Toward an AI Chatbot-Driven Advanced Digital Locker

Arindam Dan, Sumit Gupta, Shubham Rakshit and Soumadip Banerjee

Abstract The ongoing digital era is witnessing and endorsing online transactions and information exchange at the speed of light. But the increasing number of hackers and social engineers has made the digital environment susceptible and vulnerable to intrusion and attack. Also, because of the dearth of advanced security models, maintaining security and protecting integrity of sensitive information is at stake. What the world needs now is a robust and reliable security model to establish information security and secure all digital transactions. Through this project work, we are introducing an artificially intelligent chatbot that will provide a user with the menu for choosing an appropriate encryption method (out of AES, DES, RC2, and hybrid methods) for securing his/her crucial information. The proposed idea of a firewall-based advanced digital locker for authenticating user's digital signature before allowing access to the encrypted files provides the authorized user with a sense of more robustness, reliability, and a higher level of security.

Keywords Encryption · Decryption · Chatbot · Digital signature · Image steganography

A. Dan (✉) · S. Gupta (✉) · S. Rakshit · S. Banerjee
University Institute of Technology, The University of Burdwan, Golapbag (North), Burdwan 713104, West Bengal, India
e-mail: danarindam1233@gmail.com

S. Gupta
e-mail: sgupta@uit.buruniv.ac.in

S. Rakshit
e-mail: shubhamr238@gmail.com

S. Banerjee
e-mail: soumadipban000@gmail.com

M. Chakraborty et al. (eds.), *Proceedings of International Ethical Hacking Conference 2018*, Advances in Intelligent Systems and Computing 811,
https://doi.org/10.1007/978-981-13-1544-2_4

1 Introduction

The world is full of fascinating problems waiting to be solved. Security issue is one such problem that has been researched and analyzed since a long time, but due to the advent of latest technologies, there still remains a lot of horizons untraveled and unexplored. As we know, uploading of any file or document containing sensitive information to any server (like cloud storage) is a vulnerable process as chances of the file getting hacked or its content being altered comes into picture. Further, storing any sensitive information in any disk has several issues and risks involved. Thus, there arises a need for a system that could save the uploaded document in an encrypted form. If the original file is encrypted, then the hacker would not be able to decipher the contents even after getting access to the file. The presence of digital locker will provide a storage area where the encrypted file will be stored. The crucial aspect of the digital locker is that it can only be accessed via the digital signature of the authorized user. So, the chances of accessing such a locker will be a difficult task for any intruder or hacker.

The most important requirement in information security is the presence of a right person who would guide us through the entire process of file encryption. In real life, getting this person is a very difficult and challenging task. Even if we get hold of a person who will help us in understanding the intricate encryption techniques and procedures, the person will charge us a handsome amount. Moreover, the person would come to know about all the procedures used and the secret keys generated during the encryption process, thus posing a chance of blackmailing or threat in near future. Our AI chatbot proposed in this paper will be the best alternative to deal with this situation. The chatbot will act as a virtual assistant and will work as per the order and command of the user. Thus, the user will no longer have to depend on any physical entity for help.

This paper is organized as follows: Sect. 2 discusses the previous related works on various security models by different researchers. In Sect. 3, we have presented our proposed model that helps in protecting data. Section 4 discusses the implementation and results obtained. Section 5 highlights the future scope of improvements in our work. In Sect. 6, we have finally concluded our paper followed by references in the end.

2 Previous Related Work

Many researchers have proposed a variety of security models to protect and safeguard information by using the cryptographic techniques such as encryption and digital signature to name a few. This section discusses a few of the most popular works related to this domain.

The authors in the paper [1] have designed a Web services-based security model by integrating the watermark embedding and watermark detection technology components with the Web services. The proposed system architecture is based on Web services via SOAP service requester, digital certificates, XML encryption, and digital signatures to ensure secure exchange of online information between service providers while carrying out multimedia services, online services, and e-work applications.

Researchers in [2] have presented a patented security device by using a processor, an operating system (OS) software program loaded onto the processor, a type-II virtual machine monitor that will run on top of the host OS and create a user-definable number of sensitive, nonsensitive, encryption, and router virtual machines. This device is claimed to make the virtual computing environment secured and robust.

In paper [3], the authors have proposed an authentication algorithm based on the visual secret sharing scheme of the visual cryptography domain. They have offered a fool-proof lock-key mechanism in which every lock-key pair has a unique image associated with it. The lock can be opened by its paired key only, and the key cannot be duplicated. The lock has a memory and behaves like a safe door. It can be used to transmit and receive signals like the key. Here, the lock and the key can alter the pixel distribution of the secret image when an unauthorized access is triggered so that security can be established, and unauthorized access can be prevented.

