sk, Ims, Imr*; where *Ims* = *Imr*) via the secure channel to the S and R. The subsequent authentication phase does not require this operation; it is only necessary for the configuration phase. At runtime, no CSP is needed, making the process even simpler. The S/R may use the secret key *Sk* and (*Ims, Imr*) on completion of the configuration phase, to complete the subsequent authentication phase.

4.2 Authentication Phase

Below are the steps that describe the authentication phase.

Figure describes the authentication phase is described below.

1. $S \rightarrow R$: *StegoMAC* and *QR_Image*. *S* conduct the steps below:

- The M is assumed to be the S's message.
- To prevent the S from resending a previous authentication message to the R or vice versa, the $r_i \epsilon Im_s(Index)$ as the random number is generated as is the one-time anonymous MAC $M' = h(M||Sk||r_i)$.

  Afterwards, from the S's image the position P_i of r_i is computed by S.
- S generates a one-use scattered key ($SSk = r_i \times Sk$) for each user's authentication and integrity login request.
- S uses the scattering function $Sc_{SSk}(M) \rightarrow M_1$ for one use, randomly scattering the characters of M by utilizing *SSk*. Significantly, *Sc* relates to a function that utilizes *Rivest Cipher 4* (RC4) [29] to acquire one-use permuted sequence bytes of M. Specifically, the RC4 provides one-use permutation sequences, which is initialized with the *SSk* as a one-use scattered key. For instance, the RC4 offers the generated sequences with a repetition cycle of 10^{100} as a well-known cryptography algorithm. The security of this property is that it disables an attacker from retrieving and reassembling M correctly. Hypothetically, if the adversary detects the old secret keys *SSk* or M' authentication code, then a replay attack cannot be carried out on the subsequent authentication and integrity session.
- $P'_i = P_i \oplus Sk$ is generated.
- S keeps an array of location *ALO* of scattered M; $ALO = \left(L_{k(1)}, L_{k(2)}, L_{k(3)}, \ldots\right)$ for all $k \epsilon K$, where a set of all permutation spaces is represented by K.
- The S utilizes the LSB algorithm to conceal M' and *ALO* inside Im_s, generating the covered image known as *StegoMAC*. Therefore, to maintain the integrity of the request process and minimize the transmission overhead, only the *StegoMAC* that should be transferred between the S and R is required.
- The QR code is generated based on M_1, P'_i, and Im_s to acquire the QR code image called $QR\_Image = QR(M_1, L'_i, Im_s)$. The generation and reading functions of the QR code are inherently applicable to the strategy outlined. In addition, attackers fail to use the QR apps offered in the Apple App Store/Google play to retrieve correct information from the QR image as the S's message M is an

anonymous message. This property provides the advantage privacy-preserving for E2E messages delivered over the IoT-cloud.
- *QR_Image* and *StegoMAC* are submitted to *R*.

2. *R* follows the steps below to confirm the integrity and authentication of the message:
   - P_i' and M_1 are recaptured from the *QR_Image* according to the details obtained via the QR-reader application.
   - RP and M' are recaptured from the *StegoMAC* through the LSB algorithm.
   - R rearranges the message M_1 using the rearrange function $Re_{RP}(M_1) = M$ according to the sequence arising from $ALO = \left(L_{n(1)}, L_{n(2)}, L_{n(3)}, \ldots\right)$. The rearrangement of M_1 is concomitantly the reverse of the scattering process.
   - $L_i'' = L_i' \oplus Sk$ is calculated, and r_i' is extracted based on $r_i' = Im_r\left(L_i''\right)$. Then, the $M'' = h(M||Sk||r_i')$ is generated by *R*. Lastly, the *R* validates the authority and integrity of the *S*'s message if M'' matches M'. Otherwise, *R* terminates the authentication phase.

