A Simple Encryption and Decryption System

Conference Paper · May 2014

CITATIONS
2

READS
15,800

4 authors, including:

Oluwafemi Osho
Federal University of Technology Minna
39 PUBLICATIONS **197** CITATIONS
SEE PROFILE

Joseph Adebayo Ojeniyi
Federal University of Technology Minna
24 PUBLICATIONS **24** CITATIONS
SEE PROFILE

Lauretta O. Osho
Federal University of Technology Minna
6 PUBLICATIONS **13** CITATIONS
SEE PROFILE

A SIMPLE ENCRYPTION AND DECRYPTION SYSTEM

Oluwafemi Osho, Yunus O. Zubair & Joseph A. Ojeniyi
Department of Cyber Security Science
Federal University of Technology, Minna
Minna, Nigeria
femi.osho@futminna.edu.ng, yunexcyber@gmail.com, , ojeniyija@futminna.edu.ng
+2348034106811, +2348060311080, , +2348073303909

Lauretta O. Osho
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
laurettachristi@gmail.com
+2348057134292[3]

ABSTRACT
The internet generates very large amount of data on a daily basis. While some of the information are trivial others are sensitive. As a matter of fact, the security of some information traversing the internet is critical to the survival of the owner. In this study, we implement the RSA algorithm to produce a simple system for encryption and decryption of files with .txt extension. The system also incorporates digital signature to authenticate the sender of a message.

Key words: *Encryption, Decryption, RSA, Digital Signature, Software, Confidentiality, Integrity, Availability.*

1. BACKGROUND TO THE STUDY

Information is defined as a sequence of data that convey meaning to the person receiving it (Introna, 1992). It can be used to address the problem of decision making and reduces uncertainty. Information plays an important role in human life activities. Information distribution and accessibility have reduced the world to a global village. According to Meyer (2000), information is usually exchanged face to face in an oral culture tradition. Information cannot be passed on a long distances and therefore it remains within a boundary of a particular community.

Recent improvements in information technology, like the internet and electronic mail has made it possible for individual to exchange sensitive information across the globe with security. Internet, as a global interconnection of computers and computer networks, over the years is increasingly becoming an ubiquitous means for exchange of information (Adesanya, 2004; Ogbomo and Ogbomo, 2008), providing reliable and effective platform for communication, including conducting business remotely (Woherem, 2000; Ogbomo and Ogbomo, 2008). For instance, information, in the form of text messages, computer files, to mention but two, can be exchanged via electronic mail, also known as email (Nwosu, 2004; Ogbomo and Ogbomo, 2008).

However, in spite of all the benefits that these advances in IT offer for information exchange, there are attendant challenges. Messages on transit can be intercepted and accessed by an unauthorized agent. This phenomenon is known as loss of confidentiality. When the information is altered without necessary authorization, we say there is a loss of integrity. Information can also be made inaccessible to authorized users. This often occurs when the media used for the storage, processing or/and transiting the information is attacked.

The effect of disruption, loss, or damage to information and information systems are often invaluable to their proprietors. In many situations, the continuous survival of a business entity depends to a large extent on the security of its proprietary data and information. For example, in airline operations, a breach in the accuracy or security of data could lead to loss of lives.

2. STATEMENT OF PROBLEM

The underlying respective architecture of most IT systems, including the desktop computer and internet, does not guarantee security. Users with malicious intents have always found a way of exploiting one vulnerability or the other. An attack that affects the confidentiality of information often presents the platform for the integrity of such information to be compromised. Intercepted information on transit would make little or no sense to an interceptor if he is not able to decipher the content of the information. This explains why it is very necessary to ensure that even when an intruder or unauthorised user successfully obtains access to some information the confidentiality and integrity of the information remain uncompromised.

3. OBJECTIVE

The objective of this paper is to design and implement an application that encrypts and decrypts plain text files using R.S.A algorithm and utilizes digital signature technique to verify the integrity and authenticity of the message sent.

4. EXISTING SYSTEM

Designing an encryption/decryption system, amongst other things, requires decision on the basic functionality of the software, and the choice of cryptographic algorithm to be used. While the functionality supports the attractiveness of the system, the type of cryptographic algorithm actually determines how much security the system would actually provide. Hence, this forms the major component in the system design.

Currently, there are many available open-source and commercial encryption/decryption systems. Madji and Lin (2007) developed a system that employs binary rotation of bits with XOR logical operation. The application uses symmetric encryption key, which is generated using random number generation and combination. Another use of symmetric encryption key was by Abdelhalim, El-Mahallawy, Ayyad, and Elhennawy (2012). They designed and implemented a Modified Tiny Encryption Algorithm (MTEA) for use in RFID systems.

