IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 85-90
www.iosrjournals.org

Secure and Reliable Document Faxing through Wi-Fi using Cloud

Sneha Sharma, Gauri Wavhal, Manasveena Suguru, Karishma Tale
Information Technology JSPM's JSCOE Pune, India
Information Technology JSPM's JSCOE Pune, India
Information Technology JSPM's JSCOE Pune, India
Information Technology JSPM's JSCOE Pune, India

Abstract: *Secure and reliable document faxing through Wi-Fi using cloud is android based application where one can send documents through Wi-Fi within an organization. Organizations mostly use Gmail, Yahoo etc. for sending documents this can hamper the confidentiality. Hence, this application has proposed a new way of sending documents and messages which can be video audio and any file, where organization will have a private cloud which will maintain all user account. Since this is going to be implemented on INTRANET, an individual can only have access to these files within an organization. Faxing can be done in three ways: - Normal mode: where message is sent and received normally with simple encryption decryption. Semi secure mode: where message is sent from sender with a key, that key will be used to open message.(besides encryption decryption). Ultra secure mode: where message will be sent from sender with a key and another key will be sent to his phone by simple SMS so the receiver will need two keys to open the message. Highly confidential data can be sent through this mode.*

Keywords*: Wi-Fi; AES; SMS; Mode; Encryption; Decryption; Android*

I. Introduction

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. In organizations data exchange is most frequently done. Data here can be exchanged in many ways i.e. via shared network like LAN or by mailing etc. this may be the most simplest way of sharing data but it does not provide security for data since data is available in plain text format. Hence any confidentiality of the data cannot be maintained in this way.

Traditional way of sending printed documents in form of text or images is through Fax machine. Now days one can send documents in several different ways, most commonly used method is to send fax through telephone lines but now one send fax via e-mails, cell-phones, hand-held organizers, radio, satellite and cable. When data is sent through telephone line it is converted in electrical form and the data is not encrypted. Therefore, the main drawback of sending document through these methods is that the data is available in plain text format hence; the data can be accessed by the third party or unauthorised party. The solution to this problem we are providing in this application

This paper has proposed a new technique of sending documents through Wi-Fi using cloud on android phones. Cloud computing enables user to use applications without installation. This technology helps in bringing down the computation cost of organizations. Security in cloud is much better than scattered network and they are easy to manage. Cloud computing provides services in three models i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

Secure and reliable document faxing through Wi-Fi using cloud is android based application where one can send documents through Wi-Fi within an organization. This application's environment is characterized by a group of users who want to communicate with each other by exchanging data in the form if text, audio or video. The users will have android phones with Wi-Fi interfaces that can create ad-hoc network to send or receive data. When the network is operative they can execute the application. The main objective of Smart Document Faxing is to provide user an exertion free environment through which he can send his important documents within his organization with reduced efforts of providing security.

II. Literature Survey

Mobile phones have been a very efficient in sending and receiving data as they provide the ease of mobility. When confidential information is exchanged using Mobile Messaging, it is very difficult to protect the information from normal mobile message security threats like man-in-middle attack, DOS attack as well as ensure that the message is sent by authorized senders. Threats like eavesdropping, interception and modification are more likely to occur in mobile messaging [1]. Hence to provide security we need authentication, confidentiality, integrity [1]. Authentication checks the identity of sender and receiver to ensure that both the

communicating parties are valid or not. Confidentiality ensures that only the authorized person gets access to the data it prevents disclosure of information to unauthorized user in any manner. Confidentiality maintains privacy. Integrity ensures accuracy and consistency of the data throughout its life time. Data should not be modified by any unauthorized person.

To provide confidentiality to the data which is to be sent, it should be sent in encrypted format instead of sending it in plain text format [1] [2]. Encryption can be done using symmetric or asymmetric encryption algorithms. AES is a symmetric encryption algorithm which demands less computing power [3]. AES requires low RAM space for computing and it's very fast. It has been used for SMS encryption on Android phones [4].But the limitation of SMS is that it only allows limited amount of data to transmit.

