IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 January 2025, accepted 19 February 2025, date of publication 25 February 2025, date of current version 14 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3545769

RESEARCH ARTICLE

SMFA: Strengthening Multi-Factor Authentication With Steganography for Enhanced Security

AFJAL H. SAROWER[1], TOUHID BHUIYAN[2], MARUF HASSAN[3], MOHAMMAD SHAMSUL AREFIN[4], (Senior Member, IEEE), AND GAHANGIR HOSSAIN[5], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Daffodil International University, Dhaka 1216, Bangladesh
[2]School of Information Technology, Washington University of Science and Technology, Alexandria, VA 22314, USA
[3]Department of Computer Science and Engineering, Southeast University, Dhaka 1208, Bangladesh
[4]Department of Computer Science and Engineering, Chittagong 4349, Bangladesh
[5]Department of Information Science, University of North Texas, Denton, TX 76205, USA

Corresponding author: Afjal H. Sarower (afjal.cse@diu.edu.bd)

This work was supported by the University of North Texas and Daffodil International University.

ABSTRACT Traditional password-based authentication mechanisms exhibit significant security vulnerabilities, prompting the adoption of Multi-Factor Authentication (MFA) to enhance user verification. However, current MFA methods, such as OffPAD, One-Time Password Tokens (OTT), and smartcard-based systems, remain vulnerable to attacks like Man-in-the-Middle (MITM), session hijacking, replay, phishing, and denial of service (DoS). Additionally, the conventional single-server authentication approach is inefficient and inadequate for modern security needs. This study introduces Secure Multi-Factor Authentication (SMFA), a novel framework designed to address these challenges by leveraging steganography for secure credential transmission, reducing susceptibility to MITM and session hijacking attacks. SMFA also incorporates an additional Universal Serial Bus (USB) device as a supplementary authentication factor and employs a multi-server architecture to overcome the limitations of single-server models. A comprehensive analysis comparing SMFA to existing MFA protocols reveals its superior ability to counter MITM, replay, DoS, user impersonation, and password-guessing attacks. The results demonstrate that SMFA offers a robust and effective solution, addressing the weaknesses of both traditional password-based systems and current MFA methods.

INDEX TERMS User authentication, multi-factor authentication model (MFA), steganography, cryptography, privacy and security.

I. INTRODUCTION

Authentication plays a pivotal role in electronic systems by establishing the user's authenticity. This process involves the user proving their identity through three fundamental factors:

1) Something the user knows: This encompasses elements like the username, password, or specific questions directly related to the user, with answers known to the system.
2) Something the user has: This includes various items such as OTP, smartcards, NFC, and USB devices.
3) Something the user is: This refers to the user's biometric information, such as fingerprint, retina, and DNA, providing unique identifiers.

Collectively, these factors used to verify a user's identity are referred to as credentials. Despite the prevailing use of single-factor authentication, primarily based on usernames and passwords, this mechanism has raised security concerns since the late '70s [1] [2]. The primary vulnerability of the single-factor password-based system lies in password cracking through brute force and the risk of a user registering with the same password across multiple systems. Passwords are susceptible to compromise, as evidenced by numerous data breaches in recent years [3], [4], [5], [6], [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Alba Amato.

A notable breach in late 2018 exposed the data of 162 million users of a popular video messaging service [8]. Additionally, significant data leaks occurred in 2019, including 530 million user records, including Face ID, from Facebook [9], and 885 million user records from the First American Financial Corporation [27], [10]. These incidents underscore the vulnerability of passwords in safeguarding sensitive information.

In addition to Facebook, recent cyber-attacks have targeted other social media platforms like Linkedin and Sina Weibo, compromising a total of 1.2 billion records [11], [12]. Data breaches occur frequently due to inadequate security measures and policies. For instance, in 2022, a leak exposed data from 3 million patients, including SSNs, medical records, and sensitive information [13]. Given the security vulnerabilities inherent in traditional password-based systems, this research stems from the necessity of a robust authentication system.

Multi-factor authentication protocols combine numerous authentication elements to mitigate password flaws. Notably, FIDO's U2F [14] and Google 2-step [15] are two well-known multi-factor (mostly two-factor) authentication methods that have gained popularity. In particular, U2F makes use of a USB-based authentication system. These protocols are still vulnerable to frequent attacks like DOS and MITM, though. Additionally, various other authentication methods have emerged, offering specific advantages against types of attacks and security issues. Therefore, the primary concerns revolve around (i) verifying that the individual seeking access is the legitimate user and (ii) safeguarding the credentials. Thus, safeguarding user credentials during transmission over the network poses a significant challenge.

Securing the transmission of credentials plays a pivotal role in authentication, where cryptography and steganography stand out as crucial techniques. Steganography, an age-old method involving concealing data within a cover, effectively shields sensitive information [16]. In the digital realm, it utilizes images, videos, or audio files as cover objects [17]. While cryptography encrypts messages, steganography focuses on hiding their existence. Employing both ensures robust data security. Despite potential implementation expenses, industries such as banking and military networks favor steganography due to its high-security standards, making it a preferred choice for ensuring data security in authentication processes [18].

Previous studies have shown that adding a steganography system to the authentication procedure improves data security when credentials are being transmitted. Therefore, this study conducts a thorough investigation into incorporating steganography and cryptography into a newly structured authentication model. The aim is to address the security concerns stemming from conventional password-based systems. This paper contributes to the field in the following ways:

1) We carry out a thorough analysis of the entirety of research, highlighting critical weaknesses such insider threats, user impersonation, Man-in-the-Middle (MITM) attacks, and session key leakage. We present a multi-factor authentication paradigm that is intended to protect sensitive data that belongs to authorized users in order to address the security flaws in the protocols now in use.
2) We highlight the effective application of steganography to mitigate risks associated with critical attacks.
3) Burrows-Abadi-Needham (BAN) logic is used to assess the suggested authentication procedure in order to make sure it functions properly.
4) A thorough study backed up with declarations shows that the suggested protocol is secure from replay attacks, Man-in-the-Middle attacks, and other significant risks.
5) We undertake a comparison analysis, comparing the suggested protocol's security functionality and performance to previous research.

The structure of the paper is as follows: Section II delves into previous research in the relevant field. Section III outlines the proposed Multi-Factor Authentication (MFA) model, while Section IV encompasses discussion, analysis, and comparative results. Finally, Section V concludes the paper.

II. LITERATURE REVIEW

The initial phase of any secure and dependable transaction involves authentication. Conventional password-based methods play a predominant role in this crucial step to verify the user's authenticity. Simultaneously, advanced authentication mechanisms are gaining widespread adoption worldwide.

During this research, it was noted that previous investigations have explored steganography approaches and various types of multi-factor authentication mechanisms. The following section provides an overview of the relevant work conducted in this domain.

A. MFA MODELS AND PROTOCOLS

Numerous prior research endeavors have explored multi-factor authentication methodologies to verify user identities. For distributed wireless sensor networks, Das devised a three-factor authentication mechanism, claiming its resilience against certain common attacks [19].

Subsequently, Babu et al. scrutinized Das's protocol and identified its vulnerability to reply attacks and session-specific temporary information threats. An enhanced protocol addressing these shortcomings was proposed [20]. In another study [21], an authentication protocol for multi-server environments utilizing a two-factor system (password and smart-card) with RSA cryptography was presented. This protocol aimed to streamline complexities while fortifying security against known attacks. Validation showcased its effectiveness in mitigating recognized security threats. Additionally, the protocol facilitated session key agreement and mutual authentication, verified for correctness and session key freshness using the BAN logic model. Another work [22] introduced a robust three-factor mutual authentication protocol tailored for e-governance systems operating within multi-server environments. Its security was

substantiated through a comprehensive assessment involving informal security analysis, BAN logic, ROR model, and simulation via the AVISPA tool.

Shen J. et al. proposed a lightweight authentication system for cloud environments, leveraging XOR, string concatenation, and a hash function to reduce computational overhead on both client and server sides [23]. Meanwhile, Yang et al. introduced an ID-based user authentication, an enhancement of an existing scheme, and another authentication scheme for multi-server environments. However, these were designed for cloud settings, slightly escalating computational costs [24]. A concrete instance of an identity-based authentication technique was provided by Wang et al. and Das et al. [25], [26]. Although data transmission is not safe in the Wang et al. model, both models were suggested for correct user authentication. It is discovered that credentials are modifiable during transmission across the network in this regard. Das et al.'s methodology is likewise insecure since it allows for authentication bypassing without requiring any legitimate credentials. To get around the one-pass authentication process, Liu suggested the one-pass authentication and key agreement (AKA) approach [27]. Man-in-the-middle, session hijacking, and server spoofing attacks are just a some of the potential threats that Huang and Li discovered when they examined the AKA [28]. However, Tsay and Mjølsnes discovered a flaw that was open to internal and external attack [29].

