

**BAN IMPLEMENTATION OF SMFA: PRIVACY PRESERVING MULTI-
FACTOR AUTHENTICATION MODEL BASED ON USB, CRYPTOGRAPHY
AND IMAGE STEGANOGRAPHY**

BY

**AFJAL H. SAROWER
ID: 213-25-062**

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Masters of Science in Computer Science and Engineering

Supervised By

Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2023

APPROVAL

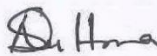
This Project/Thesis titled “**BAN Implementation Of SMFA: Privacy Preserving Multi-factor Authentication Model Based On USB, Cryptography And Image Steganography**”, submitted by Afjal H. Sarower, ID No: 213-25-062 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 17-01-2023.



BOARD OF EXAMINERS

Chairman

Dr. S M Aminul Haque, PhD
Associate Professor & Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



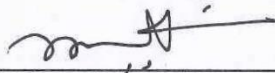
Internal Examiner

Ms. Naznin Sultana
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Internal Examiner

Mr. Md. Sadekur Rahman
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



External Examiner

Dr. Mohammad Shorif Uddin, PhD
Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

I hereby declare that, this project has been done by me under the supervision of **Dr. Touhid Bhuiyan, Professor and Head, Department of CSE, Daffodil International University**. I also declare that this project is an extension to the previous research project named MFAS which was submitted for my Bachelor degree but this project has not been submitted elsewhere for award of any degree or diploma.

Supervised by:



17/01/23

Dr. Touhid Bhuiyan
Professor and Head
Department of CSE
Daffodil International University

Submitted by:



Afjal H. Sarower
ID: 213-25-062
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I express my heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year thesis successfully.

I am really grateful and wish my profound indebtedness to **Professor Dr. Touhid Bhuiyan, Head**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of “*Information Security*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this thesis.

I would like to express my heartiest gratitude to Professor Dr. Sheak Rashed Haider Noori and Dr. S. M. Aminul Haque, Associate Head, Department of CSE, for kind help to finish my thesis and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in several discussion while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my parents, few cooperative friends and family.

ABSTRACT

Ab initio, Password-based authentication systems have been the conventional way to authenticate a user. However, these systems are susceptible to many security threats and vulnerabilities. This impelled the use of Multi-Factor Authentication (MFA) to ensure a more secure and reliable user verification process. Previous research on MFAs has claimed the usage of an extra device as an additional factor to verify the identity of a user. But the existing MFA types, such as OffPAD, OTT, and smartcard-based solutions lack the strength to prevent Man-in-the-Middle (MITM) attack, session hijacking, replay, phishing, and DOS attacks. On top of it, the traditional single server authentication mechanism suffers from inefficiency and inadequacy. This research focuses on designing an MFA model—SMFA—by using steganography for secure credential transmission. The proposed model uses steganography to conceal the user’s credential with the aim of reducing the risk caused by MITM and session-hijacking attacks. Additionally, the SMFA model entails the user to have an extra USB device as another factor to prove his/her identity, along with a proposed multi-server authentication scheme to attenuate the issue of traditional single-server authentication mechanism. A model has been formalized in several steps. This study performs an extensive analysis and comparison of this model with several other widely used protocols. Overall, the comparative analysis indicates clearly that SMFA has better security coverage than other mechanisms in response to MITM, replay, DOS, user-impersonating, and password-guessing attacks.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
CHAPTER	
CHAPTER 1: INTRODUCTION	1-3
1.1 Motivation	1
1.2 Objective	2
1.3 Organization	3
CHAPTER 2: LITERATURE REVIEW	4-8
2.1 MFA Models and Protocols	4
2.2 MFA using Additional Device	5
2.3 MFA Using Steganography in Web	6
CHAPTER 3: RESEARCH METHODOLOGY	9-15
3.1 Background	9
3.1.1 OffPAD	9
3.1.2 Remote User Authentication Scheme Using Smart Cards	9
3.1.3 Google 2-step	9
3.1.4 FIDO	10

3.2 Proposed Authentication Model	10
3.2.1 The Request Phase	11
3.2.2 The Authentication Phase	12
3.2.3 The Response Phase	12
3.2.4 The Recovery Phase: USB Lost or Damaged	13
CHAPTER 4: MODEL ANALYSIS	16-21
4.1 BAN Logic	17
CHAPTER 5: RESULT AND DISCUSSION	22-26
5.1 Security Analysis	22
5.1.1 Replay Attack	22
5.1.2 Man-in-the-middle Attack	22
5.1.3 Impersonating Attack	23
5.1.4 Offline dictionary Password Attack	23
5.1.5 DOS Attack	23
5.2 Performance Analysis	24
CHAPTER 6: CONCLUSION	27
CHAPTER 7: ACKNOWLEDGEMENT	28
REFERENCES	29-31

LIST OF FIGURES

FIGURES	PAGE NO
Figure 3.2.3: Proposed SMFA Model	4
Figure 3.2.4: Steganography Process	15
Figure 4.1: Rules in BAN Logic	17
Figure 4.1: Model with required Notation	19
Figure 5.2: Visual Representation of the Overall Performance of SMFA	26

LIST OF TABLES

TABLES	PAGE NO
Table 3.2: Notation	11
Table 5.1 Defense Level Comparison	24
Table 5.2: Performance Comparison Among Other Established Protocol	25

CHAPTER 1

INTRODUCTION

Authentication is a crucial part of an electronic system when it comes to proving the authenticity of a user. In the course of this process, the user needs to prove their identity which can be done through three basic factors:

- 1) Something that user knows: This indicates the username, password, or some questions directly related to the user whose answer is known by the system.
- 2) Something that user has: This indicates any OTP, smartcard, NFC, and USB device.
- 3) Something that user is: This indicates the user's biometric information which amounts to unique information such as the user's fingerprint, retina, and DNA.

All these three factors that are taken in consideration to verify the identity of a user are known as credentials. Single-factor authentication—i.e. the username and password-based mechanism—is a prevailing mechanism, even though it raised many security concerns in the late '70s [1] [2]. The main problem with the single-factor password-based system is cracking a password by a brute force, and the signing up with the same password in multiple systems by a single user. According to eSentire [3], hacking attempts using brute force or dictionary attacks increased by 400 per cent in 2017.