This project describes a solution that provides mobile messaging security that guarantees provision of confidentiality, authentication, and integrity service.

III. Proposed Theme

Proposing the theme to send secure and reliable documents Via Wi-Fi using cloud for handheld devices OR altogether proposing idea of sending documents, insulating them from different types of attacks like DOS attack, man-in-middle attack etc to some extent. We are developing an Android App (which is supported by Android Mobile Phones) to send documents (can consist of text, audio, video or images)

The basic objective of this application is to provide security and user friendly way to send and receive confidential data through Wi-Fi using cloud. [6] Wi-Fi allows Android devices with the appropriate hardware to connect directly to each other via Wi-Fi without an intermediate access point. The Wi-Fi provides the ease of mobility and wireless communication .Since Wi-Fi is available on variety of devices such as mobile, laptop, tablets hence it is convenient for the user to connect to the internet or to share the data using Wi-Fi.

A. Basic concept

The basic concept is illustrated in Fig. 1. This application is based on client server architecture, where clients are group android phone users and server is a cloud server. Clients will send and receive documents through Wi-Fi.

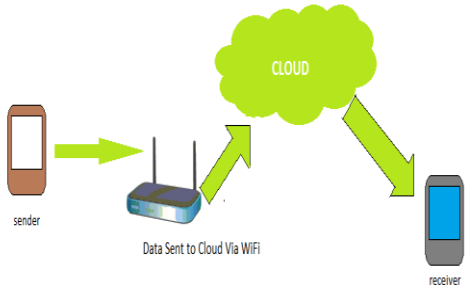

Fig. 1. Document faxing Basic concept

The documents sent will be stored at the cloud server. Documents can be sent in any of the three modes**:** **Normal mode**: where message is sent and received normally with simple plaintext format **Semi secure mode**: where message is sent will be in encrypted format **Ultra secure mode**: where the message will be encrypted twice which is explained further in detail. Highly confidential data can be sent through this mode.

B. Authentication

User will login with his login id and password. The hash of the password and logon id will be compared with the one present at the server , if it matches user will get successful login and he will be allowed to do operations like send document, read decrypted message, change password etc.

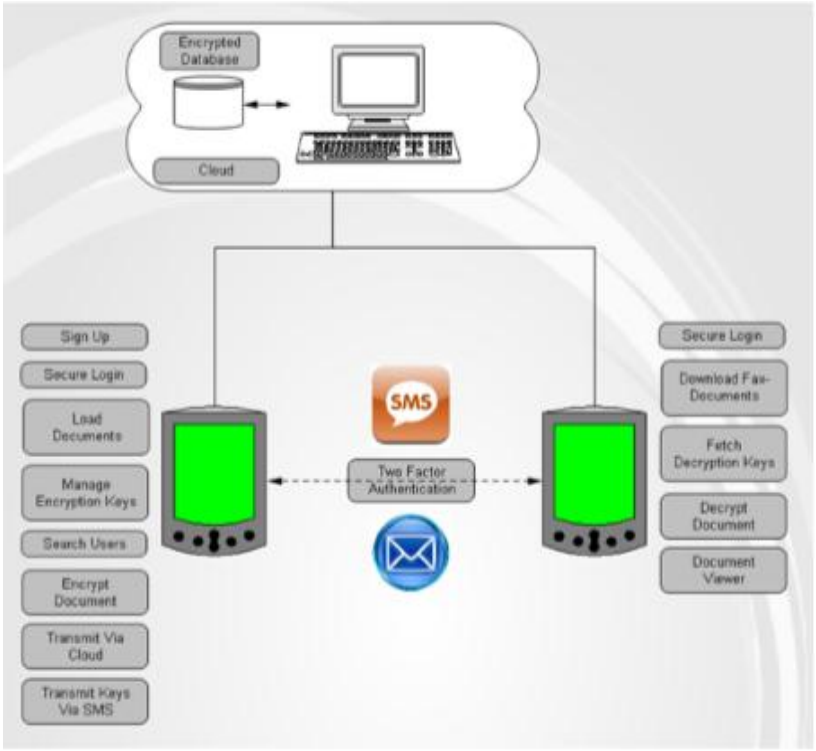

Fig. 2. Basic Architecture

C. ***Sending Document***

This app will provide user to send documents via three modes. These three modes are normal mode, semi-secure mode and ultra secure mode.