B. MFA USING ADDITIONAL DEVICE

Over the past decade, numerous sophisticated methods have emerged, advocating the inclusion of an additional device to verify user authenticity. These approaches have prompted research studies advocating for the integration of smartcards, USBs, and supplementary online devices as an extra authentication factor. A multi-factor authentication system using a user ID, password, and smartcard was proposed by Choudhury et al. [30]. Nevertheless, smartcards are not appropriate for public cloud systems and have limited usability.

An MFA system using IMEI and OTP numbers as authentication secrets in mobile contexts was introduced by Kumar et al. [31]. The concept of OffPAD, initially introduced by Varmedal et al. [32] and detailed in 2005, aimed to manage and authenticate both service providers and user identities, particularly for online transactions to prevent MITM and phishing attacks. Subsequently, Alhaidary et al. conducted vulnerability analyses and proposed enhancements to address these issues [33]. In 2016, their investigation highlighted vulnerabilities in the OffPAD-based authentication model, suggesting techniques to mitigate susceptibilities [34], revealing its extreme vulnerability to replay and MITM attacks.

Bae and Kwak proposed an authentication scheme using smartcards within a multi-gateway IoT framework to reduce communication and computational overhead [35]. However, their scheme lacked resilience against several security threats, including traceability, impersonation, gateway node spoofing, and session key disclosure attacks, while also failing to provide secure mutual authentication.

Khan et al. developed a secure mutual authentication system for smart grid communication, employing biometric-based elliptical curve cryptography, ensuring user anonymity, defending against various attacks, and reducing transmission and computation costs [36]. In response to security challenges, Masud et al. devised a user authentication mechanism prioritizing lightweight implementation and user anonymity preservation [37].

Widely used Advanced Encryption Standard (AES) was used for data security in Hufstetler et al.'s implementation of a safe multi-factor authentication scheme that replaces authentication in the current Windows version through NFC [38]. However, limitations confined its use to Windows PCs, and security threats persisted in the authentication process.

To address security concerns and enhance functionalities, three-factor authentication protocols utilizing biometric information were proposed. Although user anonymity was not guaranteed, Liu et al. proposed a biometric-based single sign-on authentication mechanism for mobile cloud computing services [39]. Chen and Chen also suggested using three factors for authentication in e-health cloud systems, but the systems were still vulnerable to intractability and session-specific temporary information attacks [40], [41].

C. MFA USING STEGANOGRAPHY IN WEB

Authentication protocols play a pivotal role in facilitating secure data exchange and communication among system entities by leveraging cryptography [42]. According to Liu, these protocols primarily ensure key agreements, data security, non-repudiation, and multi-party computation [27]. Steganography has been explored in various research studies within web authentication, presenting an opportunity to enhance authentication mechanisms through its application. Combining steganography with cryptography offers a promising avenue to bolster data security and conceal sensitive credentials.

Studies have proposed combining hashing or encryption with steganography to accomplish strong data security in digital communications. Madhuravani et al. introduced a method utilizing dynamic hashing and steganography [43], highlighting the effectiveness of combining steganography with cryptography to deceive attackers. An authentication framework called imgAuth that uses picture steganography for user profile management and authentication was described by Gunawardena et al. [44].

Choudhury et al. proposed a method employing steganography and visual cryptography for secure information sharing between customers and merchant servers, prioritizing enhanced safety [30]. Tabassum et al. [45] showcased an improved version of the Kerberos protocol, integrating biometric templates and steganography to heighten security, while Motero et al. conducted a comprehensive analysis, demonstrating its exemplary effectiveness [46].

A safe authentication method for online purchasing systems was presented by Ihmaidi et al. [47]. This mechanism uses steganography and biometrics to hide login credentials. This method uses a particular steganography algorithm to encrypt credit cards and login passwords, putting them inside an image. Mantoro et al. described in detail how to use steganography techniques to hide text passwords within graphics [48]. Furthermore, in order to guarantee data security, Danuputri et al. introduced a prototype known as ste-Chy that combines the Vigenère cipher and LSB steganography for private authentication [49]. SHA-256 was applied in order to guarantee legitimacy. The study asserts that using steganography for online authentication greatly improves data security, although it focuses on the Android environment in particular.

Hence, it is evident that numerous initiatives and models have been put forth to enhance the security of authentication processes. Multi-Factor Authentication (MFA) emerges as a superior choice, providing a heightened security level compared to the single-factor authentication system. Additionally, the potential application of steganography in authentication is apparent, but it necessitates further examination. Previous research has separately delved into steganography and authentication models.

However, little research has been done on the combined use of steganography with multi-factor authentication. Steganography has been utilized in the e-commerce industry to secure credential transfer, and it has also been integrated by certain researchers into cloud authentication models. This work makes a contribution by developing a multi-factor authentication mechanism that transmits credentials securely by using steganography. This study focuses on the smooth integration of steganography with the authentication system, taking into account the following aspects when designing the model:

1) Employing cryptography for robust data protection.
2) When the transmitted packet contains several possible cover objects, steganography is used to hide the presence of credentials within a cover item. This method works well for deceiving attackers and extending the amount of time needed to decode secret credentials.
3) Designing the model to allow the use of two distinct servers to mitigate risks and enhance efficiency.

III. RESEARCH METHODOLOGY

Multi-factor authentication surpasses single-factor authentication methods in terms of providing enhanced security. Various organizations already implement specific MFA protocols or models. The subsequent discussion revolves around these existing MFA mechanisms.

A. BACKGROUND

1) OFFPAD

OffPAD serves as an offline personal authentication device specifically designed to empower users in securely managing online transaction authentication processes. Its primary objective is to oversee online identification procedures, effectively preventing MITM and phishing attacks. Initially detailed by Josang and Pope in 2005, this personal authentication device was subsequently improved upon by Vannedal et al., leading to the development of OffPAD [32]. The device's unique feature lies in its offline nature, predominantly operating with a secure element to ensure heightened security.

2) REMOTE USER AUTHENTICATION SCHEME USING SMART CARDS

Using EIGamal's public key cryptosystem, Hwang and Li suggest integrating a smart card into user authentication [50]. This system's security depends on how difficult it is to compute discrete logarithms in finite fields. It operates as a remote user authentication system without employing a password verification table. During registration, users link their smartcard with a password. Subsequently, an authorized user seeking system access must insert the card into the device along with their ID and password during login attempts.

3) GOOGLE 2-STEP

Google introduces a two-factor authentication method called Google 2-step [15]. Primarily phone-based, this scheme allows users to utilize their phones to validate logins. Google highlights on their website several reasons why relying solely on passwords for authentication isn't adequate, asserting that '2-Step Verification can help keep bad actors out, even if they possess your password'.

During login, a verification code is dispatched to the user's computer, which needs to be entered for access. An alternative version, the 'one-tap' variant, simplifies the process by prompting users to press a 'yes' button in a phone pop-up. This second version notably enhances usability compared to its predecessor.

4) FIDO

There is a FIDO authentication standard variant that use the U2F USB token as the second factor [14]. In addition to storing secrets, this U2F USB token may also include public keys. These keys are essential for carrying out cryptographic procedures. The USB token is notable for having a button that users must press in order to validate a transaction. On its website, it states that the public key is registered on the server, and the token creates a key pair that allows a website to enable second-factor authentication. The token can be used for authentication once this one-time procedure is complete.

Through this method, the computer communicates with the server the user's login credentials and password. The server then creates a challenge, which is sent back to the user's PC. After that, the browser creates a payload that includes the challenge, the server's URL, and the session that needs to be signed by the token.