1.1 Motivation

Passwords can be compromised easily, and a compromised password-based authentication system is mainly responsible for data breaches. In 2013, Yahoo reported that three billion users were impacted by a data breach [4]. In 2016, more than 20 million users' sensitive information was exposed by a data breach of the UBER technology [5]. In consideration of the security concerns raised by the conventional password-based system, this research study owes its origin to the necessity of a C authentication system.

To extenuate password weaknesses, multi-factor authentication protocols combine several authentication factors. Among these, two multi-factor (mainly-two factor) authentication protocols (MFA)- Google 2-step [6] and FIDO's U2F [7] are prominent nowadays, where U2F is a USB based authentication mechanism. But these two protocols are prone to common attacks such as MITM and DOS. Apart from these, some other authentication mechanisms have been introduced which provide specific benefits against specified type of attacks and security concerns. Analyzing the whole scenario, it can be summarized that the main concerns are to- (i) ensure that the person requesting the access is the actual and legal user, and (ii) protect the credentials. Therefore, it is a great challenge to protect user credentials being transmitted over the network.

1.2 Objective

Credentials transmission is imperative for a secure authentication process and this can be achieved in several ways. The most popular among these are the use of cryptography and steganography. In fact, steganography is one of the oldest widely used technique to protect sensitive information. Steganography refers to hiding the existence of data within a cover. The word 'steganography' is originated from the Greekwords 'Seganos' and 'Graphy' which means 'covered' and 'writing/drawing', respectively [8]. Digital steganography techniques are responsible for hiding the presence of sensitive messages and information transmitted over the Internet. In digital steganography, image, video, and audio files can be used as cover objects [9]. While the goal of cryptography is to encrypt the message so that no unwanted person can read it, steganography aims to hide the presence of that message. Cryptography and steganography are used together to ensure good data security [10]. As far as data security is concerned, some studies indicate the use of steganography for a secure authentication process. Steganography is a very secure technique whose implementation is somewhat costly. It has been observed that the banking sector, and military and personnel networks use this technique as a preferred solution over other approaches to ensure data security [10]. Previous researches display that integrating the steganography scheme with the authentication process provides data security during credentials transmission.

In this thesis, the use of steganography in MFA authentication has been proposed. This research aims to integrate steganography with a multi-factor authentication model to resolve security issues as much as possible. The proposed multi-factor authentication model uses steganography and cryptography for data security; it also uses a USB device such as U2F [7] to prove the user's identity along with the username and the password.

1.3 Organization

In this paper, Section II contains previous researches in the relevant field. In Section III, the proposed MFA model has been described, while Section IV deals with discussion, analysis, and comparative results. Finally, Section V concludes the whole paper.

CHAPTER 2

LITERATURE REVIEW

Authentication is the primary step in any secure and reliable transaction. Traditional password based schemes are extensively used for this principal step in order to substantiate the authenticity of the user. Contemporaneously, some advanced authentication mechanisms are being adopted around the globe. During the time of this research, it was observed that some findings have already been conducted on steganography techniques and different types of multi-factor authentication schemes. The related works are described below.

2.1 MFA Models and Protocols

Lots of previous research studies have used two or more factors to prove the user's identity. A.K. Das introduced a three-factor authentication protocol for distributed wireless sensor networks and also claimed that this protocol is secure against some common attacks [11]. Babu M. N. analysed the protocol developed by A.K. Das and found that it cannot handle any reply attack or any known session-specific temporary information attack. Later, an improved protocol over the one developed by A.K. Das was proposed to serve the purpose [12].

Shen J. et al. proposed a lightweight authentication system for the cloud environment to reduce the computational cost of the client and the server side by using XOR, string concatenation, and a hash function [13]. Yang et al., proposed IDbased user authentication, which is an improved version of the existing ID-based scheme. The authors also proposed another scheme of authentication for the multi-server environment. However, these are for a cloud environment and the computational cost is slightly higher [14]. Wang et al. and Das M. L. et al. gave a model demonstration of the identity-based authentication scheme [15][16]. Both the models were proposed for accurate authenticity of the user, but data transmission is not secure in the model developed by Wang et al. In this respect, it is found that credentials can be modified while being transmitted over the network. The model

developed by Das et al. is also not secure due to the scope of bypassing authentication without providing any valid credentials.

Huang and Li proposed a one-pass authentication and key agreement (AKA) procedure to avoid the one-pass authentication procedure [17]. Ming et al. investigated the AKA and found that among others, man-in-the-middle, sessionhijacking, and server-spoofing attacks, could take place [18]. On the other hand, Tsay and Mjolsnes found a vulnerability that attackers could exploit both inside and outside [19].

2.2 MFA Using Additional Device

Throughout the last decade, various elegant approaches have been proposed that suggest the use of an extra device to verify the authenticity of a user. This led to some research studies that motivate the use of the smartcard, the USB, and extra online devices as another factor. Choudhury AJ et al. has proposed a multi-factor authentication framework that uses a user ID, password, and smartcard [20]. However, using a smartcard reduces the usability since it creates the need of another device to read the smartcard. So, this scheme is not suitable for a public cloud environment. In 2013, Kumar B et al. proposed an MFA framework using OTP and the IMEI number as authentication secrets for the mobile environment [21].

Varmedal first provided the idea to use OffPAD [22] whose details were published in 2005. This protocol supports the management and authentication of both the service provider and the user identity. This was proposed mainly for any online transaction that avoids MITM and phishing attacks. Later, Alhaidary M. et al. carried out a vulnerability analysis and proposed an improved version to resolve the issues [23]. In 2016, Alhaidary M. et al. investigated the vulnerabilities of the OffPAD-based authentication model and provided some techniques to mitigate the susceptibilities [24]. Their analysis shows that OffPAD is extremely vulnerable to replay and man-in-the-middle attacks.

Hufstetler W. A. et al. implemented a secure multi-factor authentication system using NFC to replace the authentication of the current Windows version that allows the user to log in by providing a pass code and scanning the NFC tag [25]. To avoid data manipulation, Advanced Encryption Standard (AES) is used for data security. But along with the presence of this model's limitation of only being able to work for Windows personal computer and not for any network environment, there remains some existence of security threats of this authentication process.