Paper [4] provides a comparative study and evaluation of symmetric (AES, DES, Blowfish) as well as asymmetric (RSA) cryptographic algorithms by taking different types of files such as binary, text, and image files. Different evaluation parameters such as encryption time, decryption time, and throughput are considered by the author for performing the comparison, and AES algorithm was found to yield better performance.

The authors in the paper [5] have presented a review of digital lockers specifically based on the cloud platform. They have explained the features, objectives, and working of the digital locker which was released by the Department of Electronics and Information Technology (DeitY), Govt. of India [6]. Digital lockers have been created to provide a secure and dedicated personal electronic space for storing the documents on the cloud and to do away with the paperwork-based document storage for exploring the possibilities of the Digital India Campaign.

3 Our Proposed Work

Through this project work, we are introducing an AI chatbot-driven advanced digital locker for providing a user-friendly environment to a user for protecting one's sensitive information. In this work, we have designed a chatbot named Augusta which will help its user to secure data as per user's requirement. Here, we have primarily used

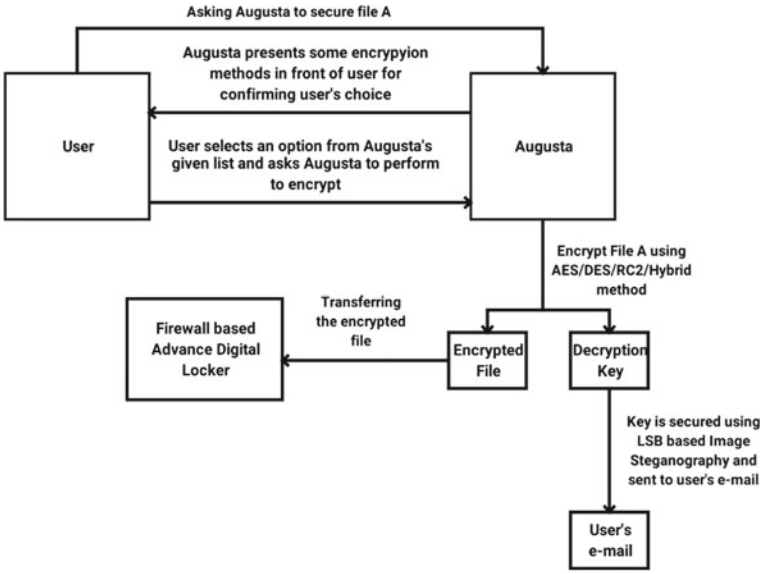

Fig. 1 Process of file encryption and transfer to advanced digital locker

four types of encryption methods, viz. Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest Cipher Encryption (RC2), and hybrid method (four hybrid methods by combining all the three named encryption methods).

As seen in Fig. 1, users will have the choice to encrypt their files as per their need, and all the encrypted files will be transferred to the advanced digital locker. This locker will be protected by a firewall. The decryption key of the corresponding encrypted files will be secured by least significant bit (LSB)-based image steganography method. Further, the resultant image version of that key will be sent to the user's email account.

We have also attempted to add an extra feature to our firewall-based advanced digital locker for checking the user's digital signature while collecting the encrypted files and for applying the decryption method consequently (see Fig. 2).

The novelty of our work lies in how an artificially intelligent chatbot is providing a user with the menu for choosing an appropriate encryption method (out of AES, DES, RC2, and hybrid methods) for securing his/her crucial information. The firewall-based advanced digital locker for authenticating user's digital signature before allowing access to the encrypted files provides the authorized user with a sense of more robustness, reliability, and a higher level of security.

