Daffodil International University

An Enhancement of Kerberos Protocol Using Biometric Template and Steganography

SUBMITTED BY

MUNIRA TABASSUM MOU
ID: 153-35-1387

SUPERVISED BY

MD. MARUF HASSAN
Assistant Professor
Department of Software Engineering
Daffodil International University

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall - 2019

DECLARATION

I, hereby, declare that I have taken this thesis under the supervision of **Mr. Md. Maruf Hassan, Assistant Professor, Department of Software Engineering, Daffodil International University.** I also declare that neither whole document nor any part of this thesis have been submitted elsewhere for award of any degree.

MUNIRA

Munira Tabassum Mou
Student ID: 153-35-1387
Batch: 18th Batch
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Certified by:

10/12/19

Md. Maruf Hassan
Assistant Professor
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

ACKNOWLEDGEMENT

First of all, I am very grateful to my Almighty Allah for giving me the opportunity to walk through the final year. I have learnt economics, politeness, ethics, and so on in the previous year of my university life. I am grateful to all of my teachers for this.

I would like to express my special thanks of gratitude to my supervisor, Mr. Md. Maruf Hassan, Assistant Professor, DIU who gave me the golden opportunity to do this wonderful thesis on the topic of Secure Authentication which also helped me in doing a lot of Research and writing of this thesis therefore I have come to know so many new things for which I am so thankful to him.

Secondly, I acknowledge the authority of Cyber Security Center, DIU (CSC, DIU) who have given me the permission to conduct my examination and for the cooperation and support to execute the study.

Besides my supervisor and the authority of CSC, I would also like to thank my parents and friends who helped me a lot to finalize this thesis within the limited time frame.

.

TABLE OF CONTENT

LIST OF FIGURE

ABSTRACT

Kerberos, a renowned token based authentication protocol, which is famous since mid-80 for its cryptographic process, assurance of privacy, and data security for identifying appropriate users. Due to its versatile characteristics, users of the system often need to remember complex passwords as the good practice of the method requires update of the same within a defined time-frame which becomes bit difficult for users to cope up with. At the same time, it also not provides adequate channel security to transmit the user credential between the pathway of the client and server. Therefore, researchers are trying to find out a simple solution where user does not necessitate memorizing the passwords where it could guarantee better user validation. In this paper, an enhancement of Kerberos authentication model has been proposed where biometric template and Steganography are incorporated to solve the existing weaknesses. Instead of taking username and password, the new solution will take a pair of random fingerprints from the user and convert it into a hash. It will then embed the hash in the randomized image and send it to the server for authentication. A security analysis of the proposed protocol is proven using BAN logic in this article where it ensures reliability, practicability and security of the enhanced Kerberos protocol.

Keywords: Cyber Security; Authentication; Kerberos Protocol; Image steganography

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

In this modern era, the demand of online applications is increasing dramatically at all domains especially in business due to its manageable, usable, and portable characteristics to satisfy the consumer's expectation. The web applications are hosting through a web server and it communicates and also provides services to its user through the public channel. There may have a chance for the attacker to intercept and modify the messages transmitted between the server and user if any vulnerability exists in the system (Kumar et al., 2018). Different types of users such as end users, support user, privileged user, admin user, etc. are working in the same platform to execute their roles for the smooth operation of the business. Therefore, it requires proper user authentication to ensure the right access for the valid stakeholders in the system as no intruders from cyberspace can claim themselves as legal user. Authentication is the essential protection mea-sure against illegal access into a system or device where an entity validates their uniqueness (Ometov et al., 2018). Generally authentication process refers to username and password of a user for accessing in the system with the provided authorization (https://www.Oreilly.com/library/view / com ptia securitytmreview/9781118113523/xhtml/sec34.html, 2019). Though Password authentication is a conventional and reliable process for user identity, there have some problems with the user-generated username and password due to the difficulties of memorization and easy to crack with brute-force attack (Lashkar et al., 2009) and the complications of handling specific username and password for individual accounts.

In the last 50 years researchers gave different solution of secure authentication using multiple complex authentication factors or credential protection mechanisms like as text based password, hard and soft token, biometric finger-print and palm-print, behavioral and contextual authentication, keystroke dynamics and so on (Van Dijk et al. 2014, Shanmugapriya et al. 2009, Brosto et al. 2000, Kesanupalli 2010, Hessle et al. 2015, Ashibani et al. 2019). Including these existing solutions, biometric authentication factors are giving more accurate clarification of legal users where other solution has remains flaws for the improvement of security, user experience, unnecessary remembering and reduced operating costs. In the other hand, the solution with biometric fingerprint is also extensively used in the identity authentication system due to its unique, stable and irreplaceable physical characteristics (Koong et al., 2014). In the field of biometric fingerprint genuine data recognition is must where attackers can acquire not more than five fingerprints (Harkeerat Kaur et al., 2019). It is however well-known those biometric templates cannot be revoked and republished as easily as classical keys or tokens (Shi et al., 2019). However, users enjoy biometric as a quick and easy process that does not deal with the inconvenience of creating or remembering and the fingerprint scanning is more secure than any password or pin. A biometric authentication system can confirm individual identities based on the physiological or behavioral characteristic that could offer a strong and convenient security solution. To design a biometric system, security and recognition accuracy are the two most important aspects (Alsaadi et al., 2015). This paper tries to merge some factors that do not need to remember by the cased users as well as it is extremely difficult to distribute, steal or clone. This work uses a portable device as first factor and ten biometric fingerprints as the second factor as it is almost impossible to steal every single fingerprint of any individual user. This work used Kerberos protocol which has been proven with logic to ensure the data security with Image Steganography techniques.

In every solutions, it is must need to evaluate security protocols. To evaluate security protocols, Burrows, Abadi and Needham produced a formal logic of authentication called BAN logic in 1989 (M. Burrows et el., 1990). Kerberos is one of the most common key distribution protocols that has a full BAN guarantee to analyze the cryptographic protocols (Mukhamedov, 2005). Lo is concluded that Kerberos is the strongest form of authentication (Lo et al., 1997). Though Kasslin and Tikkanen proved that in some cases Kerberos suffers from replay attack (Kasslin et al. 2003, Fan et al. 2009). To prevent replay attacks, this work includes image Steganography techniques. Unlike cryptography, Steganography is another way to hide the data that safeguards the secret information through a medium and the existence of the secret information which is revealed by the deliberate receiver (Rai al., 2015). Steganography means to hide the message's existence in another medium such as audio, video, image, and communication (Hussain et al., 2015). Data hiding can be achieved by implementing the Steganography and cryptography together that is resulting in greater data security as well as integrity (Rai et al., 2015).

