AbsoluteSecure: A Tri-Layered Data Security System

Oluwafemi Osho[1], Farouk A. Musa[2], Sanjay Misra[3](✉), Andrew A. Uduimoh[1], Adewole Adewunmi[3], and Ravin Ahuja[4]

[1] Federal University of Technology, Minna, Nigeria
{femi.osho,a.uduimoh}@futminna.edu.ng
[2] DigitalJewels, Lagos, Nigeria
faroukm@digitaljewel.net
[3] Covenant University, Ota, Nigeria
{sanjay.misra,
wole.adewunmi}@covenantuniversity.edu.ng
[4] Vishwakarma Skill University Gurugram, Gurugram, Hariyana, India

Abstract. Data has been touted as the new oil. This attests to the level of importance it has garnered over the years. With increased proliferation of and advancements in technology, data is bound to play more prominent role. The need for data security, therefore, cannot be overstated. Existing systems for securing data often rely on one or combination of biometric, cryptography, and steganography. In this paper, we propose AbsoluteSecure, a data security system that combines the three techniques to enhance the security of data. The system is implemented using C#. To evaluate its performance, experiments are performed to assess its usability and security. Specifically, on usability, its capacity to successfully enroll a new user's fingerprint and authenticate an enrolled user are evaluated. On the other hand, to ascertain its security, we measure how much it can detect and deny access to unauthorized users, both at the authentication and usage levels. The results of the experiments show that AbsoluteSecure can ensure the confidentiality, integrity, and availability of data.

Keywords: Cryptography · Steganography · Biometric · Multi-layer security

1 Introduction

In recent times, the world has indeed experienced much technological progress. This has helped to improve the way we carry out various operations, thereby saving computational time and resources, leading to improved results. However, these improvements in technology have posed their attendant challenges, such as the need to secure highly-priced data. This is due to the activities of attackers who continue to develop and deploy increasingly sophisticated tools and methods, to carry out different attacks against users' data. Some of the attacks include data modification, deletion, denial of service, impersonation, eavesdropping, and identity theft [1, 2]. According to a survey by Ponemon Institute in 2018, the estimated average total cost of a data breach was $3.86 million. This was an increase of 6.4% when compared to the preceding year.

R. Damaševičius and G. Vasiljevienė (Eds.): ICIST 2019, CCIS 1078, pp. 243–255, 2019.
https://doi.org/10.1007/978-3-030-30275-7_19

The report also forecasted the likelihood of reoccurrence of breach over the next two years as 27.8% [3].

Security of confidential data is unarguably very important. It is the sole foundation of data confidentiality, integrity and availability, which are paramount in the transmission of data in data systems [4].

Table 1. Summary of existing studies

Category	Method	Scheme	Work
Single	Cryptography	RSA	Jamgekar et al. [6] Osho et al. [7]
		AES	Elfakharany [8]
	Steganography	Audio	Verma et al. [9]
		Image	Kamath [10]
		Video	Bodhak et al. [11]
	Biometrics	Brain	Damasevicius [12]
		Fingerprint	Patel [13]
		Gait	Damasevicius [14]
		Voice	Paunovic et al. [15]
Hybrid	Cryptography + Biometrics	AES + Fingerprint	Ojeniyi et al. [4]
	Cryptography + Steganography	Blowfish + Image	Dixit et al. [16]
		Image + RSA	Gupta et al. [17]
		Visual Cryptography + Text	Roy et al. [18]
	Biometrics + Steganography	Fingerprint + Face + Image	Paul et al. [19]
		Fingerprint + Image	Shubhangi et al. [20]
		Skin + Image	Shejul et al. [21]
	Multimodal biometrics	Face + fingerprint	Shanthini et al. [22]

To improve data security, many systems have been proposed (Table 1). These systems make use of different techniques individually or in combination, such as cryptography, steganography, and biometrics, to enhance the security of data. Each of these techniques, however, have some limitations. For instance, in cryptography, the cipertext, if intercepted by an adversary, could be subjected to cryptanalysis. Similarly, a message concealed using steganography could be exposed if subjected to steganalysis. Consequently, a data security system that one of or combines both cryptographic and steganographic techniques would need further improvement. One option is to integrate both techniques with biometrics. Biometrics leverages the uniqueness in the physical or behavioural attributes of an individual or entity [5]. Table 2 presents the performance of different mitigation mechanisms using one, two or combination of the three techniques against different attacks.