Basically, the strategy proposed utilizes effective and practical cryptographic primitives. It consists of fundamentally simple operations that can be employed in devices with limited processing capabilities, such as mobile SDs. The low E2E complexity is primarily attributed to two significant factors: first, the efficiency of the cryptographic primitives and LSB utilized and second, the functionality of the QR in carrying secure messages and MACs between SDs. Furthermore, the proposed scheme is applicable to a wide variety of scenarios without modification.

5 System Evaluation

Theorem 1. Our scheme can resist rlay attack.

Proof. An adversary accomplishes a replay attack by eavesdropping on the login message, which has been sent by the legitimate S to the R. Subsequently, the adversary reuses this message to impersonate the legitimate S or R when logging into the system in the next session. Under our proposed scheme, each new request initiated by the S/R should be identical to the *CSP*'s keys (Sk, r_i, P_i', Im_s). Therefore, an adversary cannot pass any replayed message to *R* for authentication. Results showed that the scheme will also function to resist this attack without synchronization clocks. Therefore, in the proposed secure E2E message, attackers cannot tamper with messages because they are unaware of the symmetric key Sk kept by *S* and *R*, and the distinct random r_i that is used in place of a timestamp. Furthermore, the covert variables (r_i, P_i') are employed once for each login message request by the S/R. This results in the requirement for the corresponding SDs of *S* and *R* to run the authentication phase as described above, with the result that any adversaries seeking desirable this type of relay attack will be detected by *R* and the attack would be unsuccessful.

Theorem 2. Prevention of forgery and parallel-session attacks.

Proof. If an adversary attempts to impersonate the S/R, the access to a valid session message (M, *StegoMAC*, Pi') through secret parameters (Sk, ri, Ims/Imr, *and* Pi') will

be required. Given that the attacker will not possess any knowledge of *Sk* or *Ims/Imr*, required to calculate StegoMAC, M', and Pi′, this type of attack will be averted.

Theorem 3. Prevention of insider attack.

Proof. Any user wishing to register with the CSP for remote-access services has to provide identity information. Acquiring the user's *MAC* from the cover image *StegoMAC* is considered unfeasible for the CSP due to the utilization of the secret key *Sk*, authenticated sessions keys (*ri, Pi*), and one-way hash function *h(.).* Furthermore, the primary values (*StegoMAC*, M', *ri*, *and Pi*) are generated only once for each login request by a user. This means that even the service provider is ignorant of the user's main values (*StegoMAC*, M', *ri*, *and Pi*). The scheme proposed can therefore avert insider and *CSP* impersonation attacks.

Theorem 4. Prevention of reflection attack.

Proof. This form of attack happens after legitimate users submit their login message to the *CSP*. The adversary attempts to obtain the user's login message and sends it (or an updated version of the message) back to the same user. In the proposed scheme, the adversary will fail to deceive the service provider due to inability to use the main values (*StegoMAC and Pi*) sent from the *S* to *R*. The adversary will be unable to use these values again since they are generated only once for each login request by the *S/R*. The scheme proposed can therefore avert reflection attacks.

Theorem 5. Prevention of MITM attack.

Proof. Between the S and the R, this form of attack can effectively intercept messages; then, when the entity logs out of the CSP, these messages are used by the attacker. The variables sent from the *S* to the *R* are securely encrypted in this proposed work and vice versa. As a session request from the *S* to *R* the *R*, to create nonce sensitive data $(StegoMAC, M', Ims/Imr, ALO, and\ Li')$, the random value *ri* is generated by the S for further security. When the S/R signs off from the CSP CSP, these nonce-sensitive variables become useless. Therefore, this variable *ri* is used only once, while an attacker identifies messages between the *S* and *R* to learn *ri*. The M' is hidden in the cover image called *StegoMAC* after nonce generated, therefore, it is impossible for the attacker or adversary is impossible to derive M′. Thus, MITM attack is averted by the proposed scheme.

Theorem 6. Prevention of off-line guessing attack.