Symmetric cryptography, though faster for encrypting and decrypting compared to asymmetric cryptography, which explains why it is mostly used for applications that involves transfer of large data, it provides less security and is more prone to attacks (Henry, n.d.). Therefore, for any application where security is of the most essence, the need for asymmetric (public key) cryptography is inevitable. The RSA scheme, among available public key schemes, has proven to be the most widely accepted, hence most implemented (Stallings, 2011).

5. SYSTEM DESIGN

5.1 Functional/Operational Requirements

This requirement outlines the functional/operational capability that the system can be able to provide and reaction to a particular problem. The data encryption and decryption system has the following functional requirements:

i. The system shall be able to identify documents with .txt extension, for encryption.
ii. The system shall be able to generate public and private keys to be used by registered users for both encryption and decryption.
iii. The system shall be able to encrypt and decrypt text files stored in the computer system.
iv. The system shall be able to save the encrypted plain text as .txt files.

5.2 Security Requirements

The security requirement entails the capacity to control user access, manage data and also support the three security concept (e.g. confidentiality, integrity and availability of data). The security requirements of the new data encryption and decryption systems are listed below:

i. The system shall be able to authenticate users.
ii. The system must be able to deny access to illegitimate users to the system.
iii. The system shall be able to verify the sender of a message through authenticating the user's digital Signature.
iv. The system must be able to retrieve the forgotten keys by asking some security questions in order to verify user's authenticity. This is achieved via email matching and secret questions supplied by the user during registration.

5.3 Architectural Design

The system is divided into two sessions, the use application and admin session. The major components design of admin sessions includes register new user, view user information, delete user, and configure server/ client system. The registered user session includes encryption of plain text and decryption of cipher text. Figure 1 below show the architecture overview of our proposed system.

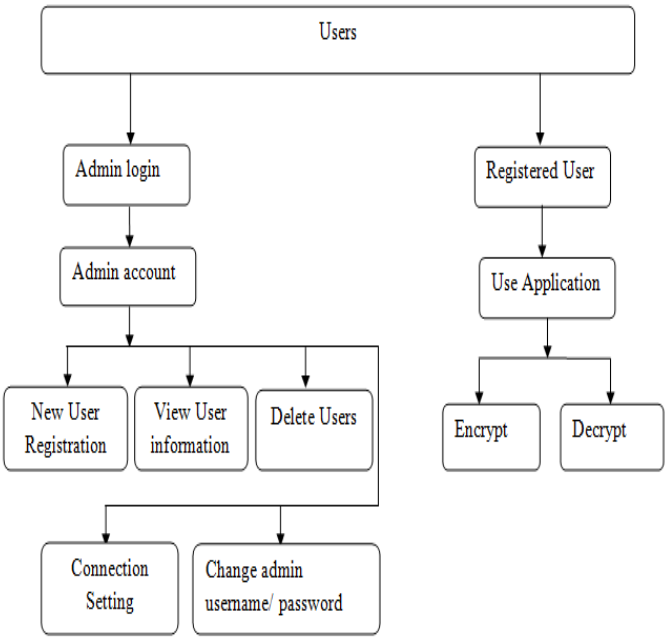

Figure 1. Architectural overview of proposed system

5.4 System Flowchart

Figure 2 depicts the system flowchart of the encryption and decryption system. The flowchart presents pictorially information about the system processes, and how they are interconnected.