B. PROPOSED AUTHENTICATION MODEL

A thorough explanation of the suggested MFA model, which may be applied to a dependable and safe authentication

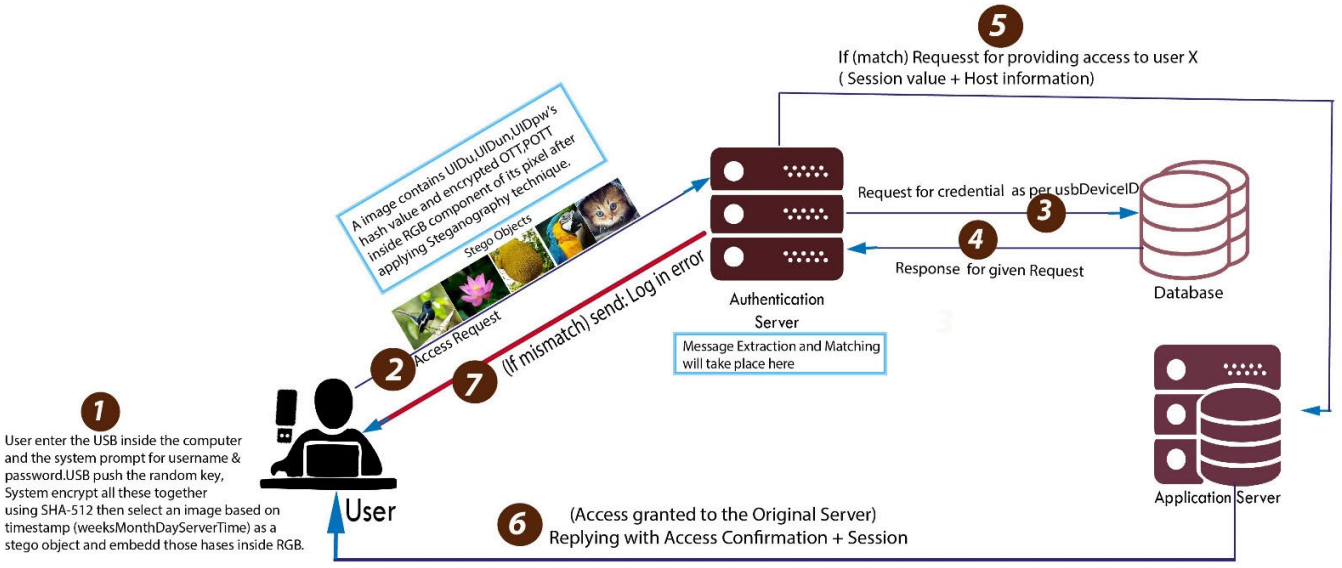

FIGURE 1. Proposed SMFA model.

procedure, is provided in this section. The suggested approach hides the existence of data and ensures data security using steganography and cryptography.

The proposed mechanism introduces a USB device as an additional authentication factor alongside existing credentials like usernames and passwords. Operating under the assumption of three distinct roles within this system—namely, the user, the authentication server, and the application server—specific functions are assigned to each role. The application server serves authorized users, while the authentication server verifies user authenticity. During login, users are prompted to utilize a registered USB device to confirm their identity.

As shown in Figure 1, this technique consists of three main phases: the request phase, the authentication phase, and the response phase. During the server login request procedure, users are required to utilize their registered USB device, which has a Stego validator that generates and stores One-Time Tokens (OTTs).

Assuming User A tries to log in, the registration procedure is skipped for the sake of this study. As such, the registration phase is skipped in this context and the proposed USB-based, multi-server authentication system consists of three main phases: the login phase, the authentication phase, and the registration phase. Whenever a new user signs up on the server or within the system. The authentication server provides the user with a USB device to produce the one-time token after receiving the registration request. Below is a description of each step.

1) THE REQUEST PHASE

i. Login is requested by User to the system (S_a).
ii. User A enters USB device to the system (S_a). System reads UID_u and the banner Bo enclosed within the Stego validator S_{vu}.
iii. Bo is matched by Client side. If matche found, then system prompts the user to provide their UID_{un} and $UsID_{pw}$.
iv. Upon prompted by the system, User A provides UID_{un} and UID_{pw} (UID_{un}, UID_{pw}).
v. Newly generated OTT from S_{vu},(UID_{un}, UID_{pw}), timestamp Tsc is received by client side.
vi. Hash operation is performed on the following UID_u, UID_{un}, utilizing the SHA-512 hashing algorithm at the client side. Thereafter, employing asymmetric algorithm, encryption on OTT and POTT (OTT, POTT) is performed.
vii. One image is chosen from a collection of images (group of 3/4/5/7/10) based on the OTT stored in S_{vu}.
viii. Use the appropriate and efficient steganography technology to embed the hashed data inside the chosen image.
ix. Send this image together with other images after the credentials have been embedded and encrypted E_n(OTT,POTT) to the authentication server S_p.

2) THE AUTHENTICATION PHASE

i. S_a obtains the picture files and E_n(OTT,POTT).
ii. After successfully decrypting the E_n(OTT,POTT), find the STo,i and pull out HASH, H(h1) from STo,i.
iii. Execute the hashing process on H(h1) and produce H(h2).
iv. Rsh = h2 —— Ch and Rott = POTT —— DBOTT
v. Store OTT in DBOTT only if Rsh and Rott both is TRUE. Redirect to S_a.

3) THE RESPONSE PHASE

i. Access request to C_u is received by S_p.
ii. A session is created by S_p.
iii. Finally, access is given to C_u.

TABLE 1. Proposed authentication model notation.

Notation	Description
$\mathbf{S_a}$	Authentication server
S_p	Application server
S_{vu}	Stego validator
UID_u	USB identification number
UID_{un}	Username
UID_{pw}	Password
$ID_{r,u,a}$	Authentication server identity request
OTT	Stego validator generated One-time token
POTT	Previously used OTT stored in stego validator
H(h)	Secure one-way hash function
$\|\|$	Compare Operator
E_n	Encrypted

4) THE RECOVERY PHASE

In the scenario of USB device loss or damage, this research presents two suggested approaches. Firstly, users are advised to register an additional USB device to mitigate the impact of such sporadic incidents. Registering multiple devices enables users to have at least two USB sticks registered, allowing access with the other device in case of loss or damage to one. The reporting process should be user-friendly, while the authentication server needs to revoke the stego validator and OTT of the lost USB device upon confirming the authenticity of the loss or breakage report.

This study suggests that using multiple registered USB devices is the best course of action since it reduces the need and bother of account recovery. This strategy, meanwhile, might not be totally adequate. A re-registration procedure may be taken into consideration as a solution to this limitation, subject to the organization's unique user situation, security requirements, and regulations. Reissuing account details and verifying one's identification in full, however, can result in higher service overhead. It's important to note that the SMFA procedure doesn't explicitly advocate for this but presents it as a potential alternate mechanism. The decision on which approach to adopt should be made by organizations, taking into account risk management and security policies. Figure 1. illustrates the architecture of the proposed model, which integrates the SHA-512 HASH function and RSA encryption to conceal original data.

This model leverages multiple images, selecting a single image to conceal data using an appropriate steganography technique. POTT manages the image selection for steganography application. There are other data-hiding methods available in the discipline of image steganography, but the most popular and straightforward one is the LSB replacement algorithm. Any image steganography method with a strong security level, however, can be used with this framework. The peak signal-to-noise ratio (PSNR) and mean square error (MSE) between the Cover object and the Stego object are taken into account during the security evaluation process. The following formula can be used to get the PSNR [51] between two images:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij})^2$$

$$m \quad numberofrowsincoverimage$$

$$n \quad numberofcolumnsincoverimage$$

$$x_{ij} \quad pixelvaluefromcoverimage$$

$$y_{ij} \quad pixelvaluefromstegoimage$$

$$PSNR(x, y) = \frac{10\log_{10}[max(max(x), max(y))]^2}{x - y^2}$$

The pixel values at places i and j in the Cover picture are represented by the equations as ij, and the pixel values at positions i and j in the Stego image are indicated by bij. Research indicates that when the PSNR (peak signal-to-noise ratio) between two images (Cover image and Stego image) exceeds 40dB, it indicates good quality. A higher PSNR implies lower imperceptibility. Notably, between two identical and unchanged pictures, the PSNR is infinite. Hence, any image steganography technique achieving a minimum of 40dB PSNR in this model suffices to conceal credentials effectively.

The recommendation is to employ an algorithm yielding the maximum PSNR to minimize perceptibility, signifying a higher level of security. The general procedure for concealing credentials in this model follows these steps:

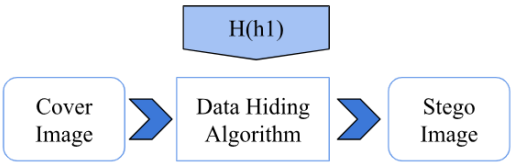

FIGURE 2. Procedure of cover object generation.