2.3 MFA Using Steganography in Web

Authentication protocol is responsible for secured data exchange and communication between the entities related to the system through the appliance of cryptography [26]. According to Liu et al., authentication protocol mostly ensures key agreements, data security, non-denial methods, and multiside computation [27]. Several research studies have used steganography in web authentication. There is a scope to work with authentication by using steganography. To improve data security and hide the existence of sensitive credentials, steganography and cryptography can be combined together. Some researchers suggest the use of steganography, and hashing or encryption together to achieve very reliable data security in digital communication. Madhuravani B. et al. stated that the use of steganography and cryptography is the best combination to misguide attackers, and in response showed a technique by using dynamic hashing and steganography [28]. Gunawardena S. et al. discussed a framework of authentication called imgAuth that uses image steganography for authentication and user profile management [29]. The author carried out an analysis claiming that it can act as a universal authentication framework and holds the right balance between security, integrity, and availability. This framework is resistant against some popular attacks. Roy et al. proposed a method that uses steganography and visual cryptography for the sharing of information between the customer and the merchant server by providing more safety [30]. The benefit of this method is that it prevents the misuse of information on the merchandise site. The limitation of this method is the use of OTP to provide more security: since there are two OTPs, there is a concern about the synchronization between client and server.

Ihmaid A. et al. proposed a secure authentication mechanism for any online shopping system which uses biometrics and steganography to hide the credentials [31]. The proposed system encrypts the sensitive cards and credentials and hides them within an image using a specific steganography algorithm. Mantoro T. et al. described the process of hiding the textual password in an image using the steganography technique [32]. All sensitive and critical information is encrypted to prevent any brute force attack. Here, LSB steganography and AES are used to hide the textual password to ensure good security of an authentication system for android. Montro T. et al. also presented a prototype named ste-Chy, which is a combination of LSB steganography and Vignere cipher—this process is used for a confidential authentication purpose to ensure data security [33]. Moreover, SHA-256 was used to achieve authenticity. The research claims that sharing of confidential data through online authentication using steganography is considerably secure. But the current study explains the technique by considering the android environment. After reviewing the above-discussed contributions, it can be comprehended that many initiatives and models have been proposed for a secure authentication process. MFA provides a better security level than the single-factor authentication system [20].

Moreover, it can be perceived that steganography can be used in authentication but it definitely requires further analysis. Notable research has been conducted separately on steganography and the authentication model. However, there has been limited research on the multi-factor authentication system and steganography, collectively. Some researchers use steganography in the model of cloud authentication, while others use it in the e-commerce sector for secure credentials transmission. The contribution of this study amounts to designing a multi-factor authentication model that uses steganography for secure credentials transmission. This research study focuses on integrating steganography with the authentication system.

The following factors have been considered while designing the proposed model:

1. Using cryptography for data protection.

2. Using steganography to hide the existence of credentials inside a cover object, where the transmitted packet contains multiple possible cover objects. This technique is effective in misguiding the attacker and also increases the decoding time of the hidden credentials.
3. Designing in a way where two different servers can be used to reduce risk and increase efficiency.

CHAPTER 3

RESEARCH METHODOLOGY

Multi-factor authentication is a cut above than single factor authentication mechanisms when it comes to providing better security. There are already some MFA protocols or models that are being used by different organizations. The next discussion is about the existing MFA mechanism.

3.1 Background

3.1.1 OffPAD

OffPAD is an offline personal authentication device. This device is used to provide the user with tools for securely managing the authentication process for online transactions. The aim is to manage online identification to circumvent MITM and phishing attacks. In 2005, Josang and Pope first published details of this personal authentication device. After that, Vannedal et al. proposed and improved a version of this and called it OffPAD [22]. The specialty of this device is that mostly it remains offline entailing a secure element.

3.1.2. Remote User Authentication Scheme Using Smart Cards

Hwang and Li suggest that a smart card be used as a part of user authentication based on ElGamal's public key cryptosystem [34]. The security of this mechanism relies on the difficulty of computing discrete logarithms over finite fields. This is a remote user authentication system that does not use a password verification table. At the time of registration, the user registers their smartcard along with the password. When an authorized user attempts to log in to the system, this card must be inserted into the device along with ID and password.

3.1.3 Google 2-step

Google proposes a two-factor authentication mechanism, which is known as Google 2-step [6]. This is mainly a phonebased scheme where the user may use their phone to confirm the login. On their website, Google states several reasons why password-only

authentication is not sufficient and also states that ‘2-Step Verification can help keep bad guys out, even if they have your password’. A verification code is sent to the user’s computer that has to be entered during the login. Another version of this mechanism is the ‘one-tap’ version, where the user simply presses a ‘yes’ button in a pop-up on the phone. The second version is undoubtedly better than the previous one as far as usability is concerned.

3.1.4 FIDO

There is a version of FIDO’s authentication standard that uses the U2F token as the second factor [7]. The U2F USB generates a token and can store secret as well as public keys. These keys are being used to perform cryptographic operations. The USB token has a button that a user must press to confirm a transaction. According to their website, ‘To enable second-factor authentication for a website, the token generates a key pair and the public key is registered on the server. This operation is performed once, and the token can then be used for authenticating.’ In this mechanism, the computer forwards the user’s login details and password to the server. Next, the server generates a challenge which is sent to the user’s computer. The browser generates a payload containing the URL of the server and challenge, session be signed by token.

3.2 Proposed Authentication Model

This section gives a detailed demonstration of the proposed MFA model that can be used for a secure and reliable authentication process. The proposed system uses cryptography and steganography for ensuring data security, and concealing the presence of data. The proposed mechanism uses a USB device to add an extra factor to existing factors such as username and password. Taking the assumption that there are three different roles in this proposed scheme: the user, the authentication server, and the application server, the functions can be put in a defined process, i.e. - the application server will be responsible for providing service to the authorized user, while the authentication server will be

responsible for verifying the authenticity of the user. At the time of login, users will be required to use a registered USB device to prove identity.

The proposed scheme is divided into the request phase, the authentication phase, and finally, the response phase. The notation used in this scheme are listed in detail in Figure 1. In this process, at the time of requesting the server for a login, a user must use their USB device that has been registered during the user registration process. The USB contains a Stego validator responsible for generating and storing OTT. This paper ignores the registration process here and hence assumes that User A takes login attempts. So, the proposed USB-based, multi-server authentication scheme basically consists of three phases—the registration phase, the login phase, and the authentication phase. The registration phase is invoked whenever new users register in the system or the server. Upon receiving the registration request, the authentication server issues a USB device to the user so that it can be used to generate the one-time token.