Table 2. A summary of data attacks and performance of different mitigating techniques

Category	Attack	Cryptography	Cryptography + Steganography	Cryptography + Steganography + Biometrics
Confidentiality	Data theft	No	No	Yes
	Cryptanalysis	No	No	Yes
	Brute force	No	No	Yes
	Sniffing	No	Yes	Yes
	Eavesdropping	Yes	Yes	Yes
	Man in the middle	Yes	Yes	Yes
	Key logging	No	No	Yes
Integrity	Data diddling	Yes	Yes	Yes
	Data modification	Yes	Yes	Yes
	Masquerading	No	No	Yes
	Salami attack	No	Yes	Yes
Availability	Denial of service	No	No	Yes
	Data deletion	No	No	Yes
	Buffer overflow	No	No	No

This study proposes and implements a secure data security system that demonstrates the integration of cryptography, steganography and biometrics for enhancing security of data.

The rest of the study is organized as follows: in section two, we review related concepts. Section three presents the proposed system. A proof-of-concept and evaluation of the performance of the system are presented in sections four and five respectively. Section six concludes the study.

2 Literature Review

2.1 Cryptography

Cryptography is a technique used to secure digital information or communication from unauthorized access. It is used for providing access control mechanism in systems and preventing attackers, who gain unauthorized access to systems, from accessing confidential information. It has been widely adopted by the intelligence organisations, government, individuals and also the military.

Cryptography exists in two categories: symmetric (also called private key cryptography) and asymmetric cryptography (also known as public key cryptography). In symmetric cryptography, the same key is used for the sending and receiving of messages, that is, the same key is employed for encryption and decryption [23] The key is known to both the sending and the receiving parties. Examples are Data Encryption Standard (DES) and Advanced Encryption Standards (AES).

In Asymmetric, also known as public key, cryptography, two different keys are generated for the encryption and decryption process. The key used for encryption, known as the public key, is known to any encrypter, hence it being termed public. The key used for decrypting is called the private key. One of the most popular is the RSA cryptosystem. It is widely used in various protocols and platforms. Others include Rabin, ElGamal, NTRU, and Paillie.

Cryptography is indeed a very sustainable means of securing data and communication lines. However, irrespective of the strength of a cryptosystem, it can still be exposed to cryptanalysis in the event of interception by an unauthorized party [24].

2.2 Steganography

Steganography has been used over the years to protect valuable data through obscurity. In steganography, data is protected by concealing it in a covert medium, which masks the existence of the data. Data undergoes steganography to produce a stego-object [25]. The stego-object comprises of a cover medium and the payload. The cover medium is the media used to mask the data. The data that is being masked is called the payload.

Steganography is widely used by intellectual property holders, using a technique known as watermarking, to protect their works against piracy [20]. It can also be combined with cryptography to attain improved security of data [16]. Modern steganography uses a wider variety of media as the cover medium. These include audio, video, image, and text.

It is important to note that steganography does not modify or transform a given data, it merely masks the data with a specified medium (cover medium) in such a way that makes it unable to be noticed by anyone. Therefore, the security of a steganographic process depends entirely on the eradication of the possibility of it being identified by an adversary [26].

2.3 Biometrics

Biometrics involves the various techniques used to identify individuals using their unique psychological or behavioural qualities. These qualities include the human voice, signature, face, fingerprint, DNA, retina, iris, and ear shape [13, 15, 27–30].

Biometrics as a form of authentication has been in usage since the 1890s. It was used in Argentina where a fingerprint template was created. Fingerprint biometrics then became an official measure for identifying humans in the 1900s.

Biometric features of individuals are extremely unique and the possibility of counterfeiting biometric traits is quite impossible. That makes it an efficient technique for human identification, hence its common use for authentication [5].