IV. MODEL ANALYSIS

This model uses an authentication server and an application server to create a shared key between three principals and a database. Although it uses the timestamp as a nonce, it is based on the shared key. Three principals- U, AU, and AP is provide for the above-mentioned proposed model. Thereafter, K_U, K_{AU}, and K_{AP} are their public keys; K_{UAU}, K_{UAP}, and K_{AUPU} are their shared keys; and DB is the authentication server database. Additionally, AU generates the timestamp T_{AU}, while U generates TU; and AT generates the timestamp T_{AP}. Moreover, the lifetime L is generated by U. Only in cases where mutual authentication is necessary are the third, fifth, and sixth messages utilized. In this case, POTT is previously utilized, and Stego validation generates OTT as the one-time token. The validation of OTT saved in Stego is used.

Below is a representation of this message sequence.

Message 1. U → AU: $\{T_{U,}K_{UAP}\{T_U$, OTT, U_{ID}, U_{PASS}, U$\}$ $K_{AU}\}$ K_{UAP}

Message 2. AU → DB: $\{T_{AU}$, OTT, U_{ID}, U_{PASS}, U $\{T_U$, DB, K_{AUDB}, AU$\}$ $K_{DB}\}$ K_{AUDB}

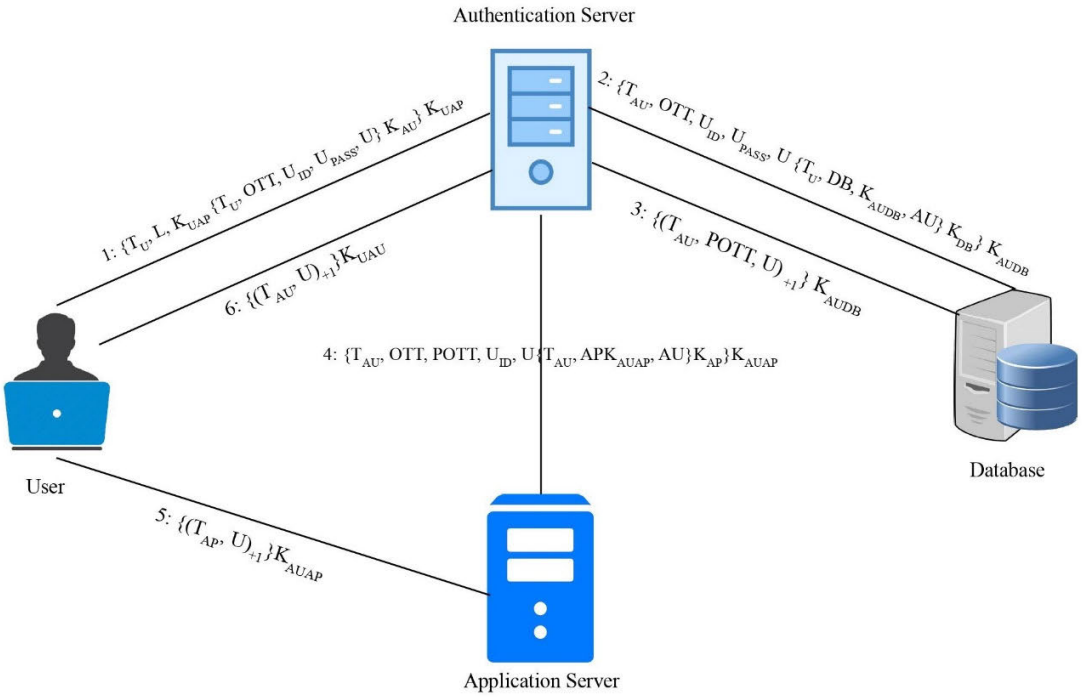

FIGURE 3. Credential flow of proposed model.

Message 3. DB → AU: $\{(T_{AU}, POTT, U)_{+1}\}\ K_{AUDB}$

Message 4. AU → AP: $\{T_{AU}, OTT, POTT, U_{ID}, U\{T_{AU}, APK_{AUAP}, AU\}\ K_{AP}\}\ K_{AUAP}$

Message 5. AP → U: $\{(T_{AP}, U)_{+1}\}\ K_{AUAP}$

Message 6. AU → U: $\{(T_{AU}, U)_{+1}\}\ K_{UAU}$

Initially, U transmits an encrypted message with OTT that includes a timestamp, a lifetime, a session key for U, AU, and U_{ID}, and U_{PASS}. It is individually encrypted using the AU public key, which only the AU can decrypt using the private key.

After decrypting it, AU transmits it back to the database to verify that the UID, U_{PASS}, and relevant OTT match the POTT that was previously saved. In the event that this session was created recently, DB matches the authenticator message by decrypting it with the enclosing key. It will then replay using the most current timestamp of the authenticator.

Following its satisfaction, the primary AU will send a message to AP including a timestamp, the session information for U, OTT, and POTT, as well as a shared key that it will decrypt using AP's private key. If the session was also created lately, the entire communication will be decrypted using the shared key between AU and AP. Following the satisfaction of this principle, AP will use U's session key to grant access to U's replay. Therefore, the principal U must be believed by the principal AP, if it can be demonstrated that the principal AU believes the principal U and the principal AP believes AU. As a result, the model will be verified. We have demonstrated the session key agreement between our ideas using BAN logic. Several guidelines based on BAN logic are provided below to aid in our comprehension of the overall model's efficiency.

A. BAN LOGIC

BAN logic is used to analyze the security of cryptographic protocols, such as authentication protocols or key exchange protocols. It is based on the idea of using a set of inference rules to determine the security properties of a protocol. The logic has three main rules: the authentication rule, the key generation rule, and the key transport rule. The authentication rule states that if a user A has authenticated another user B using a protocol P, then A believes that B is genuine. The key generation rule states that if a user A generates a key K using a protocol P, then A believes that only users who have participated in P know K. The key transport rule states that if a user A sends a message encrypted with key K to user B using a protocol P, then A believes that only users who have participated in P can decrypt the message. By applying these rules to a protocol, BAN logic can help to identify potential vulnerabilities or attacks. For example, if BAN logic determines that a protocol allows an attacker to impersonate a user or obtain a user's secret key, then the protocol can be considered insecure. Overall, BAN logic is a useful tool for analyzing the security of cryptographic protocols and is widely used in the field of computer security. This research has used BAN Logic to ensure the security of our proposed authentication model. Rules used to make formal analysis for this proposed model have been identified below-

i. Message Meaning Rules: for sharing keys:

$$\frac{P \text{ believes } P \leftrightarrow Q,\ P \text{ sees } \{X\}k}{P \text{ believes } Q \text{ said } X}$$

For public keys:

$$\frac{P \text{ believes } P \leftrightarrow Q,\ P \text{ sees } \{X\}k-1}{P \text{ believes that } Q \text{ said } X}$$

For public keys:

$$\frac{P \text{ believes } P \leftrightarrow Q, P \text{ sees } < X > y}{P \text{ believes that } Q \text{ said } X}$$

ii. Nonce- Verification Rules

$$\frac{P \text{ believes fresh } (X)\ , P \text{ believes } Q \text{ said } X}{P \text{ believes that } Q \text{ believes } X}$$

iii. Jurisdictions Rules

$$\frac{P \text{ believes that } Q \text{ controls } X, P \text{ believes } Q \text{ believes } X}{P \text{ believes } X}$$

The following presumptions have been supplied in order to analyze this protocol:

AU believes AU $\overset{K_{UAU}}{\longleftrightarrow}$ AU believes fresh(T_U)

DB believes DB $\overset{K_{AUDB}}{\longleftrightarrow}$ DB believes fresh(T_{AU})

AP believes AP $\overset{K_{AUAP}}{\longleftrightarrow}$ AP believes fresh (T_{AU})

AU believes U controls (AU $\overset{K}{\longleftrightarrow}$ U) U believes fresh(T_{AP})

The first three assumptions on the left are made with regard to the common keys between the three principals and the database. It is clear from the four assumptions on the right that the model largely depends on the use of synchronized clocks. Both the database server and the principals trust that timestamps created elsewhere are accurate. The principals' and the database's confidence in the server's ability to produce a strong encryption key is shown by the following set of three presumptions. By using the rules of the assumptions that have been proposed, the idealized model is analyzed. For the sake of conciseness, several formal details required for the machine-assisted proof are specified exclusively for Messages 1, 2, and 4. Later on, similar elements were left out.

The detailed analysis will make use of the following notation described in Table 2.

The following are the proof's primary steps:

AU is sent Message 1.