Proof: This form of attack involves methodically checking all possible login values until the correct value is identified. Under the proposed scheme, an eavesdropper does not possess the primary authenticated parameters (*Sk and Ims/Imr*) produced during the configuration phase through the CSP via a secure channel to generate the valid M*AC* M'. Therefore, the authenticated parameters used by the *S* and *R* are difficult to guess. In addition, the initial configuration phase is used only once before it is discarded. This limits the time before expiration. Furthermore, in the authentication phase, the attacker cannot guess the *MAC* M' parameter as the necessary one-time random number $ri \in Ims(Index)$ to reassemble this secret information will be unknown. Thus, it is impossible to reuse the random number, as it is no longer valid after its first usage. Consequently, the

R will not respond unless confident of the correct M' of the *S*. Therefore, the proposed scheme can circumvent information disclosure via the strict communication protocol that is set up between the *S* and *R*. Therefore, the proposed scheme can avert off-line attack.

Theorem 7. Prevention of DOS attack.

Proof: This form of attack typically attempts to prevent or inhibit the services of all communication facilities and resources. In such an instance, the authentication system permits a password or a key change by a legitimate user. This process is vulnerable to DOS attack. Under the proposed scheme, the one-time position *Pi* of *ri* is generated from the *S's* and *R's* image independently by *S* and *R* without necessitating any interaction. Furthermore, the proposed scheme does not utilize a central component in the authentication phase; alternatively, the *CSP* is employed only once in the configuration phase and is then discarded. Therefore, our scheme is unsuitable for targeting by DOS attack.

Theorem 8. Prevention of online key-guessing attack.

Proof. This form of attack involves attempts to corrupt communication processes by utilizing an online key-guessing attack to obtain *Sk*. Such an attack will be unsuccessful because *Sk* is shared between *S* and *R* corresponding *SDs* during the configuration phase through the *CSP* via the secure channel. Therefore, to predict the corresponding *Sk* of both *SDs*, the attacker will need to pass the configuration phase. Given that the corresponding Sks are only retained by the corresponding *SDs* of *S* and *R*, the proposed scheme can robustly combat and avert online key-guessing attack.

Theorem 9. Prevention of message privacy attack.

Proof. Previous research has shown that messages are unprotected when transmitted between *S* and *R* corresponding *SDs* [18–27]. In particular, attackers can utilize a malicious smart device in the IoT-cloud to pick up any communication transmitted between *S* and *R*. In the proposed scheme, the message is protected with a scattering function $ScSSk(M) \rightarrow M1$ resulting in one-time random scattering of the characters of *M* by using the one-time scatter key *SSk* and *RC4*. Additionally, *M1* is hidden inside an image QR_Image, which means that attackers can only see a non-meaningful QR_Image. Therefore, the proposed scheme can easily avert message privacy attack.

Theorem 10. The propose scheme can support of user's message anonymity.

Proof. If a *S/R* attempts to resend a previously sent message while an attacker is eavesdropping on the *S's* login request, then the attacker will not be able to utilize the identical *MAC* M' as the S. This *MAC* M' is concealed within the *S*'s image *Ims* to generate a cover image called *StegoMAC*. Simultaneously, the *S* produces *ri* once for each request by the *S*. Therefore, *ri* is extracted from the *S's* image $ri \in$ Ims, which exists only in *R* and S *S*. Furthermore, an attacker will not have access to the primary keys (*Ims, Imr, Sk, and ri*) with which to generate the cryptographic hash function $M' = h(M||Sk||ri)$. Therefore, an attacker cannot easily procure the *S's MAC*. The proposed scheme is clearly supportive of the user's message anonymity during communications.

Theorem 11. Promotion of known-key security and session key agreement.

Proof. In the proposed scheme, when the S sends messages to the *R* or vice versa, the secret key *Sk* is used to generate $M' = h(M||Sk||ri)$. The same key is also utilized to encrypt the position *Pi* of *ri* within the *S's* image *Ims*. An attacker will not be able to access the session keys, and therefore obtain fresh values of *Sk*, which is only generated in the configuration phase by the *CSP* via the secure channel. Therefore, the attacker will not be able to obtain these secret parameters and key security is maintained.