1.1.1 Authentication

Authentication is a process that is used to define and verify a client and/or server identity in the computer network. Although the username and password combination is a common way to authenticate the user's identity, there have been many other forms of authentication methods. As instance passcode is used to unlock phone, laptop, computer and other network devices. On the other hand, biometrics features also applied for authenticating user's identity. In the 1960, computers were a much larger, extraordinarily expensive and relatively slower than today which was beyond the reach of most people, mainframe computers could be usually found in some universities and largest companies. Because of the expensive computer availability, MIT has built time-sharing operating systems that would allow multiple users to share the resources that a single computer offers. As giving solution of these problems in 1961, a MIT scientist, Professor and one of CTSS founders Fernando Corbato used passwords to secure user files on this multi-user time-sharing system Nonetheless, passwords were the first tool used to authenticate computers more than 50 years ago, they quickly revealed some problems that need to be addressed in order to increase security.

Human relationships are trust-based, so the true authentication history goes back long before the first written documents referencing it. Therefore, the creation of culture has become more complicated with the passage of time. Therefore, as society has become more complicated, new ways have been developed to verify people. In the past, humans formed tribe who found ways to authenticate each other at night using specific sounds or keywords. Though it was easy to authenticate by simply looking at the well-known people, it is quite difficult to authenticate unknown people without knowing something about them. Most likely, in the late B.C. And the beginning of A.D. Periods, regular keywords were used by Roman soldiers. A general in the Roman army, for example, had led thousands of soldiers, but was unable to know them all personally if a soldier walked up the street and claimed to be part of his army, he needed some way to prove it. In those cases, they used specific keywords. Besides keywords, society has developed many authentication factors, such as personal identification numbers (PIN), passwords and other types of unique ID. These analog forms of identification brings us to the age of modern civilization which allow till now even strangers to authenticate one another and in which overcome the weakness of traditional keyword methods.

The key concept contributed to most of the other operating systems by continuing to develop with added security. In a word, the development of hash-based password storage systems by Morris in the 7o's has gone a long way to make authentication systems safer than before. As digital systems gain password-based protection for security, researchers and hackers have also found ways to exploit them as well, prompting the industry to pursue ever more reliable authentication methods. To combat this in 1980's, many different OTP (One-time passwords) standards develop along with the emergence of two or multi-factor authentication as well. Since 2000, MFA is essentially the combination of more than two authentication factors for ensuring better reliability for the actual users. Lastly, these approaches incorporate with the biometric features for the smartphone and computer devices therefore each user can use a password, specific token or biometric features for authenticating individual users' identity.

1.1.2 Kerberos Protocol

Kerberos is a network authentication protocol which is developed by the Massachusetts Institute of Technology (MIT) for authenticating requests for service using secret key cryptography to provide trusted hosts with security over an insecure network. This protocol uses tickets to authenticate a client and prevent the network's transmission of plain text passwords. Kerberos V1-V3 started to develop in 1983 by Massachusetts Institute of Technology (MIT) for protecting network services provided to the Project Athena. The Needham –Schroeder symmetric key protocol of

1978 was used as a starting point for this protocol. Kerberos V4 was primarily designed by Steve Miller and Clifford Neuman, who first publicly presented the Usenex conference paper in 1988, making Kerberos one of the most commonly used protocols. In 1993, Neuman and Kohl released Kerbeors v5 with the aim of addressing v4 limitations and security issues as RFC 1510. In 2005, the update v5 was released with RFC 4120 by the Internet Engineering Task Force (IETF) Kerberos working group, which added numerous features and updated various cryptographic standards to keep Kerberos significant and up to date. The Kerberos protocol infrastructure primarily consists of Kerberos itself, secured redundant authentication servers, a centralized account and password store that configures authentication mechanisms.

1.1.3 Image Steganography

Steganography is a method for hiding the text that is only revealed to the intended recipient. At the present security system, there are many forms of steganography that use many different mediums to transmit hidden information Steganography provides high carrier capacity to keep embedded message invisible and to preserve cover press fidelity. Steganography has been derived from Greek word "Stego" which means "Covered" and "Graphia" which means "writing" (*UKESSAYS*). It is an ancient secure strategy for hiding data. Herodotus referred to the tradition of secret writing in one of his seminal works of history named Histories during the 400 B.C. In his writings he has mentioned that for the use of Steganography techniques, the servant had travelled freely with secret messages between the borders without carrying anything controversial. It came to the present to the United States as early as the Revolutionary

War, during which it took the form of secret message drops, code words, and invisible inks used by General George Washington and a team of spiesFollowing the tragedy of 11 September 2001, investigations revealed that terrorists from Al'Queda were allowed to transmit images containing hidden messages via usenet. Steganography provides high carrier capacity to keep embedded message invisible and to preserve cover press fidelity. This method's efficiency is that for embedding one could not realize that which media file has been altered therefore human visual system won't be able to distinguish between the image before modulation and the image after modulation. Due to the affordable price of digital cameras today the availability of natural images is not a problem therefore natural images are the best candidates for cover image since they have higher resolution providing flexibility and other necessary aspects. If the name of the owner is found in the digital image and the actual image, the original data will be distorted or lost and if the malicious user knows if there is any modification, the Steganographic approach will be defeated and less successful. The embedded message is very fragile and if any modification is made to the stego picture the whole secret message are distorted. The effectiveness of Steganographic techniques are lies on the ability to be fooled an unintended user where the layers of communication can be more than one layer.

Many forms of covers exist for hiding messages, from image, video, and sound to text to IP packets. Such as LSB encoding, are considered especially weak, whereas transform domain and feature modification techniques may be slightly stronger. have contemplated developing steganography that hides messages from computers rather than hiding them from humans, and have developed more advanced techniques for hiding data within JPEGs and within Internet traffic.

1.2 MOTIVATION OF THE RESEARCH

In online based modern civilization, authentication is needed for every aspects of our day to day life. It is also a trouble to memorize individual username, password and PINs for separate systems. In the previous researches has been shown different solutions however there have flaws. Therefore, author of this thesis motivates to overcome these problems with an effective accommodation.

1.3 PROBLEM STATEMENT

After reviewing the above literatures, it is found that it is difficult to memorize various usernames and passwords for individual systems and though the password is so strong however it can be shareable. Data security also hampers if the communication paths are insecure.