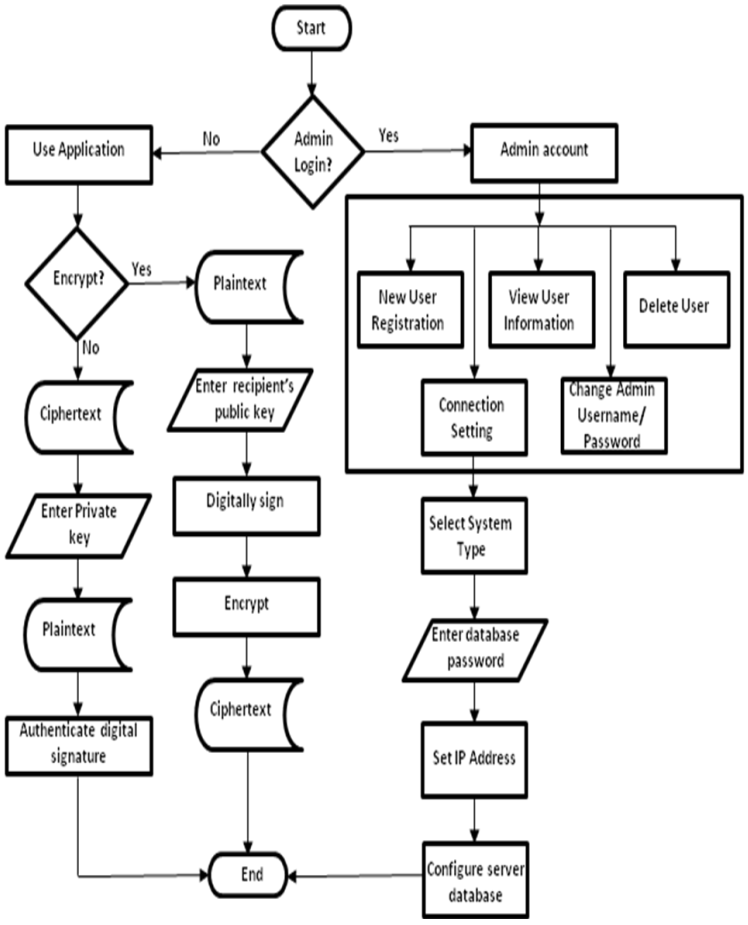

Figure 2. System Flowchart

6. SYSTEM IMPLEMENTATION AND TESTING

In the implementation of the encryption and decryption system, Java was used for the front-end programming, while MySQL was utilized for database management.

6.1 System Testing

Figure 3 below displays options for login into admin account or the use application. Only the administrator can have access to admin login while only registered users can use the application.

Figure 3. Login interface

Upon successful logging in by the administrator, the Admin account interface, represented by Figure 4, is displayed. Available options include New User Registration (figure 5), which when clicked display new user registration form where a new user can be created; View User Information, which displays user information based on the user public key; Delete User, which, as the name implies, provides the option for the admin to delete any user from the database using the user public key; Connection Setting, which allows for server of client system configuration; and lastly, the Change Admin Password/Username, which when clicked displays an interface through which admin can change user name and password.

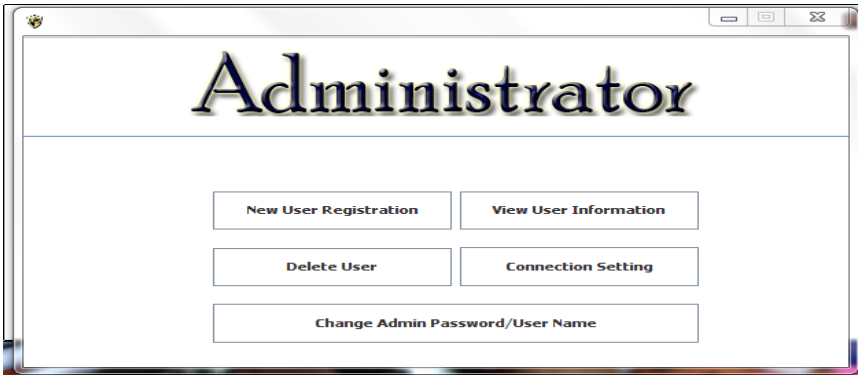

Figure 4. Admin account interface

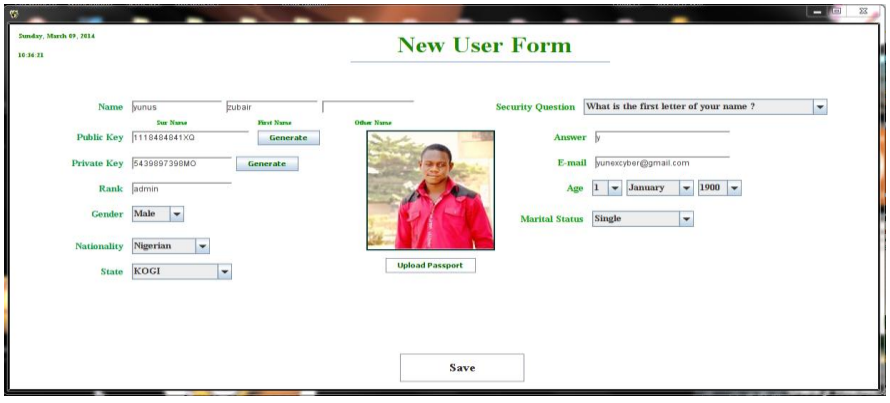

Figure 5. New User Registration interface

To create a new user, in addition to personal information, unique public and private keys are generated.