Theorem 12. Protection of S/R QR code.

Proof. The function of the *QR* code in the proposed scheme is vital because it contributes to protecting the *S's/R's* message without divulging the existence of any other information within the IoT's entities in the communication channel. Therefore, the S sends the *QR_Image* with the concealed *StegoMAC* to the *R*. The *QR_Image* is also generated on Pi on a one-off basis for each authentication phase, thereby circumventing an attacker from acquiring any advantage by sniffing or activating an *MITM* attack through the *QR_Image* and *StegoMAC* (see Table 2). Furthermore, the proposed scheme does not incur additional cost for reading and generating the *QR* code since the mobile application for reading *QR* codes is free in the Apple App Store and Google Play. Thus, our scheme supports an inexpensive means of retrieving Pi' and *M*, that are subsequently used to validate the user's message. The mobile application can be installed in any IoT device, such as a smartphone, tablet, or laptop. Therefore, the proposed scheme can maintain *E2E* message transmission and privacy without the additional hardware requires.

Theorem 13. Maintenance of message integrity.

Proof. In the circumstance where an adversary attempts to extract or change the message M embedded within an image *QR_Image* before sending it again to the *R*, the *R* will verify the integrity of the *S's* message by generating M'' and comparing it with M′. The adversary will fail to implement his or her attack because if the results do not match, the *R* will confirm that the message does not have integrity. The proposed scheme can clearly maintain and support message integrity.

Theorem 14. Support of user anonymity.

Proof. If an attacker attempts to eavesdrop on the user's authentication and integrity request, the user's login request and identity will not be available from *M* since it is protected via a scattering function $ScSSK(M)$ based on a one-off scatter key *SSk*, that is concealed from the attacker and generated only once for each user's login request. Therefore, an attacker will have difficulty determining the user's authentication request and identifying or reassembling the message *M*. The proposed scheme is clearly supportive of the anonymity of the user's authentication request.

Table 2. QR Code for Each Authentication Phase

Message	P_i'	Cryptographic hash()	QR Code
Basra	1234567	9c59b55a530e18407064e7 749fb5329895353997	
Iraq	6257890	4a1022e3027ff38799505e ea2d083e6fcd54da46	
China	7866543	476114bda8cb89511ccf8f 2195ba1befe0f9100a	

5.1 Discussion

Conventional security solutions are susceptible to a range of attack mechanisms [7, 8] and are inapplicable to SDs that work in the IoT-cloud. The suggested functions of the lightweight MAC and secure message characteristics are proposed to enable secure E2E communications. These communications include the lightweight secure exchange key agreement between two or more SDs in the IoT-cloud and also secure E2E message transmission. Enhancement of the message delivery function in the IoT-cloud is a recent development. The lightweight MAC can be used by a pair of SDs for an E2E communication user session. It can permit greater adaptability for a device with limited processing power such as a smartphone. Furthermore, successful prevention of a wide range of attacks has been demonstrated by the security analyses above. Therefore, the proposed scheme is perceived to meet the basic security requirements of the communication between E2E SDs mentioned in [8].

5.2 Experimental Results

Given that conventional security schemes are not lightweight, they are not applicable for E2E SDs in the IoT-cloud environments. Several experiments to evaluate the efficiency and effectiveness of the proposed scheme are evaluated below. Trial messages with small sized images of 512 $\times$ 512 pixels are chosen to demonstrate the performance characteristics of the proposed lightweight and secure scheme. All experiments are conducted on a PC with a 2.40 GHz Cori 3, a Windows 10 operating system of 64-bits, 4 GB of RAM, and Matlab R2008a.

Performance Investigation

Figure 1 depicts the processing time of the authentication phase. The average time for the authentication phase in the proposed scheme is 0.0682 s for each user, demonstrating that the proposed solution is fast and lightweight.