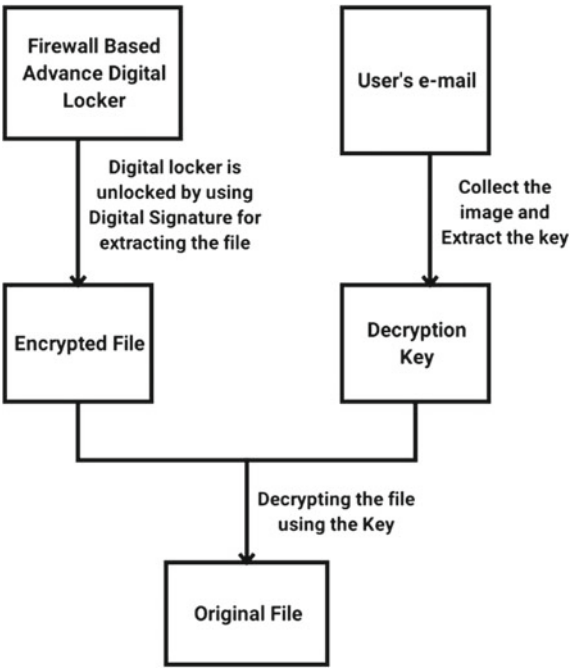

Fig. 2 Process of original file retrieval

4 Implementation and Results

To implement our proposed system, we have used Python 3.5 and SQLite. The algorithms such as AES [7, 8], DES [8, 9], RC2 [10], hybrid encryption, LSB-based image steganography [11, 12] are used in our project work. The operating system on which our project is built is Windows 10.

We have designed our AI-based chatbot named Augusta (see Fig. 3) which is capable of providing a user with a simple, understandable, and friendly environment for sharing and putting across his/her requirements. The chatbot provides the user with a menu of choices wherein a user can select which encryption algorithm the user wants to use for encrypting his/her file. Firstly, the user has to select the path from where the original file (where sensitive information is stored) is to be retrieved. After the path has been specified by the user, the chatbot asks the user to choose which encryption algorithm the user wants to use for encrypting the original file. Based on user's entry, the original file will be encrypted, and the user will be informed about successful completion of the encryption process. When the user chats with Augusta and opts for encrypting a file, he/she is prompted by Augusta to select the path where the original file is stored (see Fig. 4).

Fig. 3 Screenshot of AI chatbot Augusta

The creation of digital locker is shown in Fig. 5, and the encrypted files are stored in .dat format in the digital locker after the user chooses the encryption process, and the chatbot performs the encryption process successfully (see Fig. 6).

A comparative study based on the advantages and disadvantages offered by different security models has been given in Table 1 to comprehend how our proposed model is better than other existing approaches.

In Table 2, we have shown the performances of different encryption techniques, viz. AES, DES, and RC2 and their hybrid counterparts, viz. AES-DES, AES-RC2, DES-RC2, and AES-DES-RC2 on the basis of different factors such as key length, round(s), block size, speed, and security. On analyzing, it has been observed that as the hybrid models work in levels, they tend to offer more security than basic encryption techniques. The hybrid AES-DES-RC2 method offers the highest level of security at the cost of slow speed because three different levels L1, L2, and L3 of encryption is utilized in implementing this approach.