Biometric systems generally consists of three units, viz., the sensor, the data processing unit and the user application. The sensor refers to any component used to collect the minutiae data from the individual. The data processing component handles the collection and matching of user biometric trait. The user application gives the user the interface to interact with [27].

Authentication in biometric systems follow three steps. The biometric sample of the user is first collected and stored. At authentication, the matching algorithm collects a test sample, which is compared with the stored one. A mathematical value is then generated and the degree of similarity and dissimilarity is calculated. A match is met when the mathematical degree reaches a biometric mean set by the matching algorithm [27].

3 Proposed Tri-Layered Data Security System

Analysis of existing data security systems revealed the use or one or combination of cryptographic, biometric, and steganographic techniques for securing data. Each of these techniques has its own limitations, as well as combining any two of them.

3.1 Requirement Definition

There are some core and basic functional and non-functional requirements a data security system must satisfy to effectively secure data. These include the following:

- The data security system should ensure new users are successfully enrolled.
- The data security system should ensure unauthorized persons cannot gain access to authorized users' data.
- The data security system should ensure a legitimate user cannot gain unauthorized access to the data of other users.
- The data security system should be easy to use.

3.2 Framework of Proposed System

To enhance data security, we propose AbsoluteSecure, a tri-layered data security system that leverages biometrics, cryptography and steganography for securing data. The system combines fingerprint biometrics, Advanced Encryption Standard (AES), and LSB image steganography. The proposed system is presented in Fig. 1.

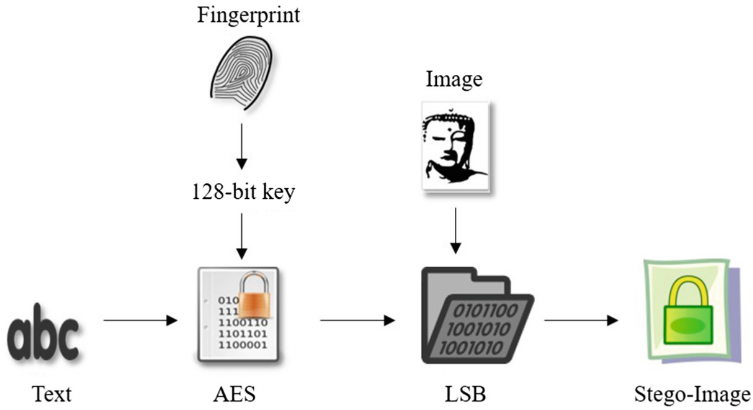

Fig. 1. Proposed tri-layered data security system

The fingerprint biometrics component serves two purposes: authentication and generation of a 128-bit key used for both encrypting and decrypting messages. The key is generated using the minutiae points extracted from the fingerprint. To extract the minutiae points, the steps include [31, 32]:

- Image preprocessing using histogram equalization.
- Segmentation of the preprocessed fingerprint.
- Orientation field estimation, which helps in the recognition of poor quality latents.
- Image enhancement. This is done before minutiae extraction for the purpose of further enhancing the fingerprint image. Methods used include Gaussian Low-Pass Filter and Gabor Filter.
- Region of Interest (ROI) selection using binarization and morphological operators.
- Thinning.

The system uses the Advanced Encryption System (AES) to encrypt/decrypt the data. The AES uses a 128 bit key length, generated from the user's fingerprint biometric features. It consists of layers, which manipulate a 4 by 4 array of bytes, or 128 bits of data path, commonly called the state. Every round of AES undergoes four stages: key addition, byte substitution, permutation of the data on a byte level (ShiftRows), and mixing blocks of four bytes (MixColumn) [33, 34]. The block diagram of the AES is presented in Fig. 2.

3.3 Process Design

To use our proposed tri-layered data security system, a user would need to be enrolled on the system. The enrollment and usage processes are described below.

Enrollment

Enrolment of a new user is usually facilitated by the administrator. The new user specifies a user name and password. Thereafter, the biometric details are captured. Once this process is complete the user subsequently can use the system.

Usage

Depending on the user, there are two level of access: administrator and ordinary user. While both categories of users have access to use the system for securing their data, the administrator has the additional privilege of facilitating the enrolment of new users. Figure 3 depicts an activity diagram of levels of usage our proposed system.