TABLE 3.2: NOTATION

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	One-time token generated by Stego validator
POTT	Previously used OTT stored in Stego validator
$H(h)$	Secure one-way hash function
\parallel	Compare operator
E_n	Encrypted

3.2.1 The Request Phase

- i. User A requests for login to the system (S_a).
- ii. User A enters their USB device to the system (S_a). It reads UID_u and the banner B_o contained by the Stego validator S_{vu} .

- iii. Client side matches the Bo. If it matches, then it prompts the user to enter their UIDun and UsIDpw.
- iv. UserA provides UIDun and UIDpw (UIDun, UIDpw).
- v. Client side receives the newly generated OTT from Sv_u, (UIDun, UIDpw), timestamp Tsc.
- vi. Client side hashes the following UID_u, UIDun, UIDpw by using the SHA-512 hashing algorithm.
- vii. Client side encrypts OTT and POTT (OTT, POTT) using the asymmetric algorithm.
- viii. Client side selects a particular image from a group of images (group of 3/4/5/7/10) based on the OTT stored in Sv_u.
- ix. Embed the hashed inside the selected image using the suitable and effective steganography technique.
- x. Once the credentials are embedded within the image, send the image with other images and encrypted En(OTT,POTT) to the authentication server Sp.

3.2.2 The Authentication Phase

- i. Sa receives the image files and En(OTT,POTT).
- ii. Decrypt the En(OTT,POTT) and find the ST_{o,i} and extract HASH, H(h1) from ST_{o,i}.
- iii. Perform the HASH operation on H(h1) and produce H(h2).
- iv. Rsh = h2 || Ch and Rott = POTT || DBOTT
- v. If Rsh is TRUE and Rott is TRUE Store OTT in DBOTT. Redirect to Sa.

3.2.3 The Response Phase

- i. Sp receives access request to Cu. Sp creates session.
- ii. Provide access to Cu.

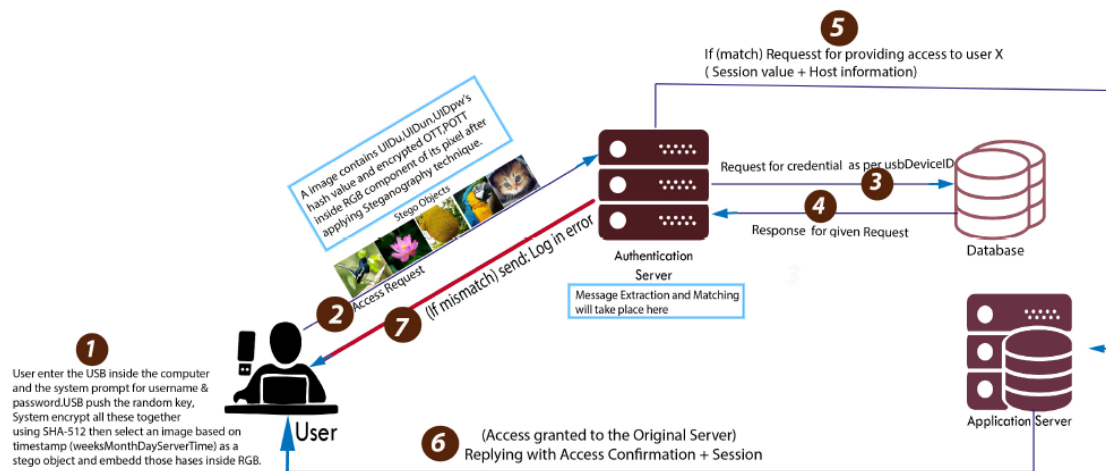


Figure 3.2.3: Proposed SMFA Model

3.2.4. The Recovery Phase: USB Lost or Damaged

For the event of the loss or breakage of the USB device, this research finding has come to a conclusion by suggesting two different approaches. Users shall register another additional USB to reduce the impact of this sporadic incident. Registration process of multiple devices will allow users to register at least two USB sticks so that if one is ever lost or damaged, the user can log in with the other device. The reporting mechanism must be effectively convenient for users, and the authentication server shall revoke the stego validator and OTP of the lost USB device after confirming that the loss or breakage report is true.

So, using multiple registered USB devices is the recommended practice found by this study; which will reduce the hassle and need for account recovery. However, to some extent this method might not be sufficient. For tackling such inadequacy, re-registration process can be adopted. Although it is subjected to the organization's user case, security requirement and policies. Reissuing the account information and full identity confirmation may increase the service overhead. The procedure of SMFA does not set this as a recommendation but a possible alternate mechanism. Organization's will decide which one to adapt by considering the risk balance and security policies.

Figure. 2 shows the architecture of the proposed model. This model is constructed in such a way that it uses the SHA- 512 HASH function and RSA encryption to hide the original data. This model also uses multiple images from which a single image is used to hide the presence of data through the most suitable steganography technique. POTT is responsible for the selection of the image for the application of steganography. There are many data-hiding techniques in the field of image steganography. The LSB replacement algorithm is the simplest and most popular among them. For this proposed model, any image steganography technique with a good security level can be used. The security measurement can be done by considering the PSNR (peak signalto- noise ratio) and MSE (mean square error) of the Cover object and the Stego object. The formula for calculating the PSNR [37] between two images is:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{ dB}$$

PSNR is calculated in dB. PSNR dep PSNR is calculated in dB. PSNR depends on MSE. The mathematical definition of MSE [38] is:

$$MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i, j) - Y(i, j)]^2$$

In the above-mentioned equations, i, j refers to the pixel value at positions i and j of the Cover image, while b_{ij} refers to the pixel value at positions i and j of the Stego image. Research proves that if the PSNR between the two images (Cover image, Stego image) becomes higher than 40dB, it can be considered as of good quality [37].