1) Normal Mode: In normal mode user uploads documents first and then sends the document. Normal mode will not provide any security since documents are sent in plain text format. Hence documents which do not need any confidentiality can be sent through normal mode.

2) Semi-secure Mode: In semi-secure mode the document uploaded gets encrypted using AES algorithm, this encrypted document is sent to the sender. Encrypted document is saved at server side.

*3) Ultra-secure Mode****:*** In ultra-secure mode the document uploaded gets encrypted twice. First time when the document is attached while sending the message and it is again encrypted using sender's key which is sent through SMS on receiver's mobile phone. The basic architecture is illustrated in Fig. 2

The data sent through this application is divided into chunks; hence data is transmitted in chunks this enables the user to send any amount of data irrespective of its size. The document sent is stored in encrypted format at the cloud server so security is well maintained at the server end also.

D. ***Receiving Document***

At the receiver end, the documents received can be viewed in the following ways based on which mode it is sent i.e. normal mode, semi-secure mode or ultra-secure mode.

1) *Normal Mode*: If the document was sent in normal mode, the receiver can directly view the document by simply downloading it.

2) Semi-secure Mode: if the document was sent in Semi-secure Mode, the receiver will download the document .Before viewing the document; it will directly get decrypted at the receiver end.

3) *Ultra-secure Mode:* if the document was sent in Ultra-secure Mode, the receiver will receive an SMS in his mobile phone. This SMS will contain a key which will be used for decrypting the document. First the user will download the document, while viewing the document it will ask for a password, the key received through SMS should be entered here.