Annotation rules result in that:

AU sees$\{T_U, L, K_{UAP}\{T_U, OTT, U_{ID}, U_{PASS}, U\}K_{AU}\}K_{UAP}$

TABLE 2. Proposed authentication model formal analysis notation.

Notation	Description
U	User
AU	Authentication server
AP	Application server
DB	Database
OTT	One-time token generated by Stego validation
POTT	Previously used OTT stored in Stego validation
U_{ID}	ID for User
U_{PASS}	Password set by User
T_{AU}	Timestamp of Authentication
T_{AP}	Timestamp of Application server
T_U	Timestamp from User side
K_{UAU}	Shared key between authentication server and user
K_{UAP}	Shared key between application server and user
K_{AUDB}	Shared key between database and authentication server
K_{AUAP}	Shared key between application and authentication server
K_{AU}	Key of authentication server
K_{AP}	Key of application server
K_{ADB}	Public key of authentication server database
K_{DB}	Secret key of authentication server database

Nonce verification rules applies and yields-

AU believes U believes(T_U, (AU $\overset{K_{UAU}}{\longleftrightarrow}$ U)).

Again, we break a conjunction, to obtain the following:

AU believes U believes(AU $\overset{K_{UAU}}{\longleftrightarrow}$ U).

Then we instantiate K to K_{UAU} in the hypothesis:

AU believes U believes(AU $\overset{K}{\longleftrightarrow}$ U).

Deriving the tangible

AU believes U believes(AU $\overset{K}{\longleftrightarrow}$ U).

Finally, the jurisdiction rules applies and yield the following:

AU believes AU $\overset{K_{UAU}}{\longleftrightarrow}$ U

This concludes the analysis of Message 1.

U passes U_{ID}, U_{PASS}, and OTT on to AU, together with a message containing a timestamp. Initially, AU can decrypt only the following message-

U believes AU $\overset{K_{UAU}}{\longleftrightarrow}$ U

This outcome can be logically obtained in the same manner as Message 1. Through the message's meaning, jurisdiction

and nonce-verification are hypothesized. This communication can be decrypted by AU with knowledge of the new key. The following can be inferred from the message's meaning and the proposed nonce-verification:

$$\text{U believes AU believes(AU} \overset{K_{UAU}}{\longleftrightarrow} \text{U)}$$

At this point, AU transmits an encrypted message to the database in order to determine UID, UPASS, and OTT. As previously stated, DB responds with assurance that it agrees with AU. Subsequently, AU notifies AP in order to verify U's identification and grants U access by creating a session for U. It is demonstrated by using these three principles in accordance with the preceding ones that-

$$\text{AU believes AP believes(AP} \overset{K_{AUAP}}{\longleftrightarrow} \text{AU)}$$

We deduce:

$$\text{AP believes that AU believes(AP} \overset{K_{AUAP}}{\longleftrightarrow} \text{AU)}$$

Here, with $\text{AP} \overset{K_{AUAP}}{\longleftrightarrow} \text{AU}$, AP receives a communication from AU enabling U to take its place. (Message that will actually send about U's U_{ID}, U_{PASS}, and OTT). So, it can be inferred that:

$$\text{AP believes that AU believes U}$$

And from this, the following theory is derived

$$\text{AP believes that AU controls (AP} \overset{K}{\longleftrightarrow} \text{AU)}$$

Again, with $(\text{AP} \overset{K}{\longleftrightarrow} \text{AU})$, AP receives a communication from AU enabling U to take its place. (Message that will genuinely send about U's U_{ID}, $U_{PASS,}$ and OTT).

Consequently, the following is derived-

$$\text{AP believes that AU controls U.}$$

Thus, the jurisdiction rule comes into play and produces the following:

$$\textbf{AP believes U}.$$

V. RESULT AND DISCUSSION

This part will provide security, performance analysis, and outcomes in order to emphasize the advantages of the suggested method. Performance study contrasts the suggested design with a few different schemes, whereas security analysis specifies the degree of resistance against attacks.

A. SECURITY ANALYSIS

Attack scenarios have been taken into consideration when analyzing the suggested SMFA model from a security standpoint. Some attacks have been prevented and security risk is decreased by SMFA. By applying this model, the following kinds of attacks can be prevented or mitigated.

1) REPLAY ATTACK

For example, attacker A is taken into consideration in the event that they manage to intercept the user's conversation with the authentication server. Stego image files are available to this attacker. This attacker will need to resend the packet to the server in order to log in. But in this instance, the POTT has been modified, therefore the attacker would fail. Here, an OTT that is dynamic will place POTT after each successful authentication. Replay attack is therefore stopped.

2) MAN-IN-THE-MIDDLE ATTACK

The man-in-middle attack, which creates separate connections with the victims (the client and the AS) and then relays messages between them to create the impression that they are speaking face-to-face over a private connection, is an example of an active eavesdropping technique. In actuality, the attacker is controlling the entire conversation. All communications between the two victims must be able to be intercepted by the attacker, who can then insert new ones.

The suggested plan lowers the potential risk provided by an MITM attack and builds a robust defense against it. Steganography is used in this approach to conceal the existence of credentials. The attacker would not be able to alter the credentials, even in the event that the SSL fails and their existence is made public. The intricacy of this technique is the cause. For the purpose of illustration, let's say that Attacker A obtains a packet containing a collection of photos and wishes to obtain the sensitive information. Finding the carrier object (ICc), getting the secret hash (R_h), and then performing hash recovery (H_r) are the first challenges. It is impractical to overcome these obstacles. Once more, even though these challenges are successfully finished, the POTT and OTT are entirely randomly generated and dynamic. This means that the suggested strategy cannot withstand any MITM attack.

3) IMPERSONATING ATTACK

Even if the username and password are correct, an attacker cannot connect in to the server pretending to be the original user by sending a legitimate credential to the server. This occurs because the unauthorized user is unable to process POTT, which prevents them from completing the authentication process.

4) OFFLINE DICTIONARY PASSWORD ATTACK

Under the suggested scheme, Attacker A would not be allowed to utilize a USB device that is duly registered, but they might be able to create UID_{un} and UID_{pw} if they attempt to log in using the dictionary password. It would simply not be possible to generate OTT and POTT, even in the event of USB cloning, and pass the verification. It is therefore verifiable that the suggested technique renders it computationally impossible for an attacker to pass authentication in the absence of the relevant legitimate user.

TABLE 3. Security comparison with existing multifactor authentication schemes.

	Resist Replay Attack	*Resist Man-in-the-Middle Attack*	*Resist Impersonating Attack*	*Resist Password Guessing Attack*	*Resist Denial of Service Attack*
Nurkifli and Hwang[52]	✓	✓	✓	✗	✓
Chen and Chen [53]	✓	✗	✓	✓	✓
Sudhakar et al.[54]	✓	✗	✗	✓	✗
Google 2-step[15]	✓	✗	✓	✓	✗
Cho et al. [22]	✓	✓	✓	✓	✗
Vermadel et al's OffPAD [32]	✓	✗	✓	✓	✓
Aman et al.[55]	✗	✓	✗	✗	✓
Nyangaresi and Yenurkar [40]	✓	✓	✓	✓	✗
Saqib et al. [56]	✓	✓	✓	✓	✗
Han et al.[57]	✓	✗	✓	✓	✓
Proposed Model: SMFA	✓	✓	✓	✓	✓

5) DOS ATTACK

The model makes use of a specialized authentication server, whose job it is to confirm the legitimacy and notify the application server of the verification status. This method of switching servers avoids any denial of service attacks.

Another factor that is being used is a USB device. Without the physical USB device, the authentication server would not be passed, even if numerous random requests could be sent to it. Consequently, the application server would not be impacted in any way. It is clear from the previous discussion that the suggested paradigm lowers the risk provided by any MITM attack and builds resistance against replay, impersonation, offline password guessing, and DOS attacks. Table 3 compares the suggested and current models in respect to various attack scenarios.

B. PERFORMANCE ANALYSIS

The performance is reported in this subsection from both the organization's and user's point of view. An identity-validating USB device is employed in the suggested model to generate a dynamic one-time token. Nothing about clock synchronization is required for this OTT. What distinguishes this model from others is the use of steganography to ensure data privacy. As an authentication element, smartcards were utilized by Jung H. et al. and Hwang and Li et al., however the authors neglected to account for computational cost and privacy [50]. Clock synchronization problems plague the Varmedal's model [32].

The following performance analysis indicator have been used to evaluate our proposed model's efficiency along with a comparative analysis based on similarity and relevancy.