The administration has the privilege of viewing all the systems connected to the server using the encryption/decryption system. Information accessible includes the device name, system type, and IP address of the system which is either client or server, system status which is either connected or disconnected. Through the same interface (figure 6), the administrator can disconnect certain or all clients connected to the server, and reconnect them, as the case may be.

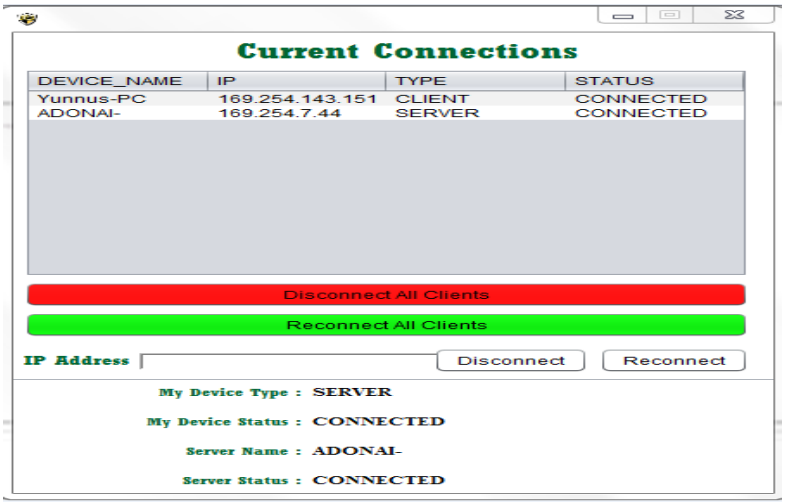

Figure 6. Current Connection interface on server system

For a user to encrypt a plaintext, the plaintext is located, the content of which is then displayed on the text area of the interface. The sender then supplies his or her public key, that of the recipient, digitally sign the message, and then encrypt it. The plaintext is automatically converted to a ciphertext. The corresponding ciphertext can saved and then sent over the network. The encryption/decryption interface, represented by figure 7, also contains menus that provide the mechanism for retrieving forgotten private key and outrightly changing the private key.

For decryption, the recipient locates the ciphertext. The application displays the ciphertext on the text area of the interface. The recipient then enters the private key on the decryption panel and then clicks the decrypt button. If the private key entered by the user matches with the private key of the intended receiver of the message, the application converts the ciphertext to plaintext, otherwise an error message is displayed and the message will not be decrypted.

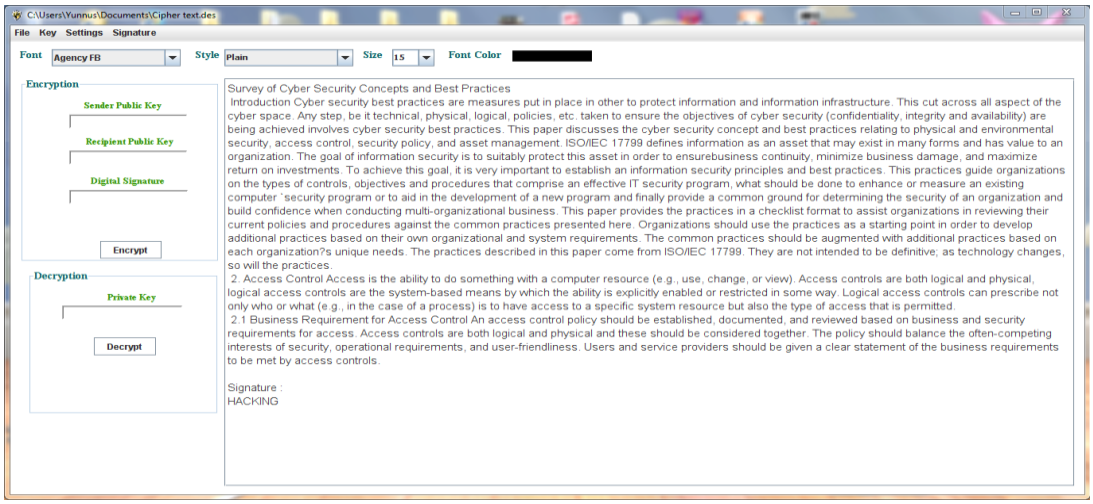

Figure 7. Encryption/decryption interface

The interface below (figure 8) allows the recipient to verify the authenticity of the message, by ascertaining its sender. This ensures non-repudiation of the message by the sender.