This means that the higher the PSNR, the lower the imperceptibility. However, the PSNR between two same and unchanged pictures is infinity. So, any image steganography technique that achieves at least 40dB PSNR can be used in this model to obtain the goal of hiding the presence of credentials. It is recommended that the algorithm having the maximum PSNR be used to achieve the least imperceptibility, which indicates the

maximum-security level. The general credentials-hiding procedures used in this model are as follows:

$$H(\text{UID}_u, \text{UID}_{un}, \text{UID}_{pw}) \longrightarrow H(h1).$$

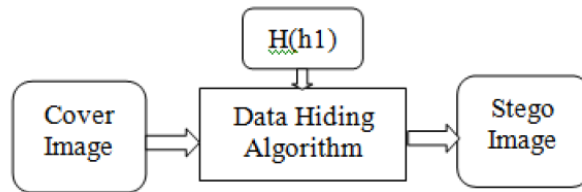


Figure 3.2.4: Steganography Process

It can be seen in figure 3.2.4 that stego image is the final output after applying suitable steganographic algorithm.

CHAPTER 4

MODEL ANALYSIS

This model establishes a shared key between three principals and a database with the assistance of an authentication server and an application server. It is based on the shared key but makes use of the timestamp as nonce. The model described above is provided with three principals- U, AU, and AP. Next, KUAU, KUAP, and KAUPU are their shared keys; KU, KAU, and KAP are their public keys; and DB is the authentication server database. Moreover, U generates the timestamp TU; AU generates the timestamp TAU; and AT generates the timestamp TAP. Furthermore, U generates the lifetime L. The third, fifth, and sixth messages are used only if mutual authentication is required. Here, OTT as the one-time token is generated by Stego validation and POTT is previously used OTT stored in Stego validation is used. This message sequence is represented below. First, U sends an encryption message containing a timestamp, a lifetime, a session key for U, AU and UID,

Message 1. $U \rightarrow AU : \{ T_U, L, K_{UAP}, \{ T_U, OTT, U, U_{ID}, U_{PASS}, U \}_{K_{AU}}, K_{AU} \}_{K_{AUDB}}$

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

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

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

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

Message 6. $AU \rightarrow U : \{ \{ T_{AU}, U \} + 1 \}_{K_{AU}}$

UPASS with OTT. It is encrypted separately with the public key of AU that only can read the AU decrypt with the private key. AU first decrypts it and again sends to DB for matching the UID, UPASS, and the respective OTT with the stored POTT. If this session has been created recently, DB uses the enclosed key to decrypt the authenticator message and match it. Then, it will replay with the authenticator's recent timestamp.

Once the principal AU is satisfied, it will send a message to AP with a timestamp, the session of U, OTT, POTT with also its own shared key decrypt with the private key of AP. The full message decrypt with the shared key between AU and AP checks it: if the session is also created recently, then it will decrypt it. Once this principal AP is satisfied, it will proceed to use the session key of U and give access to the replay of U.

So, if it can be proved that the principal AU believes the prin principal U, and the principal AP believes AU, then the principal AP must believe in the principal U. Hence, the model will be validated. BAN logic has been used to prove the session key agreement between our principles. According to BAN logic, some rules are given below to help us understand the efficiency of whole model.

4.1 BAN Logic

i Message-meaning rules:

For shared keys:

$$\frac{P \text{ believes } P \longleftrightarrow Q, P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$

For public keys:

$$\frac{P \text{ believes } \longleftrightarrow Q, P \text{ sees } \{X\}_{K^{-1}}}{P \text{ believes that } Q \text{ said } X}$$

For Public keys:

$$\frac{P \text{ believes } Q \longleftrightarrow P, P \text{ sees } \langle X \rangle_Y}{P \text{ believes that } Q \text{ said } X}$$

ii Nonce-verification rules:

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

iii Jurisdictions rules:

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

Figure 4.1: Rules in BAN Logic

The following notation is going to be used in the in-depth analysis.

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
UID – User ID
UPASS – User password
TAU – Authentication timestamp
TAP – Application timestamp
TU – User timestamp
KUAU – Shared key between user and authentication server
KUAP – Shared key between user and application server
KAUDB – Shared key between authentication and database
server
KAUAP – Shared key between authentication server and application
server
KAU – Public key of authentication server
KAU – Secret key of authentication server
KAP – Public key of application server
KAP – Secret key of application server
KADB – Public key of authentication server database
KDB – Secret key of authentication server database

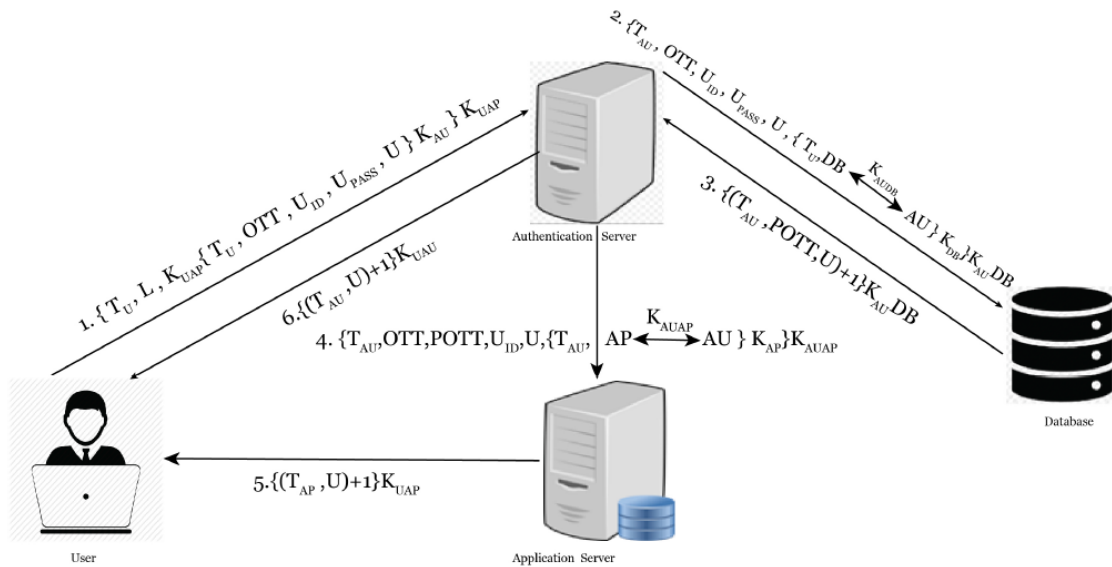


Figure 4.1: Model with required Notation

To analyze this protocol, the following assumptions has been provided:

