International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, Vol. 2(4), 2025
DOI: 10.61359/11.2206-2516

Secure File Access for Consumer Storage Devices Using Biometric Security System

S. Shama Parveen*

Email Correspondence*: shamaparveen@sethu.ac.in

[1]*Information Technology, Sethu Institute of Technology, Virudhunagar, Tamil Nadu, India

Abstract:

In order to resist unauthorized access, consumer storage devices are typically protected using a low entropy password. However, storage devices are not fully protected against an adversary because the adversary can utilize an off-line dictionary attack to find the correct password and/or run an existing algorithm for resetting the existing password. It can be used as a replacement for the username and password as a convenient log-in, or as a simple alternative to password re- sets. It can also be deployed for enhancing the boarding and KYC (Know Your Customer) methods. It has a tremendous advantage in improving a brand's user experience. In today's hi-tech world, solving the password problem has been the goal for many financial service providers and various online enterprises. Unfortunately, their customers either use weak passwords or the same passwords time and again. Furthermore, many of us should be changing the passwords regularly to avoid them being stolen or hacked by fraudsters. Biometric identification of the human iris., As demands on secure identification are constantly rising and as the human iris provides with a pattern that is excellent for identification, the use of inexpensive equipment could help iris recognition become a new standard in security systems. In addition, a password protected device may also be stolen or misplaced, allowing an adversary to easily retrieve all the stored confidential information from a removable storage device. In order to protect the consumer's confidential information that has been stored, this paper proposes a mutual authentication and key negotiation protocol that can be used to protect the confidential information in the device. The functionality of the protocol enables the storage device to be secure against relevant security attacks. A formal security analysis using Burrows-Abadi-Needham (BAN) logic is presented to verify the presented algorithm. In addition, a performance analysis of the proposed protocol reveals significantly reduced communication overhead compared to the relevant literature.

Keywords: Security Analysis, Communication Overhead, Unauthorized Access, Security Attacks, Authentication Protocol, Mutual Authentication, Computational Cost, Hash Function, Secret Key, Public Key, Denial of Service, Biometric Data, Session Key, Biometric Information, Key Agreement, Encrypted File, Impersonation Attack.

1. Introduction

Consumer storage is commonly used to store and retrieve digital information. Consumers often store confidential information, files, or digital media purchases in the device. These devices are low cost and easily portable, so the consumer often carries the device when travelling. As a result, the device may be lost or stolen by an adversary. If confidential information is not protected, an adversary can easily retrieve the stored information from the device memory. However, the adversary faces a problem retrieving the

*Information Technology, Sethu Institute of Technology, Virudhunagar, Tamil Nadu, India.

Article Timeline: Received: Apr 16, 2025; Revised: Apr 28, 2025; Published: Apr 30, 2025

information from the store if the device is password protected. It is worth noting that a user's password (typically low entropy) cannot provide a strong security system under a cryptographic dictionary attack. Indeed, many techniques are currently available to guess the password to access the device. Mutual authentication and key agreement protocols are a popular paradigm in client-server environments to prevent unauthorized access.

2. Literature Review

A. Background

In 1981, Lamport first introduced the secure communication client-server architecture and then numerous protocols have been proposed for several applications, including wireless sensor networks, medical systems and file security for USB based Mass Storage Devices (USB MSD). In order to provide secure access, authentication protocols play an important role. Significant literature is now available to provide solutions to protect confidential files stored in a USB MSD.

B. Related Work

Yang et al. first proposed a secure authentication protocol using the Schnorr Signature to protect the information stored. However, Chen et al. argued that the protocol from Yang et al. was not secure against the forgery attack and the replay attack. Furthermore, Lee et al. argued that the protocol by Chen et al.

The protocol from Lee et al. required the user's password, biometric and smartcard information as authentication tokens. More recently, He et al. demonstrated that the protocol proposed by Lee et al. was not secure against the password guessing attack, Denial-of-Service (DoS) attack and the replay attack, so proposed an improved three-factor authentication scheme.

In order to resist the DoS attack, He et al. employed the concept of the fuzzy extractor. In 2015, Amin and Biswas proposed a three-factor authentication protocol for the same environment using a hash function to achieve a lower computation cost than existing protocols. This paper proposes a mutual authentication and key agreement protocol to provide only authorized access to confidential information stored on the device with the aid of a Registration Server (RS). A new user completes a registration procedure with RS allowing RS to deliver a link via e-mail from which the user can download and install registration software in their device which also incorporates the required secure access information relevant for only each user. In order to provide secure access to files, the user provides the necessary identity, password and biometric information.