1.4 RESEARCH QUESTION

1. Is this model logically proved by BAN logic?
2. Is our proposed model giving solution to the drawbacks of password?
3. Is this proposed model ensure data security?

1.5 RESEARCH OBJECTIVES

1. First objective of this paper is to enhance Kerberos protocol with the proof of BAN logic implementations.
2. Second objective of our paper is to overcome the memorization problem using Biometric Template instead of Username and Password.
3. The last objective of our paper is to ensure data security by using Image Steganography Techniques.

1.6 RESEARCH SCOPE

The main focus of this study is to develop an effective authentication system based on the Biometric Template. Image Steganography for secure data transmission and Kerberos Protocol for mutual authentication will be used by the system. The proposed system ensures that encryption is secure and reliable than recalling or memorizing. For all current web-based applications and systems, this proposed process can be used. Many analyzes, hypotheses and opinions have rendered a fair and practical development consideration.

1.7 THESIS ORGANIZATION

The manuscript is organized as follows. Chapter 2 outlines the previous related researches to the concept of Biometric fingerprint scanning issues, multi factor Kerberos protocol and specific contributions. It is followed by a discussion on the proposed template protection concept and architecture for remote authentication is presented in Chapter 3 also the analysis of the BAN logic into the proposed model. The technique is experimentally discussed in Chapter 4 with security and privacy issues. Section 5 concludes the study with future work.

CHAPTER 2

LITERATURE REVIEW

In our research time we observe that numbers of research has been conducted on authentication system and its models and tools. The related work of this research is discussed below:

2.1 EXISTED MODEL ON AUTENTICATION SYSTEM

In order to maintain secure communication through public channels and to ensure information security for sensitive online transactions, the user needs to be validated through an effective authentication mechanism. As an active identification process, three types of authentication schemes have been widely used as text-based, two-factor token-based, biometric template-based authentication in our daily lives over the past decades where these schemes have been con guarded for multi-server environments (Leu et al. 2013, Tsai et al. 2013, Yang et al. 2008, Chen et al. 2014). The following sections discuss details of conventional authentication schemes since the middle of the 19th century.

2.1.1 Text-Based Authentication

The perspective of computer systems and applications, text-based schemes based on passwords, PINs, code words are commonly used for being authentication that have been conducted with the past researches. As instance, Durbadal Chattaraj et al.

proposed key exchange mechanism by dint of both public and private key cryptography and a dynamic password-based two-server authentication (Chattaraj et al., 2018), where they could not clarify the protection public channels from attack. Traditional password-based remote user authentication is not much secure as biometric-based remote user authentication which is proved by AKA protocol (Chaturved et al., 2017). Emanuel von Zezschwitz et al. compared Android's performance quality by both pattern and personal identification numbers (PINs) on smartphones in a field study, where they could not escape the difficulty of remembering (Von Zezschwitz et al., 2013).Through analyzing the above literature, it is found that no one can overcome the drawbacks of memorizing passwords and PINs which increases the vulnerability of authentication method from spyware and dictionary attacks that significantly reduce system security.

2.1.2 Two-Factor Authentication

Two-factor authentication based on keys, smart cards, USB drives, token devices adds an additional security layer to the authentication process by making it harder for hackers to access a user's devices or online accounts. Many researchers proposed robust solution about two-factor token-based authentication such as Hassina Nacer et al. developed a decentralized and completely distributed model for composite b services using two-way authentication, three party key establishments, and a distributed certificate authority, where they could not measures the security issues of paths (Nacer et al., 2017). Mian Ahmad Jan et al. proposed a lightweight mutual authentication scheme for an IoT environment's real-world physical objects, in which they increased the complexity using four way handshake using a simple four way handshake mechanism to verify the identities of the participating objects (Jan et al., 2019). After revising the above literature, simply it is found that, even two-factor authentication could not provide overall client, server and channel security.

2.2.3 Biometric Template Authentication

To design a defensive and reliable, two-factor user and/or machine identification and validation biometric technologies are turning out the cornerstone of an extensive array of highly secured solution. In past researches of biometric template authentication, has been con-ducted with several solution like fingerprints, palm scanning, facial recognition, iris scans, retina scans, lip recognition and voice verification (Da et al. 2019, Bhatnagar et al. 2010, Bedi et al. 2012, Sajjad et al. 2019). Srijan Das et al. developed a Lip biometric template security framework using spatial Steganography for improving the local features of the lip images (Da et al., 2019). A new scheme has been introduced to improve the security of biometric models, in which the methods of dissemination and watermark are combined to guarantee the authenticity, confidentiality and integrity of the models (Bhatnagar et al., 2010). Punam Bedi et al. proposed a multimodal biometric image watermarking scheme using Particle Swarm Optimization (PSO) with fingerprint image and demographic data on the face of a user (Bedi et al., 2012). A new hybrid technique is proposed by Muhammad Sajjad et al. that provides user authentication in the system, and also tracks whether the user passed the biometric system as normal or false, and also demonstrates that the fingerprint counterfeiting is too easy to implement (Sajjad et al., 2019). Although some of the researchers are added token based Kerberos protocol for additional security, it could not be clarify that channels are secure.

2.2.4 Token-Based Mutual Kerberos Protocol

Although three types of schemes are generally used for authentication, it needs to add token-based Kerberos protocol, for advance security, reliability and trustworthiness, which is proven by BAN’s logic (Abdelmajid et al. 2010). Rafael Mar n Lopez at al. developed an architecture that integrates a Kerberos pre-authentication mechanism to link the end-user authentication and authorization performed with the delivery of Kerberos tickets in the service provider’s domain through an AAA infrastructure (Mar n-Lopez et al., 2011).

2.2.5 Image Steganography Technique

Steganography is used to conceal messages into more complex information forms including images, audio, or videos. Several researchers conducted that, through the network, Steganography techniques added additional protection to data transmission (Kadhim et al. 2019, Minz et al. 2019, Sharma et al. 2019). Nevertheless, researchers have suggested a large number of solutions using Steganography techniques to mitigate the lack of attacks when transmitting data like as Yoon-Su Jeong et al. proposed a mutual authentication method in a situation where de-vice A communicates with device B, which is an in heterogeneous environment, using biometric information from each device user (Jeong et al., 2006). Using hash operations and XOR operations, a lightweight biometric based remote user authentication scheme for IoT service was developed by Parwinder Kaur Dhillon et al. which makes security and privacy critical to IoT (Dhillon et al., 2017). A study has identified two primary applications combining biometric and Steganography, which are access controls for the transmission of sensitive biometric data, and also proposed e-voting and e-shopping models using both platforms (McAteer et al., 2019).