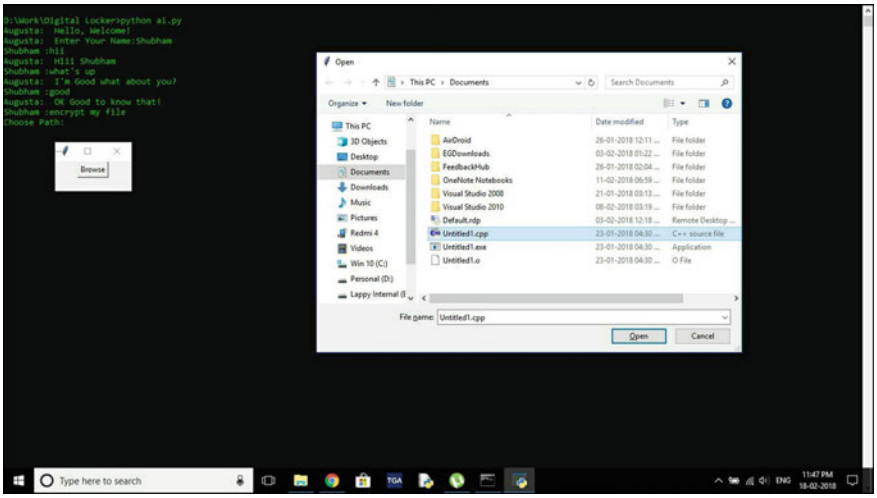

Fig. 4 Screenshot showing the selection of path where original file is stored

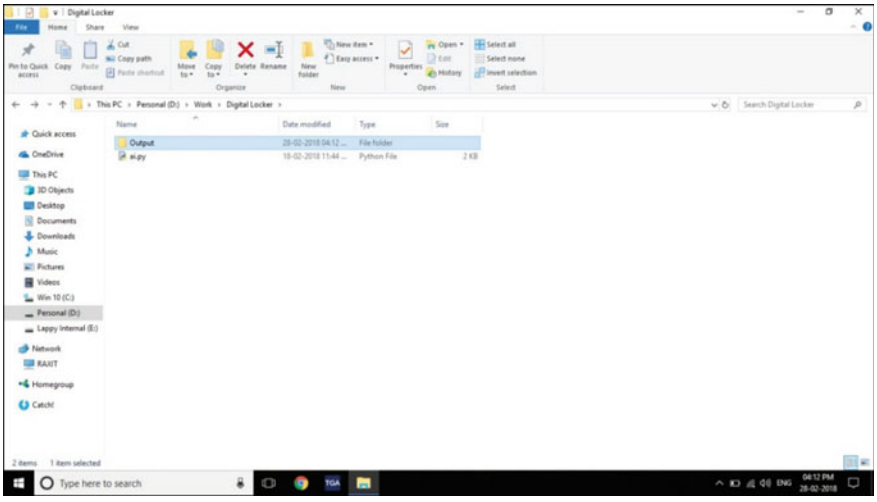

Fig. 5 Screenshot showing the folder of the digital locker

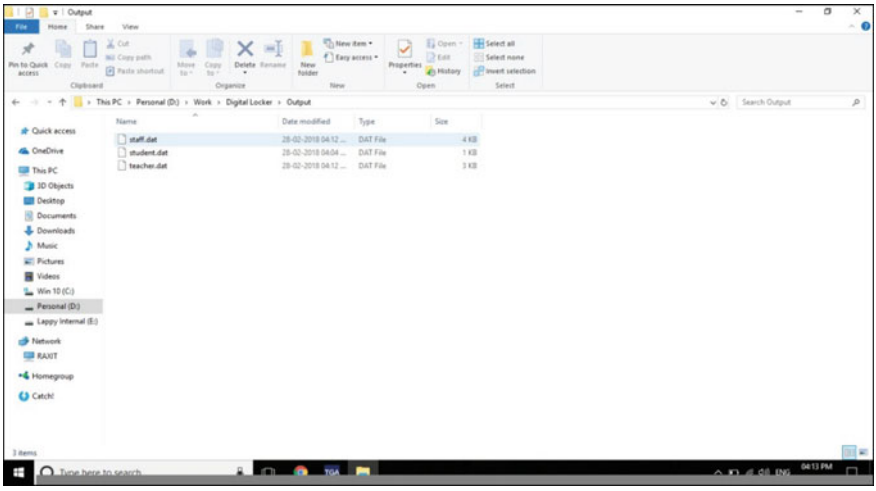

Fig. 6 Screenshot of encrypted files stored in digital locker

Table 1 Comparison of our proposed model with other existing security models

Sl. no.	Models	Advantages	Disadvantages
1	Web services-based security model	1. Digital watermarking 2. Web services via SOAP service requester 3. XML encryption and digital signatures	1. Risk of tampering and interception 2. Loss of data is possible
2	Cloud-based digital locker	1. Use of user-definable number of sensitive and nonsensitive virtual machines 2. Each encryption virtual machine is connected to one of the said user-definable number of sensitive virtual machines 3. Each encryption virtual machine includes at least one encryption algorithm	1. Requires server-client mode 2. If the host or server fails, the whole system fails
3	Device for and method of secure computing using virtual machines	1. Can be accessed from anywhere	1. No encryption technique is used 2. Chances of hacking is high
4	Our proposed model	1. Use of AI chatBot 2. Different encryption techniques including hybrid are used 3. Data is migrated to cloud storage-based digital locker 4. Decryption key is sent to user's email using LSB-based image steganography	1. Requires Internet connection

5 Future Work

Through this project work, we have aimed at creating an AI chatbot-driven advanced digital locker which would create a user-friendly environment to facilitate a user in encrypting any document by choosing any encryption algorithm (out of AES,