AU believes AU	$\longleftrightarrow^{K_{UAU}}$	AU believes fresh (T_U)
DB believes DB	$\longleftrightarrow^{K_{AUIDB}}$	DB believes fresh (T_{AU})
AP believes AP	$\longleftrightarrow^{K_{AUAP}}$	AP believes fresh (T_{AU})
AU believes U controls (AU	$\longleftrightarrow^K \rightarrow U$)	U believes fresh (T_{AP})
DB believes AU controls (DB	$\longleftrightarrow^K \rightarrow AU$)	
AP believes AU controls (AP	$\longleftrightarrow^K \rightarrow AU$)	

The first three assumptions on the left are about the shared keys between the three principals and the database. The four assumptions on the right show that the principals and the database server believe that timestamps generated elsewhere are fresh, thereby indicating that the model relies heavily on the use of synchronized clocks. The next group of three assumptions indicates the trust that the principals and the DB have in the server to generate a good encryption key. The analysis of the idealized model is conducted through the implementation of propounded rules of the assumptions. In the interests of brevity, numerous formal details that are necessary for the machine-assisted proof are delineated for Message 1, Message 2, and Message 4 only. Similar details have been omitted later on.

The main steps of the proof are as follows: AU receives Message 1. The annotation rules yield

$$AU \text{ sees } \{T_{U, L, K_{UAP}}, \{T_u, OTT, U_{ID}, U_{PASS}, U\}_{K_{AU} K_{UAP}}\}$$

Nonce-verification rules applies and yields -

$$AU \text{ believes } U \text{ believes } (T_u, (AU \xleftrightarrow{K_{UAU}} U))$$

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

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

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

$$AU \text{ believes } U \text{ believes } (AU \xleftrightarrow{K} U)$$

Deriving the more concrete-

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

Finally, the jurisdiction rule applies and yields the following:

$$AU \text{ believes } AU \xleftrightarrow{K_{UAU}} U$$

This concludes the analysis of Message 1.

U passes UID, UPASS, and OTT on to AU, together with a message containing a timestamp. Initially, AU can decrypt only the following message

$$U \text{ believes } AU \xleftrightarrow{K_{UAU}} U$$

Logically, this result is obtained in the same way as that for Message 1. Nonce-verification and jurisdiction are postulated through the meaning of the message. Knowledge of the new key allows AU to decrypt this message. Through the meaning of the message and the postulated nonce-verification, the following can be deduced:

$$U \text{ believes that } AU \text{ believes } (AU \xleftrightarrow{K_{UAU}} U)$$

Now, for identifying UID, UPASS, and OTT, AU sends an encrypted message to the database. As mentioned earlier, DB also believes AU and gives a reply with confirmation. Next, AU sends a message to AP for confirming the identity of U and gives access to U by generating a session for U. Applying these three rules according to the previous ones, it is proved that

AU believes that AP believes $(AP \xleftrightarrow{K_{AUAP}} AU)$

We deduce:

AP believes that AU believes $(AP \xleftrightarrow{K_{AUAP}} AU)$

Here, with $(AP \xleftrightarrow{K_{AUAP}} AU)$. AU sends a message to AP, allowing it to be replaced by U. (Message that will actually send about U's UID, UPASS, and OTT). So, it can be inferred that:

AP believes that AU believes U

And the following hypothesis is obtained –

AP believes that AU controls $(AP \xleftrightarrow{K} AU)$.

Again, with $(AP \xleftrightarrow{K} AU)$. AU sends a message to AP, allowing it to be replaced by U. (Message that will actually send about U's UID, UPASS, and OTT). This results in the derivation of the following:

AP believes that AU controls U.

So, the jurisdiction rule applies and yields the following:

AP believes U.

CHAPTER 5

RESULT AND DISCUSSION

In order to highlight the superiorities of the proposed scheme, this section will discuss security, performance analysis, and results. Security analysis defines the resistance level against attacks, while performance analysis compares the proposed scheme with some other schemes.

5.1 Security Analysis

The proposed SMFA model has been analyzed from the security perspective by considering attack scenarios. SMFA prevents some attacks and reduces security risk. The following types of attacks can be avoided or mitigated by using this model.

5.1.1. Replay Attack

To cite for instance, an attacker A is considered for the purpose where Attacker A will intercept the communication between the user and the authentication server. This attacker can obtain Stego image files. In order to log in to the server, this attacker will have to resend the packet to the server. However, the attacker would not be successful in this case because the POTT is now changed. Here, POTT will be placed by a new OTT for every successful authentication and OTT is dynamic. Thus, the replay attack is prevented.

5.1.2 Man-in-the-Middle Attack

The man-in-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims (client and the AS) and relays messages between them, making them believe that they are talking directly to each other over a private connection when, in fact, the entire conversation is controlled by the attacker. The attacker must be able to intercept all the messages going between the two victims and inject new ones. The proposed scheme creates a strong barrier against a MITM attack and reduces the risk caused by this attack. This scheme uses steganography to hide the existence of credentials. Even if the SSL breaks and the existence of credentials is revealed, the attacker

would not be able to manipulate the credentials. The reason is the complexity used in this scheme. To illustrate, let it be assumed that Attacker A wants to gain the confidential information and receives a packet of a group of images. The first challenge is to identify the carrier object (ICc), then to retrieve the secret hash (Rh), and finally, to perform hash recovery (Hr). It is not practical to break these challenges. Again, though these challenges are successfully completed, the OTT and POTT are totally dynamic and randomly generated. Thus, any MITM attack is not feasible for the proposed scheme.

5.1.3 Impersonating Attack

An attacker will not be able to impersonate the original user to log in the server by sending a valid credential to the server even if the username and password are valid. It happens since the illegal user cannot process POTT, making it impossible to pass the authentication procedure.

5.1.4. Offline Dictionary Password Attack

In the proposed scheme, if attacker A tries to login through the dictionary password, the attacker may be able to generate UIDun and UIDpw, but would not be able to use a legally registered USB device. Even in case of USB cloning, it would not be possible to pass the authentication—the generation of OTT and POTT just would not be feasible. Hence, it can be confirmed that the proposed scheme makes it computationally infeasible for an attacker to pass authentication without the appropriate valid user.