P1: Multi-factor security.

P2: Clock synchronization is not required.

P3: Users can select their authentication method (user ID/password, USB device, or both) independently of the authentication server's decision.

P4: Minimal computational cost.

P5: Ensure data confidentiality in the transport layer.

P6: Allows for password updates or device swaps.

P7: Authentication relies on the physical device.

Table 4 below presents a comparative analysis of the various protocols' performances using the above mentioned parameters. This model performs better overall than all the other models that have been mentioned thus far, despite having a little larger computational cost than the model developed by Varmedal et al. The inclusion of steganography in this model leads to a slight increase in computing costs. However, lighter steganography algorithms, such as the one referenced in [60], could be more efficient for embedding secret messages and would be more suitable in this context. To the best of our knowledge, the suggested plan is the first authentication model that protects credentials privacy for a secure application or network by using a USB device for authentication and steganography.

Based on thorough comparisons and performance- and security-focused findings, it can be concluded that the suggested MFA approach protects user credentials from unauthorized parties and is resistant to threats that have already been discussed. To reduce the danger associated with the traditional one-factor authentication scheme, a USB device and a dedicated authentication server are employed in this instance. The SHA-512 hashing function has been

TABLE 4. Comparative performance analysis with similar multifactor authentication schemes.

	P1: *Multi-factor security*	***P2***: *Clock synchronization is not required.*	***P3***: *User is allowed to select credential/device by own shelf*	***P4***: *Minimal computational cost*	***P5***: *Ensure data confidentiality in the transport layer*	***P6***: *Allows for password updates or device swaps*	***P7***: *Authentication relies on the physical device.*
Ryu et al.[59]	✓	✗	✗	✓	✓	✗	✗
Manickam and Devarajan [58]	✓	✗	✓	✓	✓	✗	✓
Han et al. [57]	✓	✗	✗	✓	✓	✗	✗
Hwang & li's Smart Card Solution [50]	✓	✓	✓	✗	✗	✓	✓
Vermadel et al's OffPAD [32]	✗	✗	✓	✓	✗	✓	✓
FIDO U2F [14]	✓	✓	✓	✗	✗	✓	✓
Proposed Model: SMFA	✓	✓	✓	✗	✓	✓	✓

employed to ensure cryptography, while steganography has been used to ensure transport-layer security. When all other relevant schemes fail to withstand large attacks, the proposed system succeeds, as shown in Table 4.

Despite having slightly greater computing costs than most other schemes, the developed model has rather good overall performance and security strength. A detailed analysis of computational cost is provided in the following subsection.

1) COMPUTATIONAL COST ANALYSIS

In this sub section, the computational cost of the proposed model has been discussed, juxtaposed with other pertinent models. Given the infrequency of registration and password recovery issues, our scrutiny is primarily directed towards login and internal mutual authentication phases. The computations were carried out on a computer equipped with an Intel(R) Core(TM) i3-10105 CPU @ 3.70GHz, 8.00 GB RAM (7.83 GB usable), operating on a 64-bit system with an x64-based processor. The evaluation encompasses steganographic and cryptographic operations, in addition to verification and message forwarding or redirection processes. Total time required by our proposed scheme is 7.41ms.

Table 5 is for the notations used for computational cost analysis and Table 6 compares the computational costs associated with the login and authentication phase to those associated with other comparable methods.

If steganography was not incorporated then the total time required for the proposed model is-

$$7T_h + +2T_{se}$$

Which indicates less complex in terms of computational context. However, we find that utilizing steganography increase computational complexity and reaches to-

$$7T_h + 12T_{sto} + 2T_{se}$$

TABLE 5. Notation for computational cost analysis.

Notation	Description (Time for)
T_h	One Way Hash Function
T_{se}	Symmetric Encryption
T_{ae}	Asymmetric Encryption
T_{ecca}	ECC Point Addition
T_{eccm}	ECC Point Multiplication
T_{sto}	Steganographic Operation
T_{fe}	Fuzzy Extractor Generation & Reconstructions

The comparative analysis is given below where existing password based mechanism have been considered along with multifactor authentication.

Our proposed SMFA introduces innovative features to enhance security, such as steganography for secure credential transmission and the incorporation of an additional USB device for authentication, these advancements inherently entail additional computational overhead.

The steganography process involved in concealing user credentials requires computational resources for encoding and decoding, which contributes to the overall computational cost of SMFA. Additionally, the integration of an extra USB device as a supplementary factor for user identity verification

TABLE 6. Comparative analysis for computational cost.

Schemes	Total Cost
Chen and Chen [53]	$6T_{eccm}+ 14T_h$
Cho et al [22]	$8\ T_{eccm}+12\ T_h$
Huq et al. [61]	$10\ T_{eccm}+13\ T_h$
Chen et al. [62]	$15T_h+2T_{ae}$
Sutrala et al. [63]	$25T_h+9T_{eccm}+3T_{ecca}$
Saqib et al. [56]	$10T_{eccm}+7T_h+4T_{ecca}$
Nurkifli and Hwang [52]	$6\ T_h + 4T_{fe}$
Nag et al.[64]	$19T_h$
Nyangaresi and Yenurkar [40]	$34\ T_h$
Han et al. [57]	$2T_{se}+4T_h$
Manickam and Devarajan et al. [58]	$36T_h+8T_{se}+6T_{eccm}$
Proposed Model: SMFA	$\mathbf{7T_h+12T_{sto}+2T_{se}}$

introduces overhead in terms of device recognition, communication, and verification protocols.

Furthermore, the adoption of a multi-server authentication scheme in SMFA necessitates additional computational resources for communication and synchronization among multiple servers, as opposed to the conventional single-server approach.

In comparison to traditional password-based authentication systems and other two-factor authentication methods, the computational cost of SMFA is slightly higher due to these added complexities. However, it is crucial to emphasize that this increased computational cost is justified by the significantly enhanced security coverage and mitigation of various security threats, as demonstrated in the comparative analysis.

Despite the slightly higher computational cost, SMFA emerges as a robust and effective multi-factor authentication solution, offering superior security benefits that outweigh the marginal increase in computational overhead.

VI. CONCLUSION

The proposed authentication protocol, SMFA, stands out for its resilience against diverse attacks, surpassing other protocols in terms of security. Leveraging a USB device, Cryptography, and Steganography, the SMFA protocol excels in implementing secure credential transmission and authentication. This study underscores that the fusion of steganography with authentication mechanisms significantly enhances security measures, effectively addressing prevailing security issues. Notably, the protocol demonstrates efficiency in safeguarding the integrity, confidentiality, and authenticity of transmitted data across the internet.

The SMFA protocol's security and key agreement procedure undergo validation using the BAN-logic method. Detailed analysis and comparative evaluations highlight the substantial impact of USB utilization on the client side, a dedicated authentication server, and the integration of steganography in the transmission process. These factors significantly bolster security, fostering user trustworthiness.

The research findings firmly establish the impregnability of the proposed SMFA against various attacks, including user impersonation, replay, DOS, session-hijacking, and offline password guessing attacks. Additionally, the protocol ensures mutual authentication. Despite a slightly elevated computational cost due to multi-layer protection, it notably curtails MITM attacks and their associated damage. To overcome these challenges, the intention is to implement and deploy this scheme in real-world applications while considering potential enhancements in the future.

ACKNOWLEDGMENT

The authors would like to express their gratitude to the Daffodil International University and University of North Texas for providing academic support to carry out this research project.