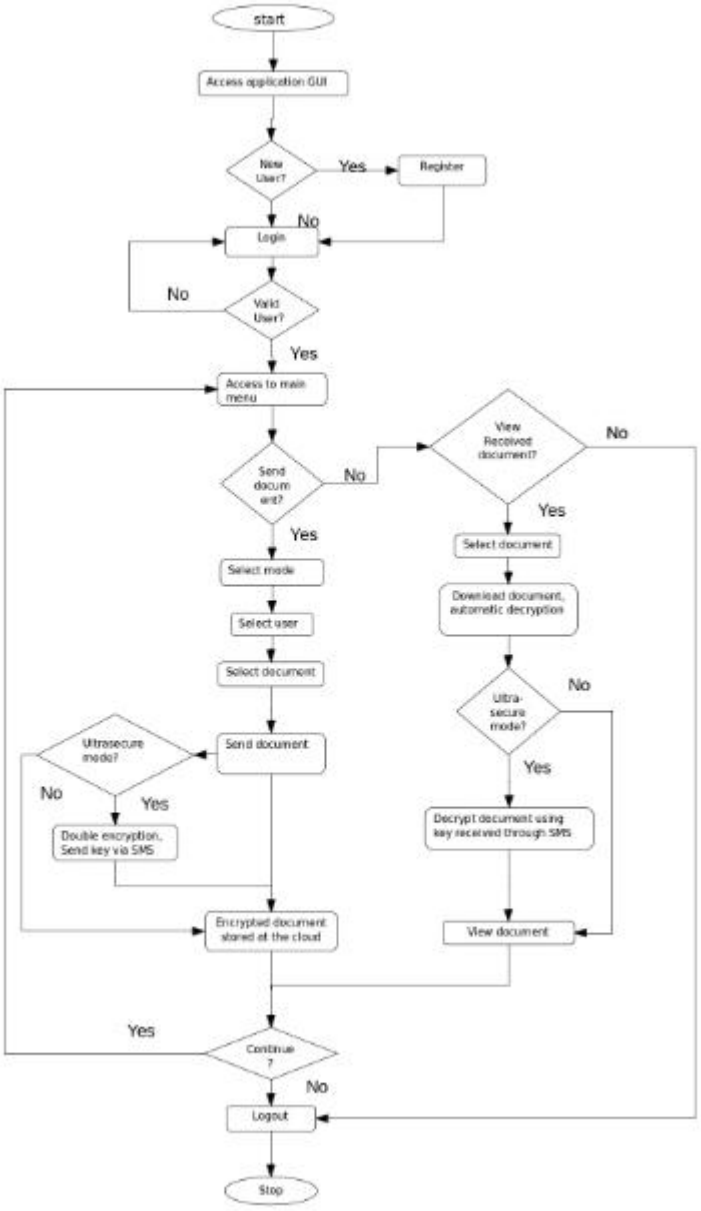

Fig. 3. Flow chart

If the key matches, the document gets decrypted and is available to receiver in plain text format.

E. Working of the application

Fig.3. shows the complete flow of Secure and Reliable Document Faxing through Wi-Fi using Cloud. First the user needs to install the App in his android cell. Once he is done with the installation he needs to register himself by providing the necessary information. After registration, the user can login and can access the services. While sending the document the user will upload the document, after attaching the document the user will select one of the three modes i.e. Normal mode, Semi Secure mode or Ultra secure mode described in earlier section. If the user is selecting ultra secure mode he need to send the encryption key (i.e. password) to the receiver through SMS.

On the receiver's side the user will first download the required document he wants to see. After decryption the document will be available to the user in plain text format.

IV. Advance Encryption Standards Algorithm/ Rijndael Algorithm

The algorithm used in this application for encrypting and decrypting the document on server is Advance encryption standard (AES). It is used for securing sensitive but unclassified material by U.S Government; this is a standard algorithm that has been adopted worldwide as cracking the cipher text generated by this is very difficult to crack. AES is a symmetric block cipher. Block size is of 128 bits and key length can

be of 128 bits, 192 bits or 256 bits called AES-128, AES-192 and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. Except for the last round in each case all other rounds are identical.

AES is based on permutation-substitution network and it works fast in both software and hardware. AES operates on a 4 X 4 matrix of bytes, termed the state, arranged as follows:

Fig. 4. State Array

Each column of the state array is a word, as is each row. A word consists of 4 bytes. State array is given as a input to each round that produces state array as a output. The output state array produced by the last round is rearranged into a 128-bit output block.

A. Overall structure of AES

The overall structure of AES encryption/decryption is show in Fig. 4. For encryption, each round consists of the following four steps:

1) Substitute bytes
2) Shift rows
3) Mix columns
4) Add round key.

In last step the output of the previous three steps is XORed with four words from the key schedule.

For decryption, each round consists of the following four steps: 1)Inverse shift rows,2)Inverse substitute bytes,3)Add round key, and 4)Inverse mix columns. Output of the previous two steps is XORed with four words from the key schedule in third step.

The last round for encryption does not involve the "Mix columns" step. The last round for decryption does not involve the "Inverse mix columns" step.

Fig. 6 shows the different steps that are carried out in each round except the last one.

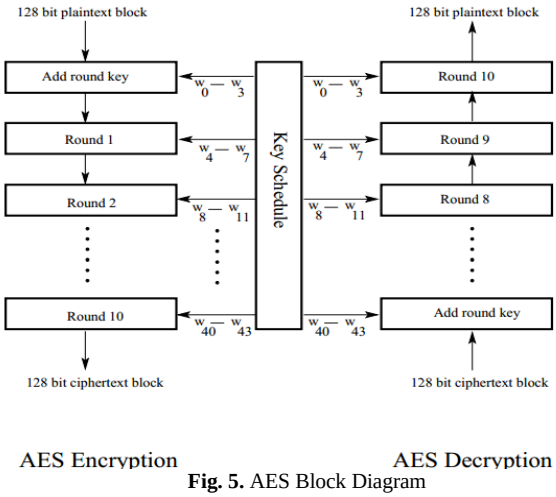

Fig. 5. AES Block Diagram

STEP 1: (called **SubBytes** byte-by-byte substitution during the forward process)(The corresponding substitution step used during decryption is called InvSubBytes.)