To secure a piece of data, a user can either load a text from memory, or manually type the text into the text field. The user is then prompted to select a recipient. The next stage entails selecting a cover image from memory, which is used to produce the stego-image

Retrieval of data follows a reverse order. After logging in to the system, the user loads the stego-image from memory, then extracts the ciphertext, and finally decrypts the ciphertext to get the plaintext. The sequence of process involved in both securing and retrieving data is illustrated in Fig. 4.

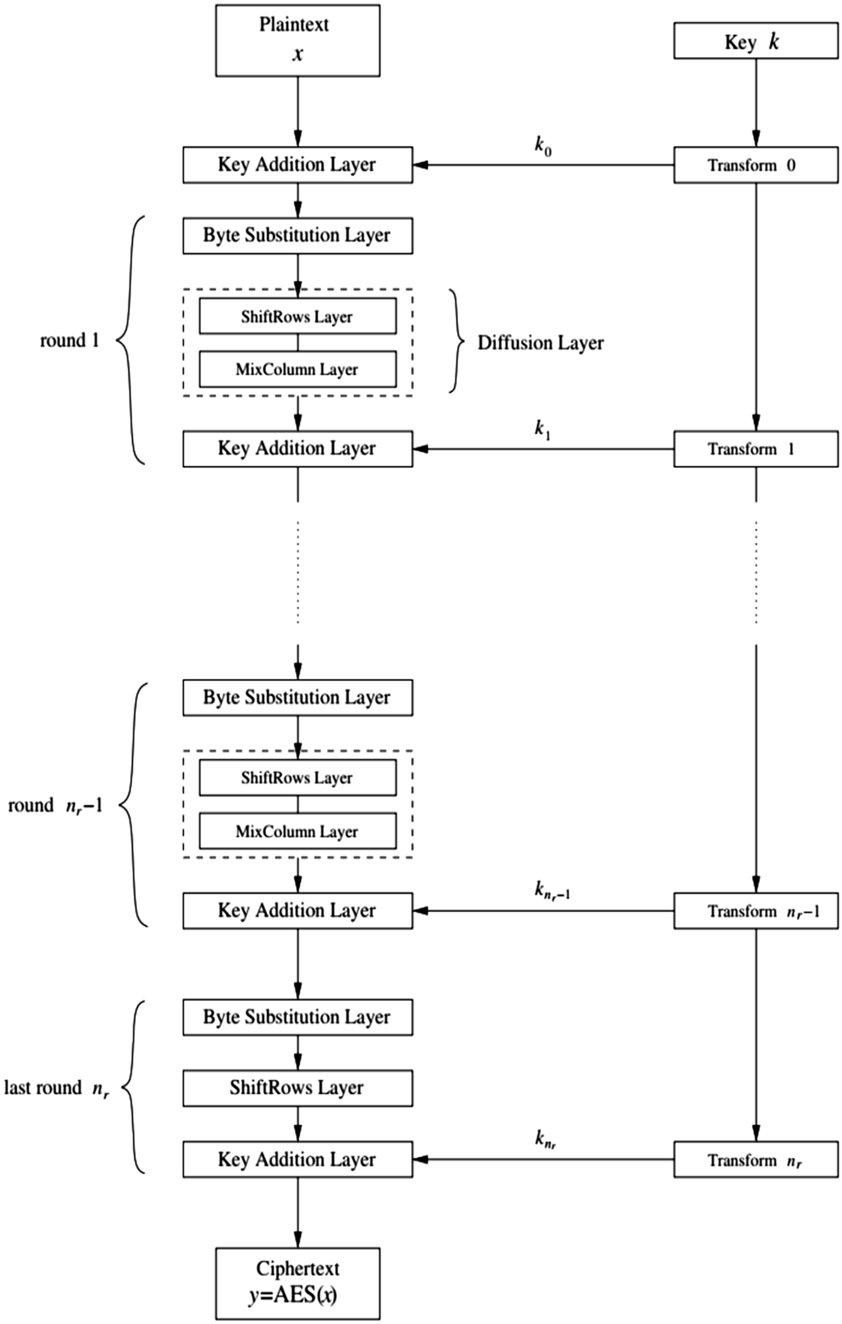

Fig. 2. AES encryption process [34]