REFERENCES

[1] R. Morris and K. Thompson, "Password security: A case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, Nov. 1979.
[2] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, San Francisco, CA, USA, May 2012, pp. 553–567.
[3] *2023 Annual Cybersecurity Threat Report—eSentire*. Accessed: May 18, 2024. [Online]. Available: https://www.esentire.com/resources/library/2023-official-cybercrime-report
[4] BBC News. (Oct. 3, 2017). *Yahoo 2013 Data Breach Hit 'All Three Billion Accounts*. Accessed: Apr. 13, 2024. [Online]. Available: https://www.bbc.com/news/business-41493494
[5] Fortune. *Uber Data Breach Exposed Personal Information of 20 Million Users*. Accessed: Apr. 13, 2024. [Online]. Available: http://fortune.com/2018/04/12/uber-data-breach-security/
[6] Csoonline. *Aadhaar Breach Report: Reactions on Freedom and Privacy*. Accessed: Apr. 13, 2024. [Online]. Available: https://www.csoonline.com/sarticle/3448722/aadhaar-breach-report-reactions-on-freedom-and-privacy.html
[7] Verge. *The Marriott Hotel Chain Has Been Hit by Another Data Breach*. Accessed: Apr. 13, 2024. [Online]. Available: https://www.theverge.com/2022/7/6/23196805/marriott-hotels-maryland-data-breach-credit-cards
[8] Baylor Univ. *World's Biggest Data Breaches of the Decade*. Accessed: May 11, 2024. [Online]. Available: https://onlinecs.baylor.edu/news/worlds-biggest-data-breaches-decade
[9] UpGuard. *Losing Face: Two More Cases of Third-Party Face- Book App Data Exposure*. Accessed: May 11, 2024. [Online]. Available: https://www.upguard.com/breaches/facebook-user-data-leak
[10] Forbes. *Understanding The First American Financial Data Leak: How Did it Happen and What Does it Mean?*. Accessed: May 11, 2024. [Online]. Available: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=2c69d98d567f
[11] Linkedin. *LinkedIn's June 2021 'Breach*. Accessed: May 11, 2024. [Online]. Available: https://www.linkedin.com/pulse/linkedins-june-2021-breach-edwin-brockner-cipm
[12] Weibo. *Selling of Weibo User Information*. Accessed: May 11, 2024. [Online]. Available: https://weibo.com/2735327001/IzCMJioqC

[13] OAG. *Symantec Mailing*. Accessed: Mar. 1, 2024. [Online]. Available: https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf
[14] Yubico. *U2F—FIDO Universal 2nd Factor Authentication*. Accessed: Jan. 26, 2023. [Online]. Available: https://www.yubico.com/solutions/fido-u2f
[15] *Google 2-Step Verification*. Accessed: Apr. 13, 2024. [Online]. Available: https://www.google.com/landing/2step/
[16] S. Sahute, S. Waghamare, and A. Diwate, "Secure messaging using image stegnography," *Int. J. Modern Trends Eng. Res.*, vol. 2, no. 3, pp. 598–608, 2015.
[17] J. Baek, C. Kim, P. S. Fisher, and H. Chao, "(N, 1) secret sharing approach based on steganography with gray digital images," in *Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Secur.*, Jun. 2010, pp. 325–329.
[18] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognit.*, vol. 34, no. 3, pp. 671–683, Mar. 2001.
[19] A. K. Das, "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1377–1404, Jun. 2015.
[20] M. N. Babu, A. S. N. Chakravarthy, and C. Ravindranath, "The design of a secure three factor authentication protocol for wireless sensor networks," in *Proc. Int. Conf. Nextgen Electron. Technol., Silicon Softw. (ICNETS2)*, Mar. 2017, pp. 184–190.
[21] R. Amin, S. H. Islam, M. K. Khan, A. Karati, D. Giri, and S. Kumari, "A two-factor RSA-based robust authentication system for multiserver environments," *Secur. Commun. Netw.*, vol. 2017, pp. 1–15, Jan. 2017, doi: 10.1155/2017/5989151.
[22] Y. Cho, J. Oh, D. Kwon, S. Son, S. Yu, Y. Park, and Y. Park, "A secure three-factor authentication protocol for e-governance system based on multiserver environments," *IEEE Access*, vol. 10, pp. 74351–74365, 2022, doi: 10.1109/ACCESS.2022.3191419.
[23] J. Shen, D. Liu, S. Chang, J. Shen, and D. He, "A lightweight mutual authentication scheme for user and server in cloud," in *Proc. 1st Int. Conf. Comput. Intell. Theory, Syst. Appl. (CCITSA)*, Dec. 2015, pp. 183–186.
[24] J. H. Yang and P. Y. Lin, "An ID-based user authentication scheme for cloud computing," in *Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Aug. 2014, pp. 98–101.
[25] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Comput. Commun.*, vol. 32, no. 4, pp. 583–585, Mar. 2009.
[26] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 629–631, May 2004.
[27] W. Liu, Q. Xie, S. Wang, and B. Hu, "An improved authenticated key agreement protocol for telecare medicine information system," *SpringerPlus*, vol. 5, no. 1, p. 555, Dec. 2016.
[28] C.-M. Huang and J.-W. Li, "One-pass authentication and key agreement procedure in IP multimedia subsystem for UMTS," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Niagara Falls, ON, Canada, May 2007, pp. 482–489.
[29] J.-K. Tsay and S. F. Mjølsnes, "A vulnerability in the UMTS and LTE authentication and key agreement protocols," in *Computer Network Security* (Lecture Notes in Computer Science), vol. 7531. Berlin, Germany: Springer, 2012, pp. 65–76, doi: 10.1007/978-3-642-33704-8_6.
[30] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A strong user authentication framework for cloud computing," in *Proc. IEEE Asia–Pacific Services Comput. Conf.*, Dec. 2011, pp. 110–115.
[31] M. Kumar, "New remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 597–600, May 2004.
[32] K. A. Varmedal, H. Klevjer, J. Hovlandsvåg, A. Jøsang, J. Vincent, and L. Miralabé, "The OffPAD: Requirements and usage," in *Network and System Security* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2013, pp. 80–93, doi: 10.1007/978-3-642-38631-2_7.
[33] M. Alhaidary, S. M. M. Rahman, M. Zakariah, M. S. Hossain, A. Alamri, M. S. M. Haque, and B. B. Gupta, "Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the OffPAD protocol," *IEEE Access*, vol. 6, pp. 6071–6081, 2018.
[34] M. Alhaidary and S. M. M. Rahman, "Security vulnerability analysis and corresponding mitigation for password-based authentication using an offline personal authentication device," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 842–849.
[35] W. I. Bae and J. Kwak, "Smart card-based secure authentication protocol in multiserver IoT environment," *Multimedia Tools Appl.*, vol. 79, pp. 15793–15811, Apr. 2020.
[36] A. A. Khan, V. Kumar, and M. Ahmad, "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach," *J. King Saud Univ.-Comp. Inf. Sci.*, vol. 34, no. 3, pp. 698–705, Mar. 2019.
[37] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, Feb. 2022.
[38] W. A. Hufstetler, M. J. H. Ramos, and S. Wang, "NFC unlock: Secure two-factor computer authentication using NFC," in *Proc. IEEE 14th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2017, pp. 507–510.
[39] W. Liu, X. Wang, W. Peng, and Q. Xing, "Center-less single sign-on with privacy-preserving remote biometric-based ID-MAKA scheme for mobile cloud computing services," *IEEE Access*, vol. 7, pp. 137770–137783, 2019.
[40] V. O. Nyangaresi and G. K. Yenurkar, "Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks," *High-Confidence Comput.*, vol. 4, no. 2, Jun. 2024, Art. no. 100178, doi: 10.1016/j.hcc.2023.100178.
[41] S. Shukla and S. J. Patel, "A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing," *Computing*, vol. 104, no. 5, pp. 1173–1202, Jan. 2022.
[42] W. Mao, *Modern Cryptography: Theory and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 2011.
[43] B. Madhuravani, P. B. Reddy, D. S. R. Murthy, and K. V. S. N. R. Rao, "Strong authentication using dynamic hashing and steganography," in *Proc. Int. Conf. Comput., Commun. Autom.*, May 2015, pp. 735–738.
[44] S.-H. Gunawardena, D. Kulkarni, and B. Gnanasekaraiyer, "A steganography-based framework to prevent active attacks during user authentication," in *Proc. 8th Int. Conf. Comput. Sci. Educ.*, Apr. 2013, pp. 383–388.
[45] M. Tabassum, A. H. Sarower, A. Esha, and M. M. Hassan, "An enhancement of Kerberos using biometric template and steganography," in *Cyber Security and Computer Science* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 325, T. Bhuiyan, M. M. Rahman, and M. A. Ali, Eds., Cham, Switzerland: Springer, 2020, pp. 116–127.
[46] C. D. Motero, J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo, and N. G. Gómez, "On attacking Kerberos authentication protocol in windows active directory services: A practical survey," *IEEE Access*, vol. 9, pp. 109289–109319, 2021, doi: 10.1109/ACCESS.2021.3101446.
[47] H. U.-D.-A. Ihmaidi, A. Al-Jaber, and A. Hudaib, "Securing online shopping using biometric personal authentication and steganography," in *Proc. 2nd Int. Conf. Inf. Commun. Technol.*, 2006, pp. 233–238.
[48] T. Mantoro, D. D. Permadi, and A. Abubakar, "Stegano-image as a digital signature to improve security authentication system in mobile computing," in *Proc. Int. Conf. Informat. Comput. (ICIC)*, Oct. 2016, pp. 158–163.
[49] C. Danuputri, T. Mantoro, and M. Hardjianto, "Data security using LSB steganography and Vigenere chiper in an Android environment," in *Proc. 4th Int. Conf. Cyber Secur., Cyber Warfare, Digit. Forensic (CyberSec)*, Oct. 2015, pp. 22–27.
[50] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 28–30, Feb. 2000.
[51] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," *IEEE Trans. Commun.*, vol. 43, no. 12, pp. 2959–2965, Dec. 1995.
[52] E. H. Nurkifli and T. Hwang, "Provably secure authentication for the Internet of Vehicles," *J. King Saud Univ. -Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101721, doi: 10.1016/j.jksuci.2023.101721.
[53] Y. Chen and J. Chen, "A secure three-factor-based authentication with key agreement protocol for e-health clouds," *J. Supercomput.*, vol. 77, no. 4, pp. 3359–3380, Aug. 2020, doi: 10.1007/s11227-020-03395-8.
[54] T. Sudhakar, V. Natarajan, M. Gopinath, and J. Saranyadevi, "An enhanced authentication protocol for multi-server environment using password and smart card," *Wireless Pers. Commun.*, vol. 115, no. 4, pp. 2779–2803, May 2020, doi: 10.1007/s11277-020-07462-4.
[55] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1123–1139, Jan. 2021, doi: 10.1109/JIOT.2020.3010893.
[56] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6925–6937, Oct. 2022, doi: 10.1016/j.jksuci.2021.07.023.