The device checks the legitimacy of the user and then negotiates a session key with RS. It is to be noted that this session key is used to encrypt the files in the storage device. The rest of the paper is organized as follows: Chapter II presents an overview of the contribution and the novelty claims. Chapter III presents the hash function, fuzzy extractor and elliptic curve cryptography. The proposed protocol is provided in Chapter IV. The security analysis using BAN logic is discussed in Chapter V. Chapter VI provides the performance evaluation and comparison of the proposed protocol with related protocols. Section VII concludes the paper. Table-1 shows the nomenclature that is used throughout the paper.

3. PROPOSED METHODOLOGY

We sought to learn filter weight form given architecture using the well-known back propagation algorithm. Several biometric spoofing benchmarks have been recently proposed, allowing researchers to make steady progress in the conception of anti-spoofing systems. The device checks the legitimacy of the user and then

negotiates a session key with RS. It is to be noted that this session key is used to encrypt the files in the storage device. This section describes the proposed mutual authentication and key negotiation protocol, which includes seven phases:

1. Registration and software installation phase
2. Login phase
3. Mutual authentication and key negotiation phase
4. File management phase
5. File accessing phase
6. Password renewal phase
7. Biometric renewal phase

Advantages

- A mutual authentication and key negotiation protocol to provide security protection of the stored information on the storage device
- Security analysis to show that the proposed protocol is robust against known security attacks
- Furthermore, in the proposed scheme, the mutual authentication and session key have been verified using BAN logic

4. SYSTEM IMPLEMENTATION

Registration and Software Installation Phase

Initially, each new user Ui must complete a registration procedure with RS. In this phase, Ui provides their information securely or in person (off-line mode) to RS. Then, RS securely sends to Ui, via e-mail, a link to downloadable registration software which must be installed in the storage device.

Step 1: Ui first chooses IDi, PWi and scans the user's biometric template, BTi, such as a fingerprint. This work uses the biometric template to provide a high degree of security since biometric templates cannot easily be forged.

Iris Biometric Authentication

Iris is one such unique modality which, due to variations in iris texture, provides tremendous discriminability among different subjects and therefore is one of the most accurate approaches for recognition. Daugman proposed the first successful algorithm based on iris codes which are being used by several commercial iris technologies and applications. Thereafter, several algorithms are proposed to advance the state-of-the-art in iris recognition.

Iris Spoofing Methods

Iris spoofing is a mechanism by which one can obfuscate or impersonate the identity of an individual. Listed below are several easy (non-surgical) ways of spoofing an iris recognition system:

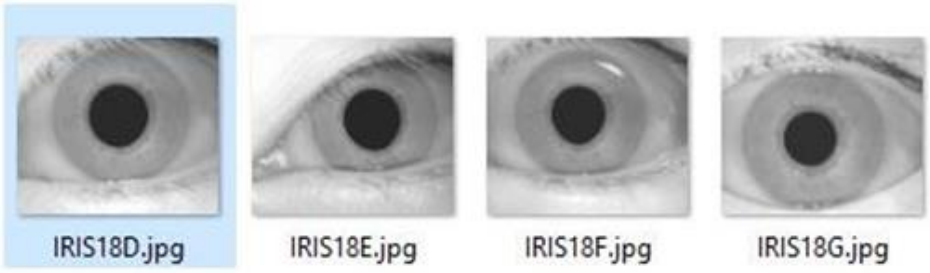
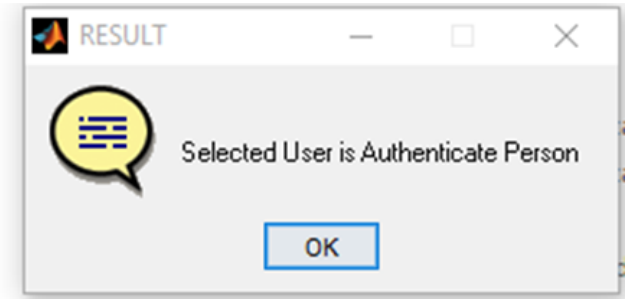


Figure-1 Iris Spoofing

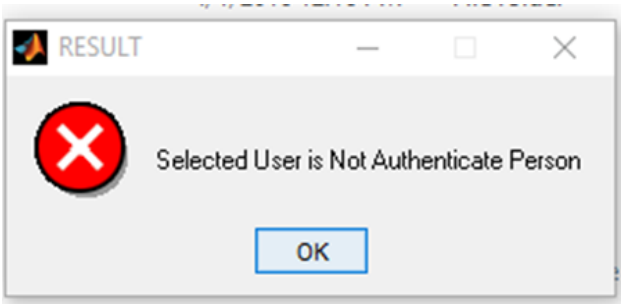
1. **Pupil dilation**: Pupil dilation can occur due to illumination variations, alcohol (substance) consumption, and medicine. As shown by Hollingsworth et al., large pupil dilation can cause iris patterns to be unrecognizable.