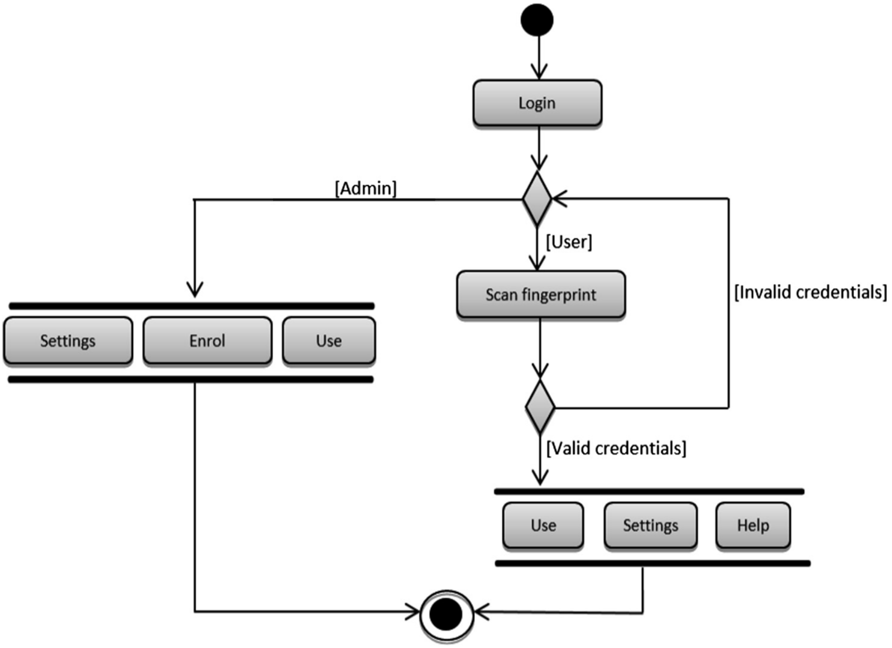

Fig. 3. Activity diagram of levels of usage

4 System Implementation

To implement AbsoluteSecure, the following hardware and software resources were used:

- C#: the programming language.
- Microsoft Visual Studio 2010: the integrated development environment, for coding, debugging and executing of source codes.
- DigitalPersona U.are.U 4000B fingerprint reader and software development kit: for fingerprint biometric enrolment and authentication.
- A Sony VAIO VPCEA45FA Laptop (Specification: 4 GB RAM, Core i3 Intel processor, 2.53 GHz Dual Core processor speed, 320 GB Hard Drive, and Windows 8 Operating System: for testing the system.