5.1.5 DOS Attack

The model uses a dedicated authentication server whose responsibility is to verify the authenticity and convey the verification status to the application server. Using different servers like this actually prevents any denial of service. A USB device is also being used as a factor. Even if multiple random requests could be sent to the server, it would not pass the authentication server without the physical USB device. Therefore, there would not be any effect on the application server. From the discussion made above, it can be summarized that the proposed model creates resistance against replay, impersonating, offline password

guessing, and DOS attacks, as well as reduces the risk caused by any MITM attack. The following table (see Figure 5.) visualize the comparison between existing and proposed models based on different attack scenarios.

TABLE 5.1: DEFENSE LEVEL COMPARISON

	Smartcard-based solution [34]	OffPAD [22]	Google 2-step [6]	Proposed model (MFAS)
Resist replay attack	No	Yes	Yes	Yes
Resist MITM attack	No	No	No	Yes
Resist impersonating attack	No	Yes	Yes	Yes
Resist password-guessing attack	Yes	Yes	Yes	Yes
Resist DOS attack	Yes	Yes	No	Yes

5.2 Performance Analysis

This subsection reports the performance from the perspectives of the user and the organization. The proposed model uses a USB device that generates a dynamic one-time token which is also used to validate the user's identity. This OTT does not need any clock synchronization. To provide data privacy, steganography is used, which makes this model different from others. Jung H. et al. and Hwang and Li et al. used a smartcard for the authentication factor, but the authors did not consider the factors of privacy and computational cost [34]. The model developed by Varmedal et al. faces clock synchronization issues [22].

P1: multi-factor security

P2: No need of clock synchronization

P3: User is allowed to select a user id and password and/or a USB device, not decided by the authentication server

P4: Low computational cost

- P5: Ensure data confidentiality in the transport layer
- P6: Supports password changes or device replacement
- P7: Authentication uses the physical device

The following tables (see Figure 6. and Figure 7.) compares the performances of different protocols based on the schemes described above.

TABLE 5.2: PERFORMANCE COMPARISON AMONG OTHER ESTABLISHED PROTOCOLS

	P1	P2	P3	P4	P5	P6	P7
H. Jung et al. [35]	Yes	Yes	Yes	No	No	Yes	Yes
A. Jyoti Choudhury et al. [36]	Yes	No	No	No	No	Yes	No
Hwang & Li, [34]	Yes	Yes	Yes	No	No	Yes	Yes
Varmadel et al.'s OffPAD [22]	Yes	No	Yes	Yes	No	Yes	Yes
FIDO U2F [7]	Yes	Yes	Yes	No	No	Yes	Yes
Proposed Model (MFAS)	Yes	Yes	Yes	No	Yes	Yes	Yes

Though the computational cost for this model is a little higher than that in the model devised by Varmadel et al. [22], the overall performance is better than any other model that has so far been mentioned. The slightly higher computational cost in this model can be attributed to the addition of steganography. To best of our knowledge, the proposed scheme is the first authentication model that uses a USB device for authentication and steganography to ensure credentials privacy for a secure application or network.

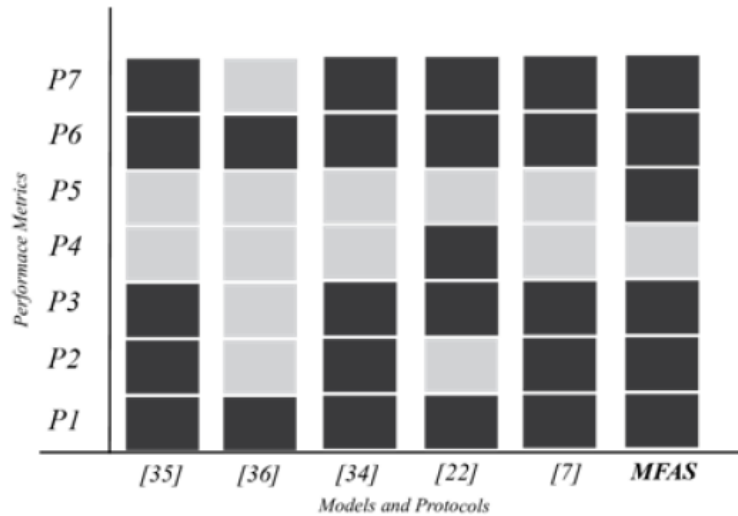


Figure 5.2: Visual Representation of the Overall Performance of SMFA

From the detailed comparisons and results based on security and performance, it can be seen that the proposed MFA model is secured against the already explained attacks and safeguards user credentials from the malicious party. Here, a dedicated authentication server is used for the authentication process and a USB device to mitigate the risk posed by the conventional one-factor authentication system. To ensure cryptography, the SHA-512 hashing function has been used, while steganography is applied to ensure transport-layer security. As illustrated in Figure 5, the proposed scheme resists all major attacks when all other relevant schemes fail to do so. Although this scheme requires slightly higher computation costs compared to most other schemes, the devised model's overall performance and security strength are comparatively good.

CHAPTER 6

CONCLUSION

An authentication protocol named SMFA is proposed which is capable of resisting various attacks and is superior to other protocols. The SMFA protocol is based on a USB device, Cryptography and Steganography in order to implement secure credential transmission and authentication. In this study, it has been observed that integration of a steganography and authentication mechanism results in better security and resolves existing security concerns. The protocol is efficient and can protect the integrity, confidentiality, and authenticity of the data transmitted over the internet. The BAN-logic method is used to validate the security features and key agreement procedure for the proposed SMFA protocol. Extensive analysis and comparative results indicate that the use of USB in client side, dedicated authentication server, and employing steganography in transmission process has a high impact on hardening the security hence user trustworthiness. Finally, research findings concluded that the proposed SMFA is impregnable to user impersonation attacks, replay attacks, DOS attacks, session-hijacking attacks, offline password guessing attacks and also provides mutual authentication. Although the protocol requires slightly higher computational cost due to multi-layer protection, it reduces the frequency of MITM attacks and damage caused by the same. To surmount, it is also intended to implement and deploy the proposed scheme in the real-world application and put forward possible improvement at a future date.

CHAPTER 7

ACKNOWLEDGEMENT

The authors would like to thank and show gratitude to the Department of CSE of Daffodil International University, Dhaka, for providing academic support.