2. **Textured contact lenses**: Several researchers have shown that a colored textured contact lens can block the actual iris patterns and confuse an iris recognition system. Inter-class and intra-class similarities are significantly affected by colored textured contact lenses. Similarly, a lens with a painted iris obfuscates the actual eye patterns and creates a different appearance which is unseen by the iris recognition systems.

Print attack: Presenting a printed image of an iris to the scanner/system can help impersonating one's identity. With appropriate printer and paper combination, the quality of printed iris can be substantial enough to mislead an iris recognition system.



a)



b)

Figure-2 a) and b) Print Attack

Login Phase

This phase ensures that a non-registered user could not install the registration software without providing the correct information. The device runs the registration software now installed in the storage device, and the software requests Ui to input their identity, password, and biometric information.

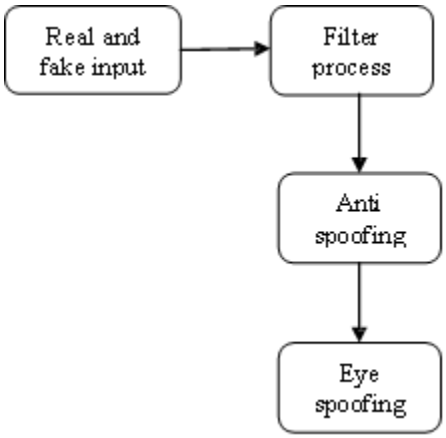


Figure-2 Login Phase

Mutual Authentication and Key Navigation Phase

This phase first achieves mutual authentication and then negotiates a session key between the registration software of Ui and RS over an insecure channel. In this process, Ui and RS perform the following steps:

Step 1: Ui runs the registration software installed in their device and then provides their IDi, PWi, and BTi to the registration software.

File Management Phase

After performing mutual authentication and key negotiation, the registration software can encrypt any chosen files (F1, F2, …, Fn), using the encryption key SKi for security protection. Note that the registration software in Ui can forget the encryption key after encrypting any files and send a confirmation message to RS. In this proposed protocol, RS maintains a table against each user Ui with the identity IDi.

File Accessing Phase

In this phase, Ui makes a request to RS to access the encrypted files stored in the consumer's storage device. In order to do it, Ui executes Steps 1-3 of the mutual authentication and key negotiation phase to verify the legitimacy of Ui and generate a new session key.

5. System Design Architecture

This network uses classic convolutional operations that can be viewed as linear and non-linear image processing operations. When stacked, these operations essentially extract higher level representations, named multiband images, whose pixel attributes are concatenated into high-dimensional feature vectors for later pattern recognition.