Figure 2 presents the authentication process time of the scheme achieved by Castiglione et al. [26]. Despite utilizing a strong HMAC-512 function in their study, their approach still suffered from high processing costs related to such function. Furthermore, their complex key management mechanism requires many complicated cryptographic procedures. The evident differences in processing times between the schemes proposed in this paper and that of Castiglione et al. are illustrated in Figs. 1 and 2. To be precise, a much shorter processing time can be seen for the scheme proposed in this paper. The average time for the authentication phase of each entity (containing the S and R entities in the IoT-cloud environment) is 0.0682 s, whereas that in the scheme reported by Castiglione et al. is 0.2754 s. The estimation parameters are summarized in Table 3. The time requirement of the scheme proposed in the present paper is again small, as shown in Table 4.

The effectiveness of the proposed scheme is tested in term of authentication accuracy. Experiment results of 3000 SDs users show that the scheme has 100% accuracy.

Table 3. Estimation Parameters

Symbol	Definition
T_h	Time processing of a hash function
T_{Xor}	Time processing of the Xor function
T_{Opr}	Time processing of mathematical operations, such as multiplication, addition, and subtraction
$T_{\|\|}$	Time processing of the concatenation function
T_R	Time processing of randomly scattering the message
T_{EM}, T_{EX}	Time processing of embedding and extracting data, respectively
T_{QREn},T_{QRDe}	Time processing of QR encoder and QR decoder, respectively

Table 4. Estimation Parameters

Phase	CSP	S	S
Setup and Registration	$2T_{Opr}$	-------	-------
Authentication	-------	$T_h + 5T_{Opr} + 2T_{\|\|} + T_{Xor} + T_R + T_{EM} + T_{QREn}$	$T_h + 3T_{Opr} + 2T_{\|\|} + T_{Xor} + T_{EX} + T_{QRDe}$
Total	$2T_{Opr}$	$T_h + 5T_{Opr} + 2T_{\|\|} + T_{Xor} + T_R + T_{EM} + T_{QREn}$	$T_h + 3T_{Opr} + 2T_{\|\|} + T_{Xor} + T_{EX} + T_{QRDe}$