After reviewing the above literature, it is found that the conventional text-based and token-based approaches are not significantly providing positive user identification because they rely on surrogate representations of user's identity. Now-a-days, the most widely used biometric techniques are fingerprint and iris scans (Ali et al. 2019, Lee et al. 2002, Wangkeeree et al. 2019, Korukonda et al. 2019, Kannavara et al. 2009). Though iris recognition is highly accurate, the cost of the image scanner may be unreasonable in some cases, which is comparatively more expensive than fingerprints. On the other hand, because of the properties of universality, uniqueness, permanence, reliability, acceptability and circumvention, fingerprint recognition is a safe, commonly used technique. Therefore, our contribution is, enhancement of Kerberos protocol that is proved by BAN logic using biometric templates and Image Steganography. In this paper, the conventional username and password system is completely avoided and the new solution for taking a pair of random fingerprints from the user is implemented which allows the real user to use it effortlessly.

CHAPTER 3

METHODOLOGY

3.1 PROPOSED MODEL

The proposed system uses biometric authentication, Cryptography and Steganography to ensure data security and presence hiding. The mechanism also uses a portable device with biometric Fingerprints to add extra factor. Let's assume that there are three different roles in this proposed scheme which are the User, Authentication server and Application server. Application server is responsible for providing service to authorized user. On the other hand, the authentication server is responsible for verifying the authenticity of the user. At the time of login, user must use a registered Portable device to prove identity. The proposed scheme is divided into the request phase, authentication phase and response phase. The notations used in this scheme are explained in detail in the Notation section. In this process while the user request to the server for login, user must use own Portable device and 10 Fingerprints which is registered during the registration process. The Proposed system is based on the shared-keys between three principals and a Database with an Authentication server and an Application Server that makes use of Timestamp as nonce.

The model is given below with the help of three principals as U, AU and AP. K_{UAU}, K_{UAP}, K_{AUAP} are the shared keys where the K_{U}, K_{AU} and K_{AP} are the public keys and DB as the Authentication server Database. In this phase U generates the timestamp T_{U}, AU generates the timestamp T_{AU}, AP generates the timestamp T_{AP} and U generates the Lifetime L respectively. The fifth, sixth and seventh messages are used only if the mutual authentication is required. Here, OTP as One time image (fingerprint) which is generated by Stego Validation and POTP as previously used OTP where it stored in Stego Validation.

The proposed model as a figure is given below-

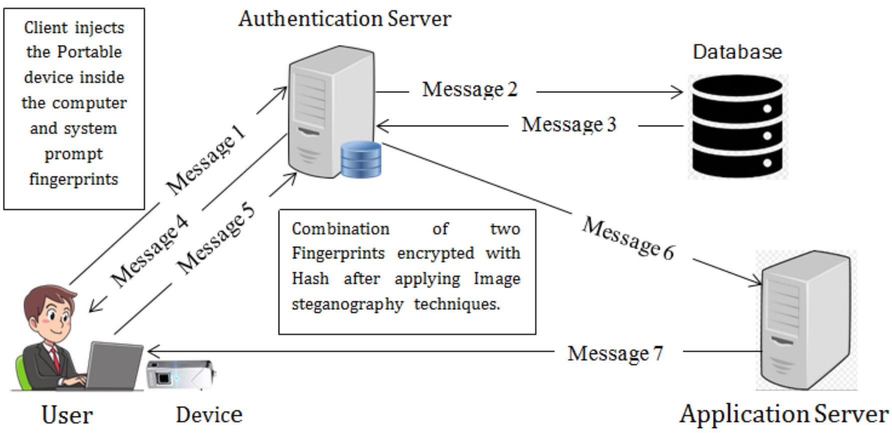
Client injects the Portable device inside the computer and system prompt fingerprints
Authentication Server
Database
Message 1
Message 2
Message 3
Message 4
Message 5
Message 6
Message 7
Combination of two Fingerprints encrypted with Hash after applying Image steganography techniques.
User
Device
Application Server

Figure 1. Proposed Model

The Messages are given below sequentially-

$$\text{Message 1. } U \longrightarrow AU : \{T_{U}, L, D_{ID}\}_{K_{CAU}}$$

$$\text{Message 2. } AU \longrightarrow DB : \{T_{AU}, D_{ID}, \{T_{AU}, DB \xleftrightarrow{K_{AUDB}} AU\}_{K_{DB}}\}_{K_{DB}}$$

$$\text{Message 3. } DB \longrightarrow AU : \{T_{AU}, D_{ID}, \{T_{AU}, U, OTP, DB \xleftrightarrow{K_{AUDB}} AU\}_{K_{AU}}\}_{K_{AUDB}}$$

$$\text{Message 4. } AU \longrightarrow U : \{T_{U}, U, \{T_{AU}, POTP, (Fg_{1}, Fg_{2}), AU \xleftrightarrow{K_{UAU}} U\}_{K_{U}}\}_{K_{UAU}}$$

$$\text{Message 5. } U \longrightarrow AU : \{T_{U}, K_{UAP}, \{T_{U}, (Fg_{1}, Fg_{2}), AU \xleftrightarrow{K_{UAU}} U\}_{K_{AU}}\}_{K_{UAU}}$$

$$\text{Message 6. } AU \longrightarrow AP : \{T_{AU}, U, D_{ID}, \{T_{AU}, AU \xleftrightarrow{K_{AUAP}} AP\}_{K_{AP}}\}_{K_{AUAP}}$$

$$\text{Message 7. } AP \longrightarrow U : \{T_{AP}, U, D_{ID}, \{T_{AU}, AP \xleftrightarrow{K_{UAP}} U\}_{K_{U}}\}_{K_{UAP}}$$

3.1.1 Notations

Several types of objects have been defined in this model as principals, encryption keys, notation and statements where the symbols U, AU, AP and DB denoted as User, Authentication Server, Application Server and Server Database sequentially. D_{ID} as Device ID and U_{NM} as Username. K_{UAU}, K_{UAP}, K_{AUAP} denotes as Shared key between U and AU, U and AP and AU and AP respectively. K_{U}, K_{AU}, K_{AP} denotes specific public keys of the principals U, AU and AP and K_{U}^{-}, K_{AU}^{-} and K_{AP}^{-} denotes the corresponding secret keys where T_{U}, T_{AU} and T_{AP} denotes specific nonce timestamp. Here, OTP denotes One Time Image generated by Stego validation and POTP as Previously One Time Image generated by Stego validation. FgX denotes the combination of two fingerprints where Fg1, Fg2… Fg10 denotes every single Fingerprint sequentially.