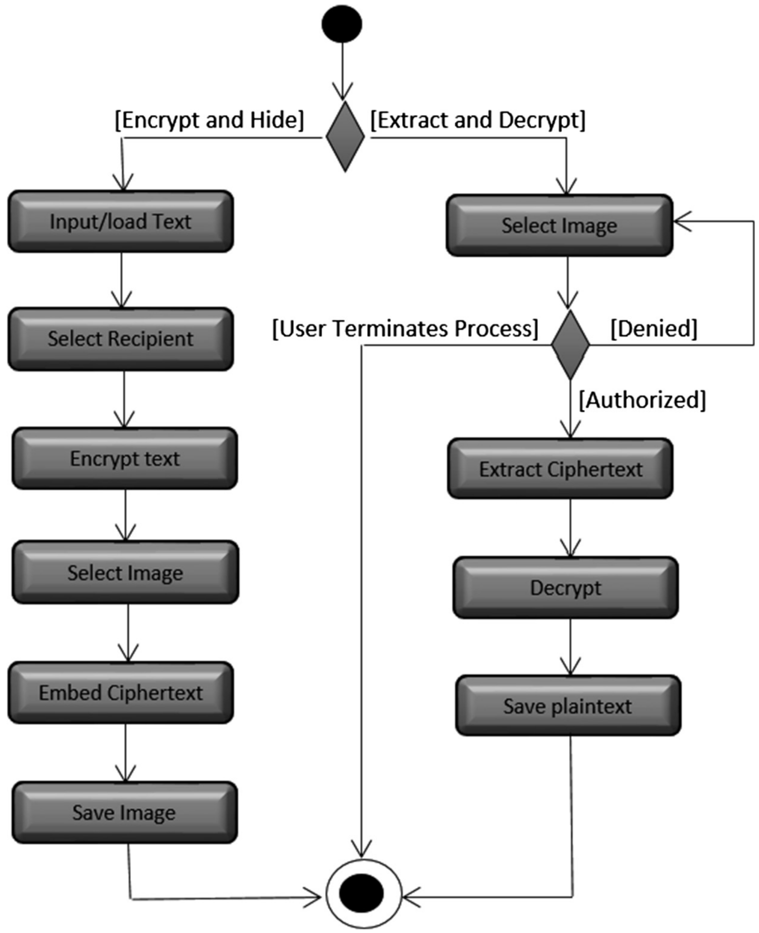

Fig. 4. Activity diagram of securing and retrieval of data

5 Performance Evaluation

To use the system, an enrolled user is presented with the login interface, which accepts the individual's username and password. If the credentials match one of the records in the database, the individual is then allowed to submit a fingerprint sample via a fingerprint scanner. If the sample matches the username and password combination, the individual is granted access to the corresponding profile.

To evaluate the performance of the system, we considered its usability and security. Twenty individuals were used, comprising ten enrolled and ten illegitimate users.

5.1 System Usability

To determine if our system was usable, we evaluated its capacity to successfully enroll the fingerprint of a new user and not reject a legitimate user. These were used to determine the failure to enroll rate (FER) and false rejection rate (FRR). The experiments were performed using ten individuals.

Failure to Enroll Rate (FER)
This implies the rate at which the biometric system fails to enroll a new user. We denote this as FER, and is calculated as:

$$\text{FER} = \frac{\text{Number of times a system refused to enrol user}}{\text{Number of trials}} \times 100 \tag{1}$$

For each of the ten individuals, there were five enrollment attempts. Out of a total of fifty trials, we recorded two instances where the fingerprint of a user was not enrolled by the system. This gives an FER of 4%.

False Rejection Rate (FRR)
This calculates the likelihood of a legitimate user being denied access. We considered the FRR at the authentication level, denoted by FRR_{Auth}, to evaluate the rate at which the enrolled users were denied login access to their respective profiles. On the other hand, the FRR_{Usg} indicates the rate at which the legitimate users could not access their data and other system functionality. In both cases, for each of the ten users, five attempts were made.

The FRR is represented mathematically as:

$$FRR = \frac{\text{Number of times an enrolled user was not recognised}}{\text{Total number of trials}} \times 100 \tag{2}$$

From our experiments, both FRR_{Auth} and FRR_{Usg} were 0%, i.e. there were no instances recorded where legitimate users could not be authenticated by the system nor allowed access to their data.

5.2 System Security

To assess how secure the system is against unauthorized access, we evaluated its capacity to detect and deny access to unauthorized users, both at the authentication and usage levels. The experiments consisted of the use of ten legitimate and ten illegitimate users.

False Acceptance Rate (FAR)
The FAR was first evaluated at the authentication stage. Denoted as FAR_{Auth}, this amounts to the rate at which illegitimate users were accepted as legitimate and successfully authenticated. Five of them were given the username and password of legitimate users. This was used to simulate a situation where the username and password of some legitimate users are known to attackers. One means of achieving this is through social engineering. The remaining five were not given any details. In real life,

these represent attackers with no prior knowledge of any legitimate users' details, who would try to brute-force to gain access to the system. Each of the test users were asked to make five login attempts.

The second experiment, represented as FAR_{Usg}, implies measuring the likelihood of users accessing the data of other users without authorization. To determine this, we asked each of the ten legitimate users to try, in five attempts, to access data belonging to other users.

Mathematically, the FAR is calculated using the formula:

$$FAR = \frac{\text{Number of times the system accepts an illegitimate user}}{\text{Total number of trials}} \times 100 \qquad (3)$$

From results obtained, both FAR_{Auth} and FAR_{Usg} were 0%. None of the illegitimate users was successfully authenticated by the system. Also, not one of the legitimate users could gain access to any other user's data.