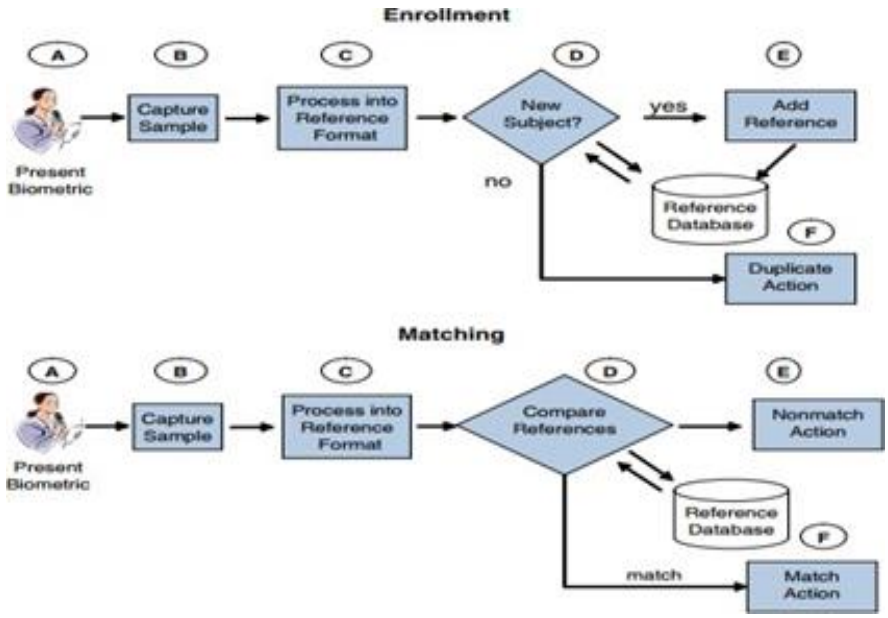


Figure-4 System Architecture

False non-match rates of fingerprint matchers are very high in the case of severely distorted fingerprints. This generates a security hole in automatic fingerprint recognition systems which can be utilized by criminals and terrorists. For this reason, it is necessary to develop fingerprint distortion detection and rectification algorithms to fill the hole.

6. Conclusion and Future Work

This network uses classic convolutional operations that can be viewed as linear and non-linear image processing operations. When stacked, these operations essentially extract higher level representations, named multiband images, whose pixel attributes are concatenated into high-dimensional feature vectors for later pattern recognition. False non-match rates of fingerprint matchers are very high in the case of severely distorted fingerprints. This generates a security hole in automatic fingerprint recognition systems which can be utilized by criminals and terrorists. For this reason, it is necessary to develop fingerprint distortion detection and rectification algorithms to fill the hole.

This network uses classic convolutional operations that can be viewed as linear and non-linear image processing operations. When stacked, these operations essentially extract higher level representations, named multiband images, whose pixel attributes are concatenated into high-dimensional feature vectors for later pattern recognition. False non-match rates of fingerprint matchers are very high in the case of severely distorted fingerprints. This generates a security hole in automatic fingerprint recognition systems which can be utilized by criminals and terrorists. For this reason, it is necessary to develop fingerprint distortion detection and rectification algorithms to fill the hole.

Face Spoof Detection

Face spoof detection requirements include:

1. Understanding the characteristics and requirements of the use case scenarios for face spoof detection

2. Collecting a large and representative database that considers the user demographics (age, gender, and race) and ambient illumination in the use case scenario of interest
3. Developing robust, effective, and efficient features (e.g., through feature transformations) for the selected use case scenario
4. Considering user-specific training for face spoof detection

For future work, we intend to evaluate such datasets using the proposed approaches here and also consider other biometric modalities such as palm, vein, and gait. Finally, it is important to take all the results discussed herein with a grain of salt. We are not presenting the final word in spoofing detection. In fact, there is important additional research that could finally take this research another step forward. We envision the application of deep learning representations on top of pre-processed image feature maps (e.g., LBP-like feature maps, acquisition-based maps exploring noise signatures, visual rhythm representations, etc.). With an n-layer feature representation, we might be able to explore features otherwise not possible using the raw data. In addition, exploring temporal coherence and fusion would be also important for video-based attacks.

7. References

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[2] M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme using smart cards," IEEE Trans. Consumer Electron., vol. CE-46, no. 1, pp. 28–30, Feb. 2000.
[3] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," IEEE Trans. Consumer Electron., vol. CE-46, no. 4, pp. 958– 961, Nov. 2000.
[4] C.-K. Chan, and L.M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. Consumer Electron., vol. CE-46, no. 4, pp. 992–993, Nov. 2000.
[5] R. Amin, and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, vol. 36, no. 1, pp. 58–80, Jan. 2016.
[6] R. Amin, and G. P. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS," Journal of Medical Systems, vol. 39, no. 3, pp. 1–17, Mar. 2015.
[7] F.-Y. Yang, T.-D. Wu, and S.-H. Chiu, "A secure control protocol for USB mass storage devices," IEEE Trans. Consumer Electron., vol. CE56, no. 4, pp. 2339–2343, Nov. 2010.
[8] B. Chen, C. Qin, and L. Yu, "A Secure Access Authentication Scheme for Removable Storage Media," Journal of Information & Computational Science, vol. 9, no. 15, pp. 4353–4363, Nov. 2012.
[9] C. Lee, C. Chen, and P. Wu, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," IET Computers & Digital Techniques, vol. 7, no. 1, pp. 48–55, Jan. 2013.
[10] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," IEEE Trans. Consumer Electron., vol. CE-60, no. 1, pp. 30–37, Feb. 2014.

8.Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

9.Funding

No external funding was received to support or conduct this study.