[57] Y. Han, H. Guo, J. Liu, B. B. Ehui, Y. Wu, and S. Li, "An enhanced multifactor authentication and key agreement protocol in industrial Internet of Things," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 16243–16254, May 2024, doi: 10.1109/jiot.2024.3355228.
[58] M. Manickam and G. G. Devarajan, "A three-factor mutual authentication scheme for telecare medical information system based on ECC," *Cyber Secur. Appl.*, vol. 2, Jan. 2024, Art. no. 100035, doi: 10.1016/j.csa.2024.100035.
[59] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, "Secure ECC-based three-factor mutual authentication protocol for telecare medical information system," *IEEE Access*, vol. 10, pp. 11511–11526, 2022.
[60] T. Bhuiyan, A. H. Sarower, R. Karim, and M. Hassan, "An image steganography algorithm using LSB replacement through XOR substitution," in *Proc. Int. Conf. Inf. Commun. Technol. (ICOIACT)*, Jul. 2019, pp. 44–49, doi: 10.1109/ICOIACT46704.2019.8938486.
[61] I. U. Haq, J. Wang, and Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102660.
[62] R. Chen, Y. Mou, and M. Zhang, "A novel three-factor authentication scheme with high security for multi-server environments," *Wireless Pers. Commun.*, vol. 124, no. 1, pp. 763–781, Jan. 2022, doi: 10.1007/s11277-021-09382-3.
[63] A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2316–2330, Mar. 2022.
[64] P. Nag, P. Chandrakar, and K. Chandrakar, "An improved two-factor authentication scheme for healthcare system," *Proc. Comput. Sci.*, vol. 218, pp. 1079–1090, Jan. 2023, doi: 10.1016/j.procs.2023.01.087.

AFJAL H. SAROWER received the B.Sc. degree (Hons.) in software engineering and the M.Sc. degree in computer science and engineering from Daffodil International University (DIU), Dhaka, Bangladesh.

He has been a Senior Lecturer with the Department of Computer Science and Engineering, DIU, since 2021. Earlier this, he was a Research Associate with the Department of Software Engineering, DIU for one and half years. He is actively involved in teaching a variety of courses related to cyber security, machine learning, database management, and software engineering. He has published several research papers in reputed journals and international conferences. He has received several organizational and government scholarships for research and training. His research interests include information security, cryptography, steganography, authentication protocols, blockchain, and intrusion detection.

TOUHID BHUIYAN received the bachelor's degree in computer science from American University, London, U.K., the master's degree in computing and information systems from the University of London, U.K., and the Ph.D. degree in information security from the Queensland University of Technology, Australia, focusing on trust management for intelligent recommendations.

He is currently a Professor of cyber security with Washington University of Science and Technology, Alexandria, VA, USA. Before joining DIU, he was employed by several Universities, including East West University, The University of Western Australia, Queensland University of Technology, University of Western Sydney, and University of Malaysia Perlis. He has more than 23 years of experience in teaching and research. He has more than 125 research publications in renowned national and international journals, books, and conference proceedings. He has also worked in the IT industry in Australia, U.K., Singapore, Malaysia, and Indonesia. His research interests include cyber security, intelligent recommendations, social networks, trust management, big data analytics, e-health, and e-learning. He received the Cyber Security: Cyber Risk and Resilience certificate from the University of Oxford. He was a recipient of the Australian Postgraduate Award (APA) and the Deputy Vice-Chancellor's Initiative Scholarship from QUT, Australia.

MARUF HASSAN is currently an Associate Professor with Southeast University, Dhaka, Bangladesh, where he has been, since November 2024 after serving ten years with Daffodil International University. He has held a position as the Head of the IT and System Audit Department, The Premier Bank Ltd., since February 2015. Prior to that, he was the Information Systems Audit Incharge with NCC Bank Ltd., from December 2012 to January 2015. He has extensive experience in the field of IT audit, information systems, and software testing. He has held various roles throughout his career, including the Manager of IT Audit with Hoda Vasi Chowdhury and Co, where he worked, from 2010 to September 2012. Additionally, he was a Senior Software Test Engineer with LEADS Corporation Ltd. and an Associate Software Engineer with Accenture Technology Solutions, where he gained project experience with the Australian Tax Office and Commonwealth Bank of Australia.

MOHAMMAD SHAMSUL AREFIN (Senior Member, IEEE) received the Doctor of Engineering degree in information engineering from Hiroshima University, Japan, with the support of the scholarship of MEXT, Japan. He is currently the Dean of the Faculty of Electrical and Computer Engineering, Chittagong University of Engineering and Technology (CUET), Chittagong, Bangladesh. He is with the Department of Computer Science and Engineering (CSE), Daffodil International University, Dhaka, Bangladesh. Earlier, he was the Head of the Department of Computer Science and Engineering, CUET. As a part of his Ph.D. Research, he was with IBM Yamato Software Laboratory, Japan. He visited Japan, Indonesia, Malaysia, Bhutan, Singapore, South Korea, Egypt, India, Saudi Arabia, Nepal, and China for different professional and social activities. His research includes privacy-preserving data publishing and mining, distributed and cloud computing, big data management, multilingual data management, semantic web, green computing, and IT for agriculture and the environment. He has more than 150 referred publications in international journals, book series, and conference proceedings. He is a member of ACM and a fellow of IEB and BCS. He is the Genera; the Chair of BIM 2023 and the IEEE CS BDC Summer Symposium 2023, the Organizing Chair of BIM 2021; the TPC Chair of ECCE 2017; the Organizing Co-Chair of ECCE 2019; and the Organizing Chair of BDML 2020.

GAHANGIR HOSSAIN (Senior Member, IEEE) received the Ph.D. degree in computer engineering from the University of Memphis, Memphis TN, USA. He is currently an Associate Professor of data science with the Department of Information Science, University of North Texas, TX, USA. He has previously worked at the Purdue School of Engineering and Texas A&M University at the Kingsville and Canyon Campuses. Throughout his career, he has secured more than $2 million in research funding from prestigious sources, such as Microsoft, the Department of Energy (DoE), the Department of Homeland Security (DHS), and the Office of Naval Research (ONR). In addition to his research accomplishments, he is actively involved in teaching a range of courses related to information systems design, information security, decision sciences, and intelligent interaction. He brings extensive experience in mentoring and coaching master's and Ph.D. research students. His expertise is well recognized in the academic community, as evidenced by his numerous peer-reviewed research articles published in reputable journals and conference proceedings. Moreover, he has authored two IT books and several book chapters, further establishing his authority in the field. His diverse research interests include artificial intelligence, machine learning applications, data science, cognitive neuroscience, cybersecurity management, and cyber-human interaction. Beyond his scholarly contributions, he actively serves as a member of various international conference program committees and fulfills the role of an ABET program evaluator for computer science and data science programs. These engagements showcase his commitment to advancing the field and ensuring quality education.