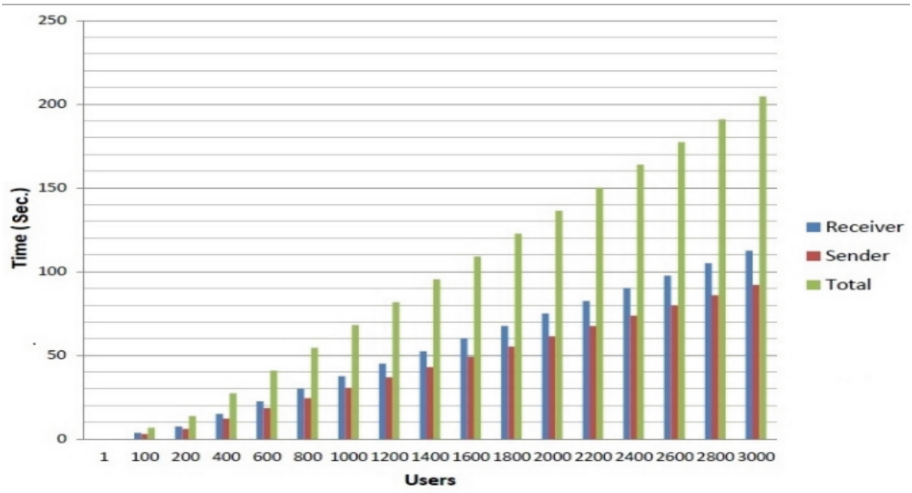

Fig. 1. Performance of the proposed scheme

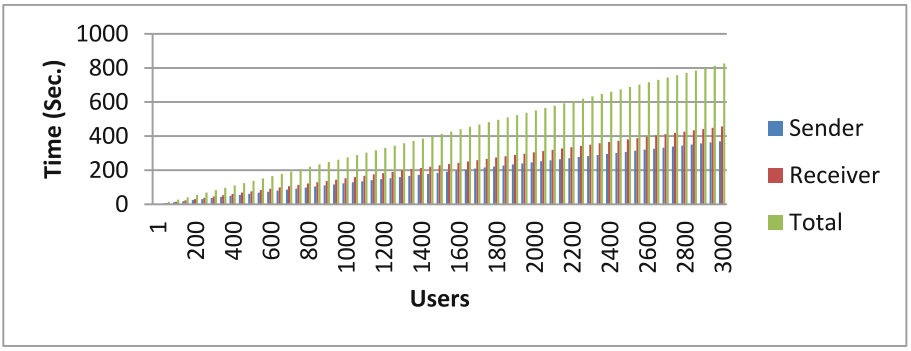

Fig. 2. Performance of the scheme of Castiglione et al. [26]

6 Conclusion

This paper demonstrates that the field of authority, integrity, and privacy-preserving validation of messages in the IoT-cloud environment is a burgeoning subject that draws increasing research attention. Currently, a significant number of relevant studies have been reported, and the IoT-cloud environment has become a rapidly expanding field. As a result of this expansion, authority and authentication techniques are anticipated to continue to grow together as the IoT-cloud and Big Data applications expand in determining innovative solutions to ever-present security challenges, despite the remarkable progress of research to date. In the scheme proposed, lightweight MAC and QR code are utilized in conjunction with randomization and steganography to facilitate the ability of SDs

to communicate securely with each other in the IoT-cloud environment and to secure E2E message delivery. QR code processes do not require extra hardware, and therefore, costs are minimized as the software is free in the Apple App Store and Google Play. The experimental results of the proposed scheme demonstrate that the findings cannot only progress the interconnectivity of the IoT-cloud entities, it can also attain a good balance between security and performance. The proposed scheme has many significant security features, including key management, user one-time key, one-time authentication code, user message integrity, and resistance to well-known malicious attacks, such as MITM, insider, and replay attacks. Additionally, the proposed lightweight MAC and secure message scheme will satisfy the basic requirements for message security via SDs in the IoT-cloud.

References

1. Al Sibahee, M.A., Lu, S., Abduljabbar, Z.A., Liu, X., Abdalla, H.B., Hussain, M.A., et al.: Lightweight secure message delivery for E2E S2S communication in the IoT-cloud system. IEEE Access **8**, 218331–218347 (2020). https://doi.org/10.1109/ACCESS.2020.3041809
2. Abduljabbar, Z.A., et al.: Privacy-preserving image retrieval in IoT-cloud. In: 15th International Conference on Trust, Security and Privacy in Computing and Communications, Tianjin, China, February 2017, pp. 799–806. IEEE Press (2017). https://doi.org/10.1109/TrustCom.2016.0141
3. Ali, Z.A., et al.: A provably secure anonymous authentication protocol for consumer and service provider information transmissions in smart grids. Cryptography **8**, 20 (2024). https://doi.org/10.3390/cryptography8020020
4. Al Sibahee, M.A., et al.: Efficient encrypted image retrieval in IoT-cloud with multi-user authentication. Int. J. Distrib. Sens. Netw. **14**(2) (2018). https://doi.org/10.1177/1550147718761
5. MobiThinking: Global mobile statistics 2014 home: All the latest stats on mobile web, apps, marketing, advertising, subscribers, and trends: Smartphone shipments/forecasts by operating system market share (2014). http://mobithinking.com/mobilemarketing-tools/latest-mobile-statsAugust
6. Ennesser, F., Ganem, H.: Establishing security in machine-to-machine (M2M) communication devices and services. In: Machine-to-Machine (M2M) Communications, pp. 227–248. Elsevier (2015). https://doi.org/10.1016/B978-1-78242-102-3.00013-7
7. Nyangaresi, V.O., Abduljabbar, Z.A., Al Sibahee, M.A., Abduljaleel, I.Q., Abood, E.W.: Towards security and privacy preservation in 5G networks. In: 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia, pp. 1–4 (2021). https://doi.org/10.1109/TELFOR52709.2021.9653385
8. Chen, H.C., You, I., Weng, C.E., Cheng, C.H., Huang, Y.F.: A security gateway application for End-to-End M2M communications. Comput. Stand. Interfaces **44**, 85–93 (2016). https://doi.org/10.1016/j.csi.2015.09.001
9. Al Sibahee, M.A., et al. (eds.): Promising bio-authentication scheme to protect documents for E2E S2S in IoT-cloud. In: 2020 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). IEEE (2020). https://doi.org/10.1109/ICSPCC50002.2020.9259519
10. Abduljabbar, Z.A., et al.: Towards efficient authentication scheme with biometric key management in cloud environment. In: The 2nd IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2016), New York, USA, pp. 146–151 (2016). https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.25