3.1.2 Message Description

1. User ⟶ Authentication Server:

   Client enters the Portable device inside the computer where the system prompts fingerprints.

2. Authentication Server ⟶ Database:

   In the first Authentication Phase, Server matches the first factor Device ID with the help of database; pick the Username that are stored in the Registration process.

3. Database ⟶ Authentication Server:

If device ID matches then pick the Username that are stored in the Registration process.

4. Authentication Server ⟶ Client :

Ask for two random fingerprints from ten.

5. User U ⟶Authentication Server :

User will give two fingerprints and System encrypt the combination of Fingerprints using Hash algorithm then select an Image based on timestamp as Stego Object and embedded these Hashes inside the Image Steganography.

6. Authentication Server ⟶Application Server:

Application Server receives access request to U.

7. Application Server ⟶User:

Application Server creates session.

3.3 MODEL DESCRIPTION

In this research, figure 1 represents the message sequences. Firstly, U enters a portable Device. After that, AU receives a request message with Timestamp, Lifetime and Device ID. That is encrypted separately with the help of shared key of U and AU which can read by AU which is decrypted with the secret-shared key. AU first decrypted the message and send it to DB for matching the D_{ID}. If this session has been created recently enough, DB uses the enclosed key for decrypting the authenticate message to match it. Then, it will replay back the User Name U_{NM}, with the combination of two random Fingerprints which is previously stored in the Database. The random picking process is implemented by Auto generated algorithm RAND (). Once the principal AU is satisfied, it will send a message to U with the previous timestamp, Username and the POTP which is encrypted by the help of User’s private key. The full message is encrypted with the help of shared keys between U and AU. U receives this message and decrypted it. After that it sends back the message with requested two Finger-prints, that is encrypted with Hash Algorithm and pass it using Image Steganography techniques. Next, AU decrypted it and if AU satisfies then it will send a message to AP with the U_{NM}, D_{ID} and request to create a session for U. The full message encrypted using the shared key of AU and AP. Then AP receives it. After receiving this AP will check it. If the session is already created then it will decrypted it. Once, this principal AP is satisfied, it will proceed to generate a session for User U, and give access to U as a replay. Therefore the contribution is, principal AU believes principal U, and principal AP believes principal AU where principal AP will must believe on principal U. Now, The Model will be proved with the help of greatest BAN logic and the concept of Kerberos protocol.

3.4 REGISTRATION PROCESS

At first, User needs to enter the Portable device into the Server for assigning Device ID. For every single Device’s, Server Database will provide a key as a private key

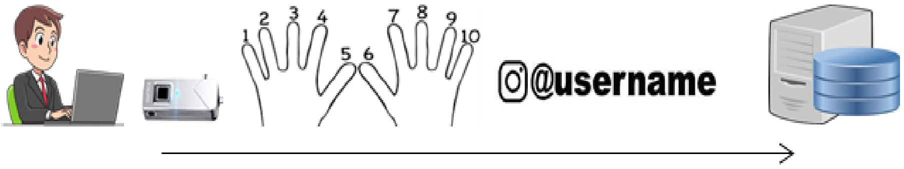

Figure 2. Registration process

that will stored in the database. After that user have to provide every (10) finger’s print sequentially according to the direction of that device. In this case, User needs to provide Username for additional security.

3.5 LOGIN PROCESS

In login process, at first user enters the portable device then with the help of database server, authentication server tries to match with the Device ID. If the Device ID matched, authentication server wants two fingerprints randomly (One from left hand and one from right hand). According to the query of Authentication Server, user will provide two fingerprints. Then, the combination of two fingerprints will go to the channel with image Steganography. After that, by the help of hash algorithm these texts will be encrypted. However, the login process will complete in 3 phases describe below:

3.5.1 Request Phase

First phase is the Request phase. In this phase, login re-quest will send through the channel from client side to server side. In Request phase-

1. User U Request for login to the system by entering the portable device to the system. It reads D_{ID}.
2. The Server side matches the D_{ID} with the help of Server Database, If matches then AU pick the Username U_{NM} from the Database and pick two finger-prints (One is from Left and one is from Right) from the corresponding D_{ID} and send to the Client side.
3. User U provides these two specific fingerprints with the given instruction.
4. Client side Hash the following combination of two fingerprints by using hashing algorithm. Client side encrypts Fingerprints Fgx using asymmetric algorithm.

5. Embed the hash into the selected image using suitable and effective Steganography technique.

3.5.2 Authentication Phase

Second phase is the Authentication phase. In that phase, server authenticates the client with legal identity. In Authentication phase-

1. AU receives the image files and En (Fgx).
2. First retrieve the En (Fgx) from Steganography.
3. Matches that received En (Fgx) with the previous En (Fgx).
4. Perform HASH operation on H.
5. Fg1 && Fg2 = = expected (Fgx1 && Fgx2).
6. If it is TRUE. Redirect to AS.

*DBh → Hash stored in Database.

*DBFgx →Fgx stored in database for previous authentication.

3.5.3 Response Phase

The last phase is the Response phase. In this phase, the server will give response to the client by creating a session. In Response phase-

1. AP receives access request to U.
2. AP creates session and provides access to U.

After all these phases, login process will be completed and authentication process also be formalized.

3.6 LOGICAL POSTULATES OF BAN LOGIC

The main logical postulates of BAN logic are given below

Rule 1. Message-meaning rules for shared keys-

$$\frac{\text{P believes P} \overset{K}{\longleftrightarrow} \text{Q, P sees } \{X\}_K}{\text{P believes Q said X}} \tag{1}$$

P believes Q said X, if P believes that the key K is a shared key between P and Q and P sees X is encrypted with the key K.