Table 3 provides a summary of the different results from the five experiments. In terms of enrolling new users, the system recorded a success rate of 96%. On the other hand, analysis of the results suggests its immense capacity to effectively secure users' data.

The system ensures confidentiality of users' information first by preventing unauthorized access by un-enrolled individual at the authentication level. Even when the username and password associated with a legitimate user are known by an un-enrolled individual, at the biometric level authentication is denied. In the same vein, for a user enrolled on the system, the likelihood of an unauthorized access to other users' data, as demonstrated by the system, was zero. It also supports confidentiality by encrypting the stored data and hiding them in an image.

Table 3. Performance evaluation of AbsoluteSecure

Metric	Rate
FER_{Auth}	4%
FRR_{Auth}	0%
FRR_{Usg}	0%
FAR_{Auth}	0%
FAR_{Usg}	0%

One of the consequences of successfully preventing unauthorized access to the stored data is the guarantee of integrity of information. As long as an attacker cannot gain unauthorized access to users' data, it cannot be modified.

Our proposed system also guarantee availability of data by preventing data deletion by unauthorized individuals. This is equally achieved by denying unauthorized users access to data belonging to legitimate users.

6 Conclusion

In this study, we proposed a multi-layer data security system that leverages on biometric, cryptography, and steganography for securing data. The system can be deployed both as a standalone or network application. The proposed system was implemented and tested. Based on the results of experiments performed to evaluate its usability and security, we demonstrated the capacity of AbsoluteSecure to provide effective security of data, ensuring confidentiality, integrity, and availability of data. Specifically, while ensuring that enrolled users are successfully authenticated and able to access their data all the time, the system ensured zero likelihood of unauthorized access to users' data.

The main focus of this study was demonstrating the integration of cryptographic, biometric, and steganographic techniques to secure data. As much as this was achieved, there are areas that were not covered. For example, the performance of the system under high-volume data could be explored in further studies. Another area worth investigating is how the integrated techniques influence hardware resources.

References

1. Ahmad, A.: Types of security threats and it's preventions. Int. J. Comput. Technol. Appl. **3** (3), 720–752 (2012)
2. Microsoft: Common Types of Network Attacks [Internet]. Microsoft Technet (2011). [cited 17 Aug 2015]
3. Ponemon Institute: 2018 Cost of a Data Breach Study: Global Overview (2018)
4. Ojeniyi, J.A., Waziri, V.O., Suleiman, I.: Improved data security framework based on advanced encryption standard and fingerprint. In: Proceedings of the International Conference on Science, Technology, Education, Arts, Management and Social Sciences (iSTEAMS), pp. 111–120. iSTEAMS Research Nexus (2014)
5. Jain, A.K., Ross, A., Nandakumar, K.: An introduction to biometrics. In: 2008 19th International Conference on Pattern Recognition, Tampa, Florida. IEEE (2008)
6. Jamgekar, R.S., Joshi, G.S.: File encryption and decryption using secure RSA. Int. J. Emerg. Sci. Eng. **1**(4), 11–14 (2013)
7. Osho, O., Zubair, Y.O., Ojeniyi, J.A., Osho, L.O.: A simple encryption and decryption system. In: International Conference on Science, Technology, Education, Arts, Management and Social Sciences (iSTEAMS), Ado-Ekiti, Nigeria, pp. 77–84. iSTEAMS Research Nexus (2014)
8. Elfakharany, S.: Secure mobile payment protocol using asymmetric encryption for authorization. J. Netw. Commun. Emerg. Technol. **2**(2), 34–40 (2015)
9. Verma, T.G., Hasan, Z., Verma, G.: A unique approach for data hiding using audio steganography. Int. J. Mod. Eng. Res. (IJMER) **3**(4), 2098–2101 (2013)
10. Kamath, P.R.: A secure and high capacity image, steganography technique. Int. J. Signal Image Process. (SIPIJ) **4**(1), 83–89 (2013)
11. Bodhak, P.V., Gunjal, B.L.: Improved protection in video steganography. Int. J. Eng. Innov. Technol. (IJEIT) **1**(4), 31–37 (2012)
12. Damaševicius, R., Maskeliunas, R., Kazanavicius, E., Wozniak, M.: Combining cryptography with EEG biometrics. Comput. Intell. Neurosci. **2018**, 1–11 (2018)
13. Patel, U.: A study on fingerprint biometrics recognition. Int. J. Eng. Sci. **1**(2), 1–6 (2015)