11. Hsing-Chung, C., Cheng-Ying, Y., Hui-Kai, S., Ching-Chuan, W., Chao-Ching, L.: A secure e-mail protocol using ID-based FNS multicast mechanism. Comput. Sci. Inf. Syst. **11**(3), 1091–1112 (2014). https://doi.org/10.2298/CSIS130924066C
12. Abduljabbar, Z.A., et al.: SEPIM: secure and efficient private image matching. J. Appl. Sci. **6**(8), 1–21 (2016). https://doi.org/10.3390/app6080213
13. Abduljabbar, Z.A., Jin, H., Ibrahim, A., Hussien, Z.A., Hussain, M.A., Abbdal, S.H., et al. (eds.): Secure biometric image retrieval in IoT-cloud. In: 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). IEEE (2016). https://doi.org/10.1109/ICSPCC.2016.7753617
14. Isa, M.A.M., Ahmad, M.M., Sani, N.F.M., Hashim, H., Mahmod, R.: Cryptographic key exchange protocol with message authentication codes (MAC) using finite state machine. Procedia Comput. Sci. **42**, 263–270 (2014). https://doi.org/10.1016/j.procs.2014.11.061
15. Attwood, A., Lamb, D.J., Abuelmaatti, O.: Position-relative identities in the Internet of Things: an evolutionary GHT approach. IEEE Internet Things J. **1**(5), 497–507 (2014). https://doi.org/10.1109/JIOT.2014.2353194
16. Hussien, Z.A., Jin, H., Abduljabbar, Z.A., Hussain, M.A., Yassin, A.A., Abbdal, S.H., et al. (eds.): Secure and efficient e-health scheme based on the Internet of Things. In: 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). IEEE (2016). https://doi.org/10.1109/ICSPCC.2016.7753621
17. Al Sibahee, M.A., Lu, S., Hussien, Z.A., Hussain, M.A., Mutlaq, K.A.-A., Abduljabbar, Z.A.: The best performance evaluation of encryption algorithms to reduce power consumption in WSN. In: 2017 International Conference on Computing Intelligence and Information System (CIIS), Nanjing, China, pp. 308–312 (2017). https://doi.org/10.1109/CIIS.2017.50
18. Swaminathan, A., Mao, Y., Wu, M.: Robust and secure image hashing. IEEE Trans. Inf. Forensics Secur. **1**(2), 215–230 (2006). https://doi.org/10.1109/TIFS.2006.873601
19. Rabadi, N.M., Mahmud, S.M.: Drivers' anonymity with a short message length for vehicle-to-vehicle communications network. In: 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), USA, pp. 132–133 (2008). https://doi.org/10.1109/ccnc08.2007.36
20. Jamil, N., Aziz, A.: A unified approach to secure and robust hashing scheme for image and video authentication. In: 3rd IEEE International Congress on Image and Signal Processing (CISP 2010), China, pp. 274–278 (2010). https://doi.org/10.1109/CISP.2010.5648278
21. Liu, Z., Lallie, H.S., Liu, L., Zhan, Y., Wu, K.: A hash-based secure interface on plain connection. In: 6th IEEE International ICST Conference on Communications and Networking in China (CHINACOM 2011), China, pp. 1236–1239 (2011). https://doi.org/10.1109/ChinaCom.2011.6158347
22. Naqvi, S.I., Akram, A.: Pseudo-random key generation for secure HMAC-MD5. In: 3rd IEEE International Conference on Communication Software and Networks (ICCSN 2011), China, pp. 573–577 (2011). https://doi.org/10.1109/ICCSN.2011.6014790
23. Chaisri, C., Mettripun, N., Amornraksa, T.: Facsimile authentication based on MAC. In: Park, J., Arabnia, H., Chang, H.B., Shon, T. (eds.) IT Convergence and Services. LNEE, vol.107, pp. 613–620. Springer, Dordrecht (2011). https://doi.org/10.1007/978-94-007-2598-0_66
24. Singh, A.K., Sharma, N., Dave, M., Mohan, A.: A novel technique for digital image watermarking in spatial domain. In: 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC 2012), USA, pp. 497–501 (2012). https://doi.org/10.1109/PDGC.2012.6449871
25. Maleki, N., Jalali, M., Jahan, M.V.: Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function. Egypt. Inform. J. **15**(2), 115–127 (2014). https://doi.org/10.1016/j.eij.2014.06.001