For Public keys:

$$\frac{\text{P believes Q, P sees } \{X\}_K\text{-1}}{\text{P believes Q said X}} \tag{2}$$

P believes Q said X, if P believes Q and P sees X that is encrypted by private key $K^{-1.}$

For Public keys:

$$\frac{\text{P believes Q} \overset{Y}{\rightleftharpoons} \text{P, P sees } \langle X\rangle_Y}{\text{P believes Q said X}} \tag{3}$$

P believes Q said X, if P believes that a secret statement Y is present between Q and P and P sees X that is encrypted by a secret statement.
Rule 2. Nonce-verification rules –

$$\frac{\text{P believes fresh(X), P believes Q said X}}{\text{P believes Q believes X}} \tag{4}$$

P believes Q controls X, if P believes on currently created X and Q has said X.

Rule 3. Jurisdiction rules-

$$\frac{\text{P believes Q controls X , P believes Q believes X}}{\text{P believes X}} \tag{5}$$

P believes X, if P believes that Q has controlled and believed on X.

3.7 ANALYSIS

To analyze this protocol, the first assumptions are given here:

AU believes $AU \overset{K_{UAUB}}{\longleftrightarrow} U$	AU believes fresh (T_U)
DB believes $DB \overset{K_{AUDBP}}{\longleftrightarrow} U$	DB believes fresh (T_{AU})
AP believes $AP \overset{K_{AUAP}}{\longleftrightarrow} AU$	AP believes fresh (T_{AU})
AU believes U controls $(AU \overset{K}{\longleftrightarrow} U)$	U believes fresh (T_{AP})
DB believes AU controls $(DB \overset{K}{\longleftrightarrow} AU)$	
AP believes AU controls $(AP \overset{K}{\longleftrightarrow} AU)$	

The first left three, is about Shared keys between the three principals and Database. The right four assumptions show that the directors and the Database server believe that the timestamps generated elsewhere are fresh; this indicates that the model relies heavily on synchronized clocks. The next group of three which indicates the trust that the principles and DB has in the server to generate a good encryption key. In Message 1, U sends its device id where AU contact with the DB for conforming the D_{ID} and then AU pick the U_{NM} which generated the OTP for further identification of U, in message 2 and 3.And in Message 4, AU requested for the combination of two random Fingerprints from U. However, it is possible to skip Message 1, Message 2, message 3 and Message 4 respectively. If it is possible to build the belief between U and AU and between AU and AP then it can be claimed that AP have believe to U. After analyzing the idealized model by applying the rules it can be assume that the analysis is straightforward. In the interests of brevity, give many of the formal details necessary for this machine assisted proof only for Message 5, Message 6 and Message 7. And it will omit similar details later on. The main steps of the proof are as follows:

AU receives Message 5. The annotation rules yield that-

$$\text{AU sees}\{T_U,\ L,\ D_{ID}\ \}_{K_{CAU}}$$

holds afterward. Since it has the hypothesis-

$$\text{AU believes AU} \overset{K_{UAUB}}{\longleftrightarrow} U$$

Applying Rule (1) and yields the following:-

$$\text{A believes U said}\{\ T_U,\ \ (AU \overset{K_{UAUB}}{\longleftrightarrow} U),\{T_U, AU \ \overset{K_{UAUB}}{\longleftrightarrow} U\ \}_{K_{AU}}\}_{K_{UAU}}$$

One of the rules to break Conjunctions (Omitted here) then produces –

$$\text{A believes U said } (T_U, (AU \overset{K_{UAUB}}{\longleftrightarrow} U)$$

Moreover, it has the following hypothesis:

$$\text{AU believes fresh } (T_U)$$

Rule (4) applies and yields –

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

Again, breaking the conjunction, to obtain the following:

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

deriving the more concrete-

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

Finally, the Rule (5) applies and yields the following:

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

Therefore it concludes the analysis of Message 5.

U passes the expected Finger-prints POTP on to AU, together with a message containing a timestamp. Initially, AU can decrypt only this message:

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

This result is logically obtained in the same way that it was acquired for Message 5 through the postulates of message, nonce-verification and jurisdiction. Knowledge of new key allows AU to decrypt this message.

Knowledge of new key allows AU to decrypt this message. Through the message-meaning and the nonce-verification postulates, deduct the following:

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

According to previous, DB also believes AU and gives replay with confirmation.

To next, AU sends message to AP for confirming the identity of U and give access U with generating session for U.

Applying these three rules according to previous it also prove that

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

Now, it can be deduced that:

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

Here with that (AP $\overset{K_{AUAP}}{\longleftrightarrow}$ AU), AU sends message to AP that can be re-placed by U. (Message that will actually send it about U's D_{ID}, U_{NM}). Now it deduced that:

AP believes AU believes U

And, it has the following hypothesis –

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

Here with that (AP $\overset{K}{\longleftrightarrow}$ AU), AU sends message to AP that can be replaced by U. (Message that will actually send it about U's D_{ID}, U_{NM}). Now it deduce that-

AP believes AU controls U

Lastly, the jurisdiction rule applies and yields the following:

AP believes U

And for that AP creates a session for User U. However, it is possible to build the belief between U, AU and AU, AP then it can be claimed that AP has believe on U.

3.8 PROPOSED IMPLEMENTATION TECHNIQUES

For our solution, we propose SHA-512 algorithm for hashing operation of user's fingerprint and LSB replacement through XOR substitution will be used for image steganography.

CHAPTER 4

DISCUSSION

In this study, biometric based authentication process has been presented which is formalized by applying the rules of BAN logic analysis with certain assumptions. The goal of BAN logic's is to explicitly identify the authentication convictions that are used in the process of user and/or machine identification. This logic ensures the security, reliability and consistent belief of our model among the principals while capturing all attributes of messages. For instance, it can be expressed that the principals have different features of trust in other principals.

4.1 ENHANCE OF KERBEROS PROTOCOL

In the analysis section, the statement AU believes U and U believes AU which has been evaluated and proved in the above analysis section where AU and U refers respectively the principals Authentication server and the User. Further-more, AU believes AP and AP believes AU, which is also illustrated in the above analysis section and refers respectively the principals Authentication Server and Application Server. According to the above believes, it can be claimed that principal AP believes on principal AU and the principal AU believes on principal U. Therefore, it can be said that principal AP believes U which means Application Server has believed on User. After analyzing this, it can be argued that the sys-tem match with the Kerberos protocol where the protocol is demonstrated by the BAN logic which ensures that the beliefs on both servers and user are authenticated (M. Burrows et al., 1990). From there, it can be said that the objectives of authentication has been established and proved the enhancement of Kerberos protocol.