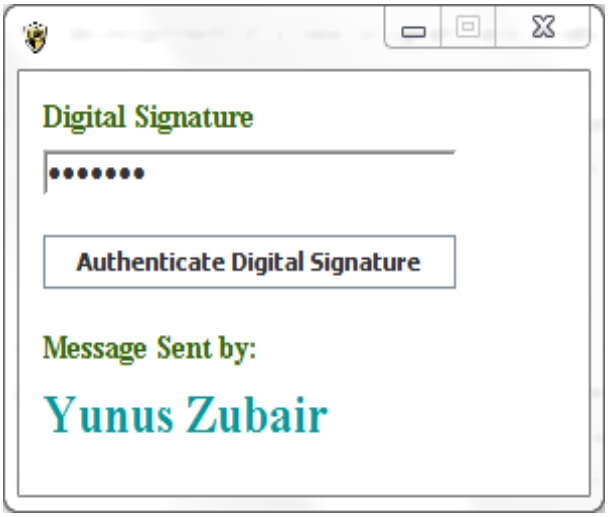

Figure 8. Authenticate digital signature interface

7. CONCLUSION

Data encryption and decryption systems are used to improve information security to secure data that, thereby providing enhanced level of assurance such that the data that are encrypted cannot be viewed by unauthorized parties in the event of theft, loss or interception. This system replaces the existing data encryption and decryption system by adding some functionality such as digital signature. Future works could be devoted to scaling the system to be able to encrypt and decrypt other types of files, including audio, video, image, to mention but three.

REFERENCES

1. Abdelhalim, M. B., El-Mahallawy, M., Ayyad, M. and Elhennawy, A. (2012). Design & Implementation of an Encryption Algorithm for use in RFID System. *International Journal of RFID Security and Cryptography (IJRFIDSC)*, Vol. 1, Issues 1-4, pp. 51 – 57.
2. Adesanya, O. (2002). The impact of information technology on information dissemination. In Madu, E.C. and Dirisu, M.B. (Eds.), *Information science and technology for library schools in Africa* (pp.10-24). Ibadan, Nigeria: Evi-Coleman.
3. Henry, D. (n.d.) *RSA: Asymmetric Cryptography and Algorithm Analysis for a Secure Computing Environment.* Retrieved from www.dwhenry.com/files/RSA.pdf
4. Introna, L. D. (1992). *Towards a Theory of Management Information.* Unpublished DCom Dissertation, University of Pretoria.
5. Madji, A. and Lin, Y. H. (2007). Simple Encryption/Decryption Application. *Internation Journal of Computer Science and Security*, Vol. 1, Issue (1), pp. 33 – 40.
6. Meyer, H. W. J. (2000). *The transfer of agricultural information to rural communities.* Unpublished doctoral dissertation, University of Pretoria, Pretoria, S. Africa.
7. Nwosu, I. (2004). Digital public relations: concept and practice, In Nwokocha, J. (Ed.). *Digital public relations: New techniques in reputation management* (pp. 33-34). Lagos, Nigeria: Zoom Lens Publishers.
8. Ogbomo, M. O. and Ogbomo, E. F. (2008). Importance of Information and Communication Technologies (ICTs) in Making a Heathy Information Society: A Case Study of Ethiope East Local Government Area of Delta State, Nigeria. *Library Philosophy and Practice 2008*, ISSN 1522-0222, pp 1 – 8.
9. Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice* (5th ed.). NY, US: Prentice Hall.
10. Woherem, E.R. (2000). *Information technology in the Nigerian banking industry*. Ibadan, Nigeria: Spectrum Books.

AUTHORS' BIOGRAPHY

Oluwafemi Osho is currently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He holds a B.Tech. degree in Mathematics/Computer Science and an M.Tech. degree in Mathematics. Before joining the institution, he served as Head of the IT Department of one of the leading mortgage banks in Nigeria. His research interests include information security, cloud security, mobile security, e-commerce security and software development.

Yunus O. Zubair has a B.Tech degree in Computer Science (Cyber Security) from the Federal University of Technology, Minna.

Lauretta Oluwafemi Osho is currently a Master degree student in the Department of Computer Science, Federal University of Technology, Minna. She holds a B.Tech. degree in Mathematics/Computer Science. Her research interests include cloud computing and software development.

Joseph A. Ojeniyi completed his B.Tech in Mathematics/Computer Science from Federal University of Technology, Minna in 2004, M.Sc. in Computer Science (Internet Security) from University of Ibadan in 2009 and Ph. D in Cyber Security Science at Federal University of Technology, Minna (in view). Before his first degree, he obtained Nigeria Certificate in Education from the Faculty of Education Technical of the Polytechnic Ibadan. He is presently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna. Some of his Research Interests Include: Web Security Standards, Computerization of Prison Records and Asymptotic Analysis of Digital Forensics Estimators.