Secure Communication with DNS through Cloud

Akash Bajaj, Srujana, Vibha.V, Sinchana P.Shetty
Computer Science And Engineering
The National Institute Of Engineering
Mysore-570008
Under the Guidance of
Mohanesh B.M.
Assistant Professor
Computer Science And Engineering
The National Institute Of Engineering
Mysore-570008

Abstract: Internet in today's world has become one of the most prominent ways to communicate through text, voice, pictures, video and many more ways. Millions of MB of data is exchanged over internet in a single day all over the world. And lots of those data is sensitive and private. Thus internet provides as point to intrude in someone's private life or intercept some sensitive data. With the increasing use of Smartphone, a big amount of data is being stored and exchange through the application running on its operating system.

This have only increased the data exchange over the network. That's why the importance of security over the exchange as well as storage of data has increased dramatically over the past few years. For providing security many different methods or ways are taken. Over those methods use of cryptography is one of the widely used methods.

Our application is designed to provide secure transmission of data like text or image over the network with the help of cryptographic algorithm. This application can be easily run on the android operating Smartphone as well as the computer with other operating system. Through this application the user can also encrypt the file or image and store it in the system memory as well as over the cloud and retrieve it whenever needed.

*****

I. CRYPTOGRAPHY

Cryptography is the study of information hiding and verification. The term cryptography is derived from the Greek words "Kryptos" which means "hidden" and "graphein" which means "to write" or can be said the art of "hidden writing". The use of cryptography can date back to thousands of years of history. Communication between kings was done by different cryptographic methods.

Cryptography emphases have evolved from linguistic to other, with extensive use of technical areas of mathematics, especially those areas collectively known as discrete mathematics.

When information is transformed from useful form of understanding to non-useful (opaque) way of understanding, it is called encryption and inverting this data back to useful message is called decryption. The person who has the knowledge of certain secret piece can only decrypt the message. This ensures the authorized use of message. The secret piece/knowledge is called key. Hence we can say cryptographic methods are used for secured communication.

II. RSA ALGORITHM

RSA is one of the first practicable public key cryptosystems and is widely used for secure data transmission. RSA stands for RON RIVEST, ADI SHAMIR and LEONARD ADLEMAN who first publicly described the algorithm in 1977. The complexity of large integer operation is the main factor that affects the efficiency of RSA system. RSA algorithm can be used for data encryption of digital signature, this advantages make it most widely used public-key algorithm. In order to guarantee the security in RSA Algorithm, the length of keys used for both public and private keys are usually kept greater than 1024 bits.

Consider two exponents, e and d where e is public and d is private and p being plaintext and c being ciphertext. Let us consider the case where Alice has to send some message to Bob by RSA algorithm, Alice uses public key to convert its plaintext to ciphertext i.e. $c=p^e \bmod n$. Likewise Bob uses his private key to invert back the ciphertext to plaintext i.e. $p=c^d \bmod n$. Let the selected prime numbers p, q be very large primes where $p\neq q$, $n=p\times q$, $\phi(n)=(p-1)(q-1)$ where e must be $1<e<\phi(n)$, $d=\overset{r}{e} \bmod \phi(n)$ as shown in fig 4.

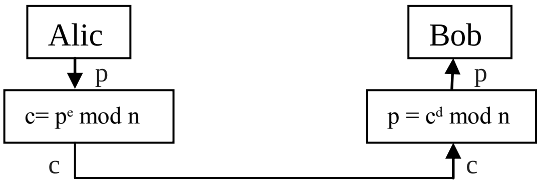


Fig 4. Encryption Using RSA algorithm

RSA uses two algebraic structures in the various phase of algorithm.

The first structure used is encryption/decryption ring. By using commutative ring **R**= <, +,> with two arithmetic operation for encryption and decryption. RSA make this ring public because the modulus n is public. Anyone can send data to another person if he knows the ring of the receiver.

The second structure is used during the key generation phase. The second structure is group **G=<**Z, supports only multiplication and division (inverse multiplication) which are needed for generation of public and private key. In RSA, the group is hidden from public because its modulus, ϕ(n), is hidden from public.

There are various attacks which can be performed on RSA, namely factorization, chosen ciphertext, encryption exponent, decryption exponent, plaintext, modulus and implementation. Although none of them are devastating on RSA.

The security of RSA algorithm depends on the fact that for a very large number *n*, we have no efficient method to divide it until now. So the private key *e* cannot be calculated out from *n* and *d*. Similarly, *d* also cannot be calculated from *n* and *e*. The attack difficulty equivalence to the division of the product of two large prime numbers, therefore the RSA algorithm has high security.

III. ANDROID

Android is a mobile operating system (OS) based on the Linux kernel and currently developed by Google. With a user interface based on direct manipulation, Android is designed primarily for touch screen mobile devices such as Smartphone and tablet computers, with specialized user interfaces. The OS uses touch inputs that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard. Despite being primarily designed for touch screen input, it has also been used in game consoles, digital cameras, regular PCs, and other electronics. As of 2015, Android has the largest installed base of all operating systems of any kind.

Android have gained popularity in Technology Company which requires a ready-made, customizable operating system which is also low-cost for their high-tech devices. Due to its open nature android has also become popular between a large community of enthusiasts and developers to use the open-source for developing its advanced features or to use it as a foundation for their community-driven projects.