Table 2 Performance analysis of different encryption techniques

Factors	Basic			Hybrid				
	AES	DES	RC2	AES-DES		AES-RC2	DES-RC2	AES-DES-RC2
Key length	128, 192, or 256 bits	56 bits	8–1024 bits, in steps of 8 bits; default 64 bits	**L1**	128, 192, or 256 bits	128, 192, or 256 bits	56 bits	128, 192, or 256 bits
				L2	56 bits	8–1024 bits, in steps of 8 bits; default 64 bits	8–1024 bits, in steps of 8 bits; default 64 bits	56 bits
				L3	N/A	N/A	N/A	8–1024 bits, in steps of 8 bits; default 64 bits
Round(s)	10–128 bit key, 12–192 bit key, 14–256 bit key	16	16	**L1**	10–128 bit key, 12–192 bit key, 14–256 bit key	10–128 bit key, 12–192 bit key, 14–256 bit key	16	10–128 bit key, 12–192 bit key, 14–256 bit key
				L2	16	16	16	16
				L3	N/A	N/A	N/A	16
Block size	128 bits	64 bits	64 bits	**L1**	128 bits	128 bits	64 bits	128 bits
				L2	64 bits	64 bits	64 bits	64 bits
				L3	N/A	N/A	N/A	64 bits
Speed	Fast	Medium	Slow	Faster than AES-RC2, DES-RC2, and AES-DES-RC2		Faster than DES-RC2 and AES-DES-RC2	Faster than AES-DES-RC2	Very Slow
Security	High	Medium	Medium	Higher than AES-RC2 and DES-RC2 but lower than AES-DES-RC2		Higher than DES-RC2 but lower than AES-DES and AES-DES-RC2	Higher than basic encryption methods but lower than hybrid methods	Highest

DES, RC2 or hybrid encryption algorithms) as per user's choice or requirement. Till now, we have completed making the chatbot, and this chatbot is capable of encrypting a file based on user's choice. But our objective in future is to develop the firewall-based advanced digital locker for storing the encrypted file. We are also aiming at sending the secured decryption key in user's email via LSB-based image steganography method. In our next endeavor, we will incorporate the digital signature-based authentication mechanism so that only the authorized user could be able to extract the encrypted file from the locker and use the decryption key (received in his/her email) to finally decrypt the encrypted file and get back the original file.

6 Conclusion

This proposed system offers an advanced user-friendly application which offers an efficient, reliable, and secured platform for file access, storage, and retrieval with a high level of data protection. The use of various encryption algorithms added up with the presence of a chatbot (which acts as a virtual assistant) enhances the acceptability and popularity of our work among the masses.

References

1. Zhang, J.: A web services-based security model for digital watermarking. In: International Conference on Multimedia Technology (ICMT), pp. 4805–4808. IEEE, Hangzhou, China (2011)
2. Meushaw, R.V., Schneider, M.S., Simard, D.N., Wagner, G.M.: Device for and method of secure computing using virtual machines. In: United States Patent, Patent number-US6922774B2, Filing date: May 14, 2001, Issue date: Jul. 26, 2005. Application number: 09/854,818, United States (2005)
3. Tunga, H., Mukherjee, S.: Design and implementation of a novel authentication algorithm for fool-proof lock-key system based on visual secret sharing scheme. Int. J. Comput. Sci. Iss. (IJCSI) **9**(3), 182–186 (2012)
4. Panda, M.: Performance analysis of encryption algorithms for security. In: International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 278–284. IEEE, Paralakhemundi, India (2016)
5. Vaijawade, V., Khelkar, N., Thakare, D.: Review on "cloud based digital locker". In: International Journal of Research in Science & Engineering (IJRISE), Special Issue: Techno-Xtreme 16, pp. 682–686 (2016)
6. National eGovernance Division, Ministry of Electronics & Information Technology (MeitY), Government of India. http://digitallocker.gov.in. Accessed 28 Feb 2018
7. Daemen, J., Rijmen, V.: Rijndael: the advanced encryption standard. Dr. Dobb's J. **26**(3), 137–139 (2001)
8. Singh, G., Supriya: A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. Int. J. Comput. Appl. **67**(19), 33–38 (2013)
9. Nadeem, A., Javed, M.Y.: A performance comparison of data encryption algorithms. In: First International Conference on Information and Communication Technologies (ICICT), pp. 84–89. IEEE, Karachi, Pakistan (2006)
10. Knudsen, L.R., Rijmen, V., Rivest, R.L., Robshaw, M.J.B.: On the design and security of RC2. In: Vaudenay, S. (ed.) Fast Software Encryption (FSE), LNCS, pp. 206–221. Springer, Berlin, Heidelberg (1998)
11. Thangadurai, K., Devi, G.S.: An analysis of LSB based image steganography techniques. In: International Conference on Computer Communication and Informatics (ICCCI). IEEE, Coimbatore, India (2014)
12. Singh, A., Singh, H.: An improved LSB based image steganography technique for RGB images. In: International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, Coimbatore, India (2015)