4.2 FINGERPRINTS INSTEAD OF PASSWORD

Since mid-19th century, password-based authentication processes were used to protect the system. Using false request such as IP spoofing, DNS spoofing, HTTPS spoofing, SSL hijacking, Email hijacking was easy to crack the password from the server by conducting eavesdropping, password guessing and brute-force attack (Yan et al., 2004). Surrogate representations was the another way to break the security system. For this reason, the system was not much secure to ensure the security. To overcome this obstacle here used the biometric fingerprint-based authentication system which protect against the surrogate representations by eliminating the need of memorizing as well as sharing username and password. For ensuring the security system, in the proposed model need to inject a device which provide a unique device id. By the help of unique device id the system authenticates the server and user and also checks the validation of the request. The traditional fingerprint based authentication system usually used two or three finger to authenticate the user. For this reason, this authentication mechanism has raised a lots of security concern due to easiness of fingerprint spoofing. To address the problem and to reduce the security flaws that is caused by the above mentioned issue, this research used a combination of pair of fingerprint. During the registration process, users have to provide 10 fingerprints from hands. Although all the fingerprints used during the registration process are received by the system. However, at the time of authenticating, server will ask random combination of two fingerprints and the prompt users have to provide that sequentially. From this, it can easily be inferred that the advancement of complexity has become a difficult level to spoof the fingerprints for a hacker or an unwanted individual.

4.3 IMAGE STEGANOGRAPHY

After applying the Kerberos Protocol, BAN logic and Biometric Authentication, it was unable to ensure the data security because the path was not enough secures or data properly encrypted. Therefore, most of the attacks such as- Man in the Middle (MITM) attack, spyware, Trojan-horse, phishing attack, hash-injection are mainly disrupt the security system when transmission of data via communication channels. Though it is quite impossible to protect a server from MITM attack for the cause of uses proxy server, it can be possible to secure data by effective data hiding techniques. To ensure the data security, this model uses image Steganography technique to secure data by data hiding in the Stego image during transmission (Alturki et al. 2001, Mare et al. 2011). The SHA-512 hash algorithm will be used in our proposed authentication system to secure the combination of fingerprints as this hash functions based algorithm performs the encryption and decryption task in a minimal time compare with other known algorithm such as DES, AES, RSA, MD2, MD5, SHA-256 that is proved by Del et al (Del et al, 2015). At the same time, as an image steganography method, the LSB replacement through XOR substitution will be used to embed the image stego since LSB replacement technique is light-weighted; therefore its processing time is less than other known steganography techniques (Touhid et al., 2019). Since the image Steganography technique hides information within an image which increases the complexity of recovering the actual data that becoming more difficult to break for the hackers.

4.4 SUMMARY

After analyzing the above study, it can be said that all the final explanation of the models has been exposed. This research has demonstrated the use of logical and synthetic logic of BAN with implementation details for verification and identification at a high level of abstraction. This authentication model can effectively achieve the security objective of mutual authentication of readers and statements and the use of biometric fingerprint and image Steganography technique makes the model effective, usable, secure from various attacks and intruders.

CHAPTER 5

CONCLUSION

Biometric based multi-factor authentication protocol has proposed in this pa-per to enhance the existing Kerberos authentication protocol where the Image Steganography technique has used to ensure the data security over the public channel. The proposed solution has been proved its rules through the renowned proofing tool of authentication protocol, BAN logic that ensures the belief be-tween both the server and the user. The advantage of this system is to authenticate the user without remembering the username and password which has made this system more unique with comparing other researches. Furthermore, the complexity of changing or remembering passwords is completely avoided in this proposed system, which ensures the e effectiveness of this solution. The pro-posed scheme has also the advantage of better combining secrecy with biometric data that can reduce the impact of the stolen identity attacks. Theoretically the model has been proved using BAN logic in this study; however, known attacks against this solution will be tested to verify the effectiveness of the solution in future.

CHAPTER 6

REFERENCES

Abdelmajid, N. T., Hossain, M. A., Shepherd, S., & Mahmoud, K. (2010, June). Improved Kerberos security protocol evaluation using modified BAN logic. *In 2010 10th IEEE International Conference on Computer and Information Technology (pp. 1610-1615).* IEEE.

Ali, S. S., Ganapathi, I. I., Mahyo, S., & Prakash, S. (2019). Polynomial Vault: A secureand robust fingerprint based authentication. *IEEE Transactions on Emerging Topics in Computing.*

Alsaadi, I. M. (2015). Physiological biometric authentication systems, advantages, disadvantages and future development: a review. *International Journal of Scientific & Technology Research, 4(12), 285-289.*

Alturki, F., & Mersereau, R. (2001, April). A novel approach for increasing security and data embedding capacity in images for data hiding applications. *In Proceedings International Conference on Information Technology: Coding and Computing (pp. 228-233). IEEE.*

Ashibani, Y., Kauling, D., & Mahmoud, Q. H. (2019). Design and Implementation of a Contexual-based continuous authentication framework for smart homes.*Applied System Innovation, 2(1), 4.*

Bedi, P., Bansal, R., & Sehgal, P. (2012). Multimodal biometric authentication using PSO based watermarking. *Procedia Technology, 4, 612-618.*

Bhatnagar, G., Wu, Q. J., & Raman, B. (2010). Biometric template security based on watermarking. *Procedia Computer Science, 2, 227-235.*

Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. *In People and computers XIV—usability or else! (pp.405-424). Springer, London.*

Burrows, M., Abadi, M., & Needham, R. M. (1989). A logic of authentication.Proceedings of the Royal Society of London. *A. Mathematical and Physical Sciences, 426(1871), 233-271.*

Chattaraj, D., Sarma, M., & Das, A. K. (2018). A new two-server authentication and key agreement protocol for accessing secure cloud services. *Computer Networks,131, 144-164.*

Chaturvedi, A., Mishra, D., Jangirala, S., & Mukhopadhyay, S. (2017). A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme. *Journal of Information Security & Applications, 32,15-26.*

Chen, B. L., Kuo, W. C., & Wuu, L. C. (2014). Robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems, 27(2), 377-389.*

Das, S., Muhammad, K., Bakshi, S., Mukherjee, I., Sa, P. K., Sangaiah, A. K., & Bruno, A (2019). Lip biometric template security framework using spatial steganography. *Patter Recognition Letters, 126, 102-110.*

Duluta, A., Mocanu, S., Pietraru, R., Merezeanu, D., & Saru, D. (2017, May). Secure communication method based on encryption and steganography. *In 2017 21st International Conference on Control Systems and Computer Science (CSCS) (pp.453-458). IEEE.*

Fan, K., Li, H., & Wang, Y. (2009, August). Security analysis of the kerberos protocol using BAN logic. *In 2009 Fifth International Conference on Information Assurance and Security (Vol. 2, pp. 467-470). IEEE.*

GeekWire.com Digital authentication: The past, present and uncertain future of the keys to online identity *https://www.geekwire.com/2018/digital-authentication-human-beings-history-trust/ (Last access 29 November, 2019)*

Hessler, C. J. (2015*). U.S. Patent No. 8,935,769*. Washington, DC: U.S. Patent and Trademark Office.