26. Castiglione, A., Di Santis, A., Castiglione, A., Palmieri, F.: An efficient and transparent one-time authentication protocol with non-interactive key scheduling and update. In: 28th IEEE International Conference on Advanced Information Networking and Applications (AINA 2014), Canada, pp. 351–358 (2014). https://doi.org/10.1109/AINA.2014.45
27. Abduljabbar, Z.A., et al.: Robust scheme to protect authentication code of message/image documents in cloud computing. In: International Conference on Computing, Networking and Communications (ICNC 2016), USA, pp. 1–5 (2016). https://doi.org/10.1109/ICCNC.2016.7440585
28. Aciobanitei, I., Buhus, I.C., Pura, M.L.: Using cryptography in the cloud for lightweight authentication protocols based on QR codes. In: 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, pp. 539–542 (2018). https://doi.org/10.1109/SACI.2018.8440949
29. Mittal, S., Kaur, P., Ramkumar, K.R.: Achieving privacy and security using QR-code through homomorphic encryption and steganography. In: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), Noida, India, pp. 1–6 (2021). https://doi.org/10.1109/ICRITO51393.2021.9596265
30. Devi, P.J., Dutta, M.S., Damerakonda, M., Gutti, D.N., Domakuntla, S.K.: One time QR-code for fake product identification. In: 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, pp. 583–588 (2023). https://doi.org/10.1109/ICIRCA57980.2023.10220784
31. Rani, E., Sakthimohan, M., Amuthaguka, D., Gnanapriya, P., Naveena, G., Ashok, A., (eds.): QR code-based login with robust RSA algorithm encryption. In: 2023 International Conference on Intelligent Technologies for Sustainable Electric and Communications Systems (iTech SECOM), Coimbatore, India, pp. 474–479 (2023). https://doi.org/10.1109/iTechSECOM59882.2023.10435118
32. Watters, P., Martin, F., Stripf, H.S.: Visual detection of LSB-encoded natural image steganography. ACM Trans. Appl. Percept. **5**(1), 5:1–5:12 (2008). http://doi.acm.org/10.1145/1279640.1328775
33. Paar, C., Pelzl, J.: Understanding Cryptography, pp. 293–319. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-04101-3
34. Hussien, Z.A., et al.: Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems. Appl. Sci. **13**(2), 691 (2023). https://doi.org/10.3390/app13020691