References

- [1] R. Morris and K. Thompson, "Password security: a case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, Jan. 1979.
- [2] J. Bonneau, C. Herley, P. C. v. Oorschot and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, 2012, pp. 553-567.
- [3] "2017 Annual Cybersecurity Threat Report | eSentire," eSentire Managed Detection and Response. [Online]. Available: <https://www.esentire.com/resources/knowledge/2017-annual-threatreport>. [Accessed: 26-Sep-2019].
- [4] "Yahoo 2013 data breach hit 'all three billion accounts'," BBC News, 03-Oct-2017. [Online]. Available: <https://www.bbc.com/news/business-41493494>. [Accessed: 01- Sep-2022].
- [5] "Uber Data Breach Exposed Personal Information of 20 Million Users," Fortune. [Online]. Available: <http://fortune.com/2018/04/12/uber-data-breach-security/>. [Accessed: 25-Sep-2022].
- [6] Google 2-Step Verification. [Online]. Available: <https://www.google.com/landing/2step/>. [Accessed: 5-Jan-2022.]
- [7] "U2F - FIDO Universal 2nd Factor Authentication," Yubico. [Online]. Available: <https://www.yubico.com/solutions/fido-u2f>. [Accessed: 14Sep-2022].
- [8] S. Sahute, S. Waghmare, and A. Diwate, "Secure Messaging Using Image Steganography", *International Journal of Modern Trends in Engineering and Research*, vol.2,no.3, pp. 598–608, 2015.
- [9] J. Baek, C. Kim, P. S. Fisher, and H. Chao, "(N, 1) secret sharing approach based on steganography with gray digital images," 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, 2010.
- [10] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.
- [11] A. K. Das, "A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1377–1404, 2015.
- [12] M. N. Babu, A. S. N. Chakravarthy, and C. Ravindranath, "The design of a secure three factor authentication protocol for wireless sensor networks," 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017.
- [13] J. Shen, D. Liu, S. Chang, J. Shen, and D. He, "A Lightweight Mutual Authentication Scheme for User and Server in Cloud," 2015 First International Conference on Computational Intelligence Theory, Systems and Applications (CCITSA), 2015.
- [14] J. H. Yang and P. Y. Lin, "An ID-Based User Authentication Scheme for Cloud Computing," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014
- [15] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme," *Computer Communications*, vol. 32, no. 4, 2009, pp. 583-585.

- [16] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," in *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629-631, May 2004.
- [17] Liu, Wenhao, "An improved authenticated key agreement protocol for telecare medicine information system" *SpringerPlus* vol. 5 555, 2016.
- [18] C. Huang and J. Li, "One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS," 21st International Conference on Advanced Information Networking and Applications (AINA '07), Niagara Falls, ON, 2007, pp. 482-489.
- [19] J.-K. Tsay and S. F. Mjøl̄snes, "A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols," *Lecture Notes in Computer Science Computer Network Security*, pp. 65–76, 2012.
- [20] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," 2011 IEEE Asia-Pacific Services Computing Conference, 2011.
- [21] M. Kumar, "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597–600, 2004.
- [22] K. A. Varmedal, H. Klevjer, J. Hovlandsvåg, A. Jøsang, J. Vincent, and L. Miralabé, "The OffPAD: Requirements and Usage," *Network and System Security Lecture Notes in Computer Science*, pp. 80–93, 2013.
- [23] 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.
- [24] M. Alhaidary and S. M. Rahman, "Security vulnerability analysis and corresponding mitigation for password-based authentication using an offline personal authentication device," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016.
- [25] W. A. Hufstetler, M. J. H. Ramos, and S. Wang, "NFC Unlock: Secure Two-Factor Computer Authentication Using NFC," 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017.
- [26] W. Mao, *Modern cryptography: theory and practice*. Upper Saddle River, N.J: Prentice Hall, 2011.
- [27] Liu, Wenhao, "An improved authenticated key agreement protocol for telecare medicine information system." *SpringerPlus*, 5.1, 2016:
- [28] B. Madhuravani, P. B. Reddy, D. S. R. Murthy, and K. V. S. N. Rama Rao, "Strong authentication using dynamic hashing and steganography," *International Conference on Computing, Communication Automation*, 2015.
- [29] S.-H. Gunawardena, D. Kulkarni, and B. Gnanasekariyer, "A Steganography-based framework to prevent active attacks during user authentication," 2013 8th International Conference on Computer Science Education, 2013.
- [30] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, 2014, pp. 1-5.

- [31] H.-D. Ihmaidi, A. Al-Jaber, and A. Hudaib, "Securing Online Shopping using Biometric Personal Authentication and Steganography," 2006 2nd International Conference on Information Communication Technologies.
- [32] T. Mantoro, D. D. Permadi, and A. Abubakar, "Stegano-image as a digital signature to improve security authentication system in mobile computing," 2016 International Conference on Informatics and Computing (ICIC), 2016.
- [33] C. Danuputri, T. Mantoro, and M. Hardjianto, "Data Security Using LSB Steganography and Vigenere Chipper in an Android Environment," 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), 2015.
- [34] Min-Shiang Hwang and Li-Hua Li, "A new remote user authentication scheme using smart cards," in IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, Feb. 2000.
- [35] H. Jung and H. S. Kim, "Secure Hash-Based Password Authentication Protocol Using Smartcards," Computational Science and Its Applications - ICCSA2011 LectureNotes in Computer Science, pp. 593–606, 2011.
- [36] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," 2011 IEEE Asia-Pacific Services Computing Conference, 2011.
- [37] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," in IEEE Transactions on Communications, vol. 43, no. 12, pp. 2959-2965, Dec. 1995.
- [38] Zhizhong Zhe and Hong Ren Wu, "A new way of pooling: starting from an image quality measure," Proceedings 7th International Conference on Signal Processing, 2004.

SMFA: Privacy Preserving Multi-factor Authentication Model Based on USB, Cryptography and Image Steganography

ORIGINALITY REPORT



PRIMARY SOURCES

1	"Cyber Security and Computer Science", Springer Science and Business Media LLC, 2020 Publication	6%
2	hal.inria.fr Internet Source	3%
3	Mada Alhaidary, SK.Md. Mizanur Rahman. "Security vulnerability analysis and corresponding mitigation for password-based authentication using an offline personal authentication device", 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016 Publication	2%
4	Touhid Bhuiyan, Afjal H. Sarower, Rashed Karim, Maruf Hassan. "An Image Steganography Algorithm using LSB Replacement through XOR Substitution", 2019	2%