Hussain, M., Wahab, A. W. A., Batool, I., & Arif, M. (2015). Secure password transmission for web applications over internet using cryptography and image steganography. *International Journal of Security and Its Applications, 9(2), 179-188.*

Jan, M. A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems, 92, 1028-1039.*

Jeong, Y. S., Lee, B. K., & Lee, S. H. (2006, November). An efficient device authentication protocol using bio-informatic. *In International Conference on Computational and Information Science (pp. 567-575). Springer, Berlin, Heidelberg.*

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing, 335, 299-326.*

Kannavara, R., & Bourbakis, N. (2009, July). Iris biometric authentication based on local global graphs: An FPGA implementation. *In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1-7). IEEE*

Kasslin, K., Tikkanen, A., & Virtanen, T. (2003). Kerberos V Security: Replay Attacks. *Enhancing Trust, Citeseer, 191*.

Kaur, H., & Khanna, P. (2020). Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. *FutureGeneration Computer Systems,102, 30-41.*

Kesanupalli, R. (2010). *U.S. Patent Application No. 12/561,186.*

Koong, C. S., Yang, T. I., & Tseng, C. C. (2014). A user authentication scheme using physiological and behavioral biometrics for multitouch devices. *The Scientific World Journal, 2014.*

Korukonda, V. R., & Reddy, E. S. (2019). IRIS BASED TEXTURE ANLAYSIS FOR VERIFCATION AND DETECTION: REVISIT.

Kumar, A., & Om, H. (2018). An improved and secure multi server authentication scheme based on biometrics and smartcard. *Digital Communications and Networks, 4(1), 27-38*

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*.

Lee, J. K., Ryu, S. R., & Yoo, K. Y. (2002). Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters, 38(12), 554-555*.

Leu, J. S., & Hsieh, W. B. (2013). Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. *IET information security, 8(2), 104-113.*

Lowe, G. (1997, June). A hierarchy of authentication specifications. *In Proceedings 10th Computer Security Foundations Workshop (pp. 31-43). IEEE.*

Mare, S. F., Vladutiu, M., & Prodan, L. (2011, October). Secret data communication system using Steganography, AES and RSA. *In 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME) (pp. 339-344). IEEE.*

Marín-López, R., Pereñíguez, F., López, G., & Pérez-Méndez, A. (2011). Providing EAP-based Kerberos pre-authentication and advanced authorization for network federations. *Computer Standards & Interfaces, 33(5), 494-504.*

McAteer, I., Ibrahim, A., Zheng, G., Yang, W., & Valli, C. (2019). Integration of biometrics and steganography: Acomprehensivereview.Technologies,7*(2), 34.*

Medium.com Kerberos and Windows Security: History *https://medium.com/@robert.broeckelmann/kerberos-and-windows-security-history-252ccb510137* (Last access 29November, 2019)

Mukhamedov, A. (2005, September). Full agreement in BAN kerberos. *In Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005. (pp. 218-223).* IEEE.

Nacer, H., Djebari, N., Slimani, H., & Aissani, D. (2017). A distributed authentication model for composite Web services. *Computers & Security, 70, 144-178.*

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y.(2018).Multi-factor authentication: A survey. *Cryptography, 2(1), 1.*

O’REILLY,Safari."*https://www.oreilly.com/library/view/comptia-securitytmreview /97811 18113523/xhtml/sec34.html*." Last access 14 October, 2019.

Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A. K., Castiglione, A., & Baik, S. W. (2019). CNN-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters, 126, 123-131.*

Shanmugapriya, D., & Padmavathi, G. (2009). A survey of biometric keystroke dynamics: approaches, security and challenges. *arXiv preprint arXiv:0910.0817.*

Truong, T. T., Tran, M. T., & Duong, A. D. (2012, September). Robust biometrics-based remote user authentication scheme using smart cards. *In 2012 15th International Conference on Network-Based Information Systems (pp. 384-391).* IEEE.

Tsai, J. L., Lo, N. W., & Wu, T. C. (2012). Novel anonymous authentication scheme using smart cards. *IEEE Transactions on Industrial Informatics, 9(4), 2004-2013.*

Rai, P., Gurung, S., & Ghose, M. K. (2015). Analysis of image steganography techniques: a survey. *International Journal of Computer Applications, 114(1).*

Shi, S., Cui, J., Zhang, X. L., Liu, Y., Gao, J. L., & Wang, Y. J. (2019). Fingerprint Recognition Strategies Based on a Fuzzy Commitment for Cloud-Assisted IoT: A Minutiae-Based Sector Coding Approach. *IEEE Access, 7, 44803-44812.*

Van Dijk, M., Bowers, K. D., Curry, S., Doyle, S. P., Triandopoulos, N., & Zolfonoon, R. (2014). *U.S. Patent No. 8,752,146.* Washington, DC: U.S. Patent and Trademark Office.

Von Zezschwitz, E., Dunphy, P., & De Luca, A. (2013, August). Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices.*In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (pp. 261-270). ACM.*

Wangkeeree, N., & Boonkrong, S. (2019). Finding a suitable threshold value for an iris-based authentication system. *International Journal of Electrical & Computer Engineering (2088-8708), 9.*

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & privacy, 2(5), 25-31.*

Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of computer and system sciences, 74(7), 1160- 1172.*

T. Bhuiyan, A. H. Sarower, M. R. Karim and M. M. Hassan, “An Image Steganography Algorithm using LSB Replacement through XOR Substitution ," 2019 International Conference on Information and Communications Technology (ICOIACT 2019), 24-25 July, Yogyakarta, Indonesia.

Del Pozo, Ivan, and Mauricio Iturralde. "CI: A new encryption mechanism for instant messaging in mobile devices." *Procedia Computer Science* 63 (2015): 533-538.

UKESSAYS https://www.ukessays.com/essays/english-language/background-of-steganography.php (last Access 29 november,2019)