14. Damasevicius, R., Maskeliunas, R., Venckauskas, A., Wozniak, M.: Smartphone user identity verification using gait characteristics robertas. Symmetry **8**(100), 1–20 (2016)
15. Paunović, S., Nešić, L., Kovačević, J.: Application of voice biometrics in protection systems and crime fighting. J. Inf. Technol. Appl. **4**(2), 59–67 (2012)
16. Dixit, P.H., Waskar, K.B., Bombale, U.L.: Multilevel network security combining cryptography and steganography on ARM platform. J. Embed. Syst. **3**(1), 11–15 (2015)
17. Gupta, S., Ankur, G., Bhushan, B.: Information hiding using least significant bit steganography and cryptography. Int. J. Mod. Educ. Comput. Sci. **6**(1), 27–34 (2012)
18. Roy, S., Venkateswaran, P.: Online payment system using steganography and visual cryptography. In: 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2014, pp. 1–5 (2014)
19. Paul, L., Anilkumar, M.: Authentication for online voting using steganography and biometrics. Int. J. Adv. Res. **1**(10), 26–32 (2012)
20. Shubhangi, D.C., Malipatil, M.: Authentication watermarking for transmission of hidden data using biometrics technique. Int. J. Emerg. Technol. Adv. Eng. **2**(5), 1–6 (2012)
21. Shejul, A.A., Kulkarni, U.L.: A DWT based approach for steganography using biometrics. In: 2010 International Conference on Data Storage and Data Engineering (DSDE), pp. 39–43 (2010)
22. Shanthini, B., Swamynathan, S.: Multimodal biometric-based secured authentication system using steganography. J. Comput. Sci. **8**(7), 1012–1021 (2012)
23. Dorst, K., Stewart, S., Staudinger, I., Paton, B.: Symmetric cryptography. In: Dagstuhl Reports Conference, pp. 1–16 (2012)
24. Atul, K.: Cryptography and Network Security, 2nd edn. Tata McGraw-Hill Education (2008)
25. Amirtharaj, R., Rayappan, J.B.B.: Steganography-time to time: a review. Res. J. Inf. Technol. **5**(2), 53–66 (2013)
26. Jayaram, P., Ranganatha, H.R., Anupama, H.S.: Information hiding using audio steganography - a survey. Int. J. Multimed. Appl. **3**, 86–96 (2011)
27. Singhal, R., Jain, P.: Biometrics: enhancing security. Asian J. Comput. Sci. Inf. Technol. **3**, 89–92 (2011)
28. Bowyer, K.W., Hollingsworth, K.P., Flynn, P.J.: A survey of iris biometrics research: 2008–2010. In: Handbook of Iris Recognition, pp. 15–54 (2013)
29. Li, Z., Park, U., Jain, A.K.: A discriminative model for age invariant face recognition. IEEE Trans. Inf. Forensics Secur. **6**(3), 1028–1037 (2011)
30. Aronowitz, H., Hoory, R., Pelecanos, J., Nahamoo, D.: New developments in voice biometrics for user authentication. In: Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH, pp. 17–20 (2011)
31. Shodhganga: Design of Secured Key Generation Algorithm using Fingerprint Based Biometric Modality
32. Jagadeesan, A., Duraiswamy, K.: Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris. Int. J. Comput. Sci. Inf. Secur. **7**(1), 296–305 (2010)
33. Katz, J., Lindell, Y.: Introduction to Modern Cryptography, pp. 1–498. CRC Press, Boca Raton (2007)
34. Paar, C., Pelzl, J.: Understanding Cryptography, pp. 1–372. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-04101-3