- This step consists of using a 16X16 lookup table to find a replacement byte for a given byte in the input state array.
- These entries in lookup table are created by using the notions of multiplicative inverses in GF(2^8) and bit scrambling to destroy the bit-level correlations inside each byte.

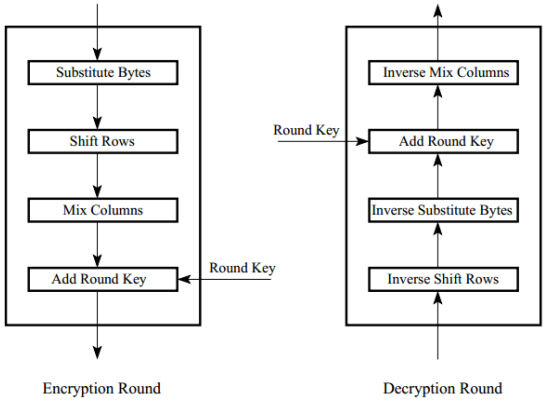

Fig. 6. Steps in AES

STEP 2: (Called ShiftRows for shifting the rows of the state array during the forward process) (The corresponding transformation during decryption is denoted InvShiftRows for Inverse shift-Row Transformation.)

The goal of this step is to scramble the byte order inside each 128-bit block.

STEP 3: (called MixColumns for mixing up of bytes in each column separately during the forward process) (The corresponding transformation during decryption is denoted InvMixColumns and stands for inverse mix column transformation.)

- The goal of this transformation is to further scramble up the 128-bit input block.
- The shift-rows step along with the mix-column step causes each bit of the ciphertext to depend on every bit of the plain-text after 10 rounds of processing.

STEP 4: (called AddRoundKey for adding the round key to the output of the previous step during the forward process) (The cor- responding step during decryption is denoted InvAddRound- Key for inverse add round key transformation.)

V. Conclusion

Secure and reliable document faxing provides security as the documents are stored in encrypted format at the server side. This application is reliable as it implements cloud computing as well as it does not have any size limitations for sending or receiving documents.

Acknowledgment

We take this opportunity to thank our project guide Prof. S.V.Todkari for his valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

References

[1] Prof. Rashmi Chavan and Prof.Manoj Sabnees ”Secured Mobile Messaging”,”2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]”.
[2] David Lisonek ”SMS Encryption for Mobile Communication”,”2008 International Conference on Se curity Technology”
[3] Rohan Rayarikar, Sanket Upadhyay and Priyanka Pimpale ”SMS encryption using AES Algorithm on Android”, ”2012 International Journal of Computer Application”
[4] Mary Agoyi and Devrim Seral ”SMS security: AN Asymmetric Encryption approach”, ”2010 sixth international conference on wireless and mobile communication”
[5] Ario Yudo Husodo and Rinaldi Munir “Arithmetic coding modification to compress SMS”, “2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia”
[6] Webpage: www.android.developer.com
[7] Webpage: http://www.guide2faxmachines.com/why-use-fax/how-fax-works
[8] G. Racherla, D. Saha, “Security and Privacy Issues in Wireless and Mobile Computing”, Proceedings of 2000 IEEE International Conference on Personal Wireless Communications, Dec 17-20, 2000.
[9] Advanced Encryption Standard, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[10] Priyanka Pimpale, Rohan Rayarikar and Sanket Upadhyay, “Modifications to AES Algorithm for Complex Encryption”, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.
[11] S. Zhao, A. Aggarwal and S. Liu, “Building secure user-to- user messaging in mobile telecommunication networks”, Proceedings of Wireless Telecommunications Symposium, Pomona, CA, 2008.
[12] N. Amani, “Using SMS as a business communication Tools for SMES”, 6th Regional Innovation System and Innovation Clusters in Africa, Tanzania, 2009.
[13] S.M. Siddique, and M. Amir, “GSM Security Issues and Challenges,” 7th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'06), pp.413- 418, June 2006.