Android has a large selection of third-party application, which a user can acquire by downloading and installing the application's APK (Android application package) file or user can also download them using an application store program that allows them to install, update and remove application from their devices. Google Play Store is the primary application store installed on Android devices. Google Play Store allows users to browse, download and update applications published by Google and third-party developers

IV. CLOUD STORAGE

Cloud storage is a model of data storage where the digital data is stored in logical pools. The physical storage spans multiple servers (and often locations) and the physical environment is typically owned and managed by a hosting company.

Cloud storage services may be accessed through a co-located cloud computer service. A web service Application Programming Interface (API) or by application that utilize the API, such as cloud desktop storage, a cloud storage gateway or web- based content management systems.

Our application stores the customer information in the cloud storage along with the data exchange by the different user. All the data stored in cloud is in encrypted form to provide the privacy to user and also to provide security against data theft.

V. PROPOSED SYSTEM AND ITS OPERATIONS

The proposed application will be developed for computer using java since it is platform independent and robust in nature. The application will also be available for Android user in the form of third-party application i.e. APK file. The APK file will be developed with the help of java and java swing.

5.1 Client Side Operation

The main goal of the application is the securing of the data. So the client side operation is based on providing security to data being sent to recipient or being stored in the system memory (locally) or stored in the cloud (globally). The main operation is listed below:-

➢ Client/User must register himself by specifying his valid email id because universal key will be sent to his email id which can be made use in future for changing his/her account details .

➢ The user can select the cryptographic algorithm for the message along with different key length. The selected algorithm will encrypt the sending message.

➢ The user can send message to another user. The message will be encrypted by the public key of the recipient.

➢ The user can also attach document with the message. The attachment will be separately encrypted and sent.

➢ The user can encrypt a text file or a image with the help of application and store it locally or in the cloud, as per their convenience. The encrypted file can be accessed through the application after decrypting it.

All these primary function will also be available on android client side.

5.2 Server Side Operation

The server will be monitoring and storing the data in the cloud. The server will store the information about the user and the user system i.e. MAC id and for android it will be device id. The server will not allow the two user to register from same device or system to provide an extra security. In the case of device lost, the user can use their universal key which will be given to them at the time of registration to register a new device to their old account.

Server will validate the identification of the client with the help of device id and email id. This application don't allow two email id to get register from the same device id. so as to secure the data of primary user of that device. using this function will also help us in implementing security measure in the time of device theft. for example every customer will be provided a universal key at the time of registration and if they lose their primary registered device then they can register a new device for the old account and can access all they inbox and sentbox and old device id will be removed , this way security of data will be ensured after the device lost or theft.

5.3 Hardware Requirements

- ➢ **Processor** : Pentium IV or above.
- ➢ **RAM**: 512 MB RAM or more.
- ➢ **Hard Disk Space:** Minimum of 1 GB.

5.4 Software Requirements

- ➢ Operating System : Windows XP or above.
- ➢ Language : Java and J2EE
- ➢ Java Software: JDK 1.6 or above.

  : Eclipse , Android studio

VI. FEASIBILITY STUDY

The main aim of this phase is to determine whether it would be financially and technically feasible to develop the product.

The feasibility assessment has to be addressed in three levels, such as:

- Economic feasibility
- Technical feasibility
- Operational feasibility
- Social feasibility

6.1 Economic Feasibility

The developing of the application requires a android SDK and a java platform to develop the program. The android SDK is freely available on the internet as well as we can download the Java platform from the internet without any cost. As lots of people want to secure their personal data from theft, this application will provide them a way to secure their sensitive data, so the application have fairly good market success probability

6.2 Technical feasibility

The developing of the system requires the knowledge of java and java swings. The reason behind choosing java as source code language is because java is platform independent language and its easier to learn and implement application in java. Java swings is used the implement the interface of the android application.

6.3 Operational Feasibility

After testing the various aspects of this application package, it has been found that the system is operationally feasible to a project is being supported by the management as well the users. The system will also produce every report needed by the management. No data is viewed by any outside resource or users who are not privileged to do so hence it is operationally feasible to do so with full security.

6.4 Social feasibility

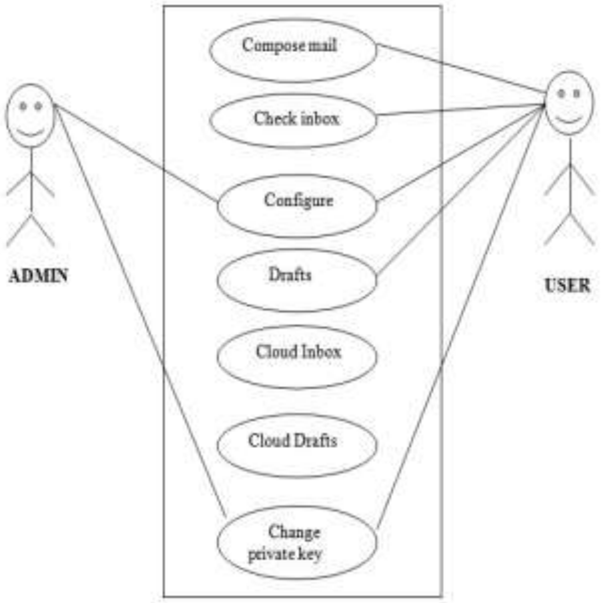
The proposed application would be of universal acceptance because of its easy accessibility and the function to secure their most sensitive data like text and image.

VII. SYSTEM DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

The system has been to designed to make the user experience better and also to meet the main aim of the application that is to provide the security to the data of user stored or being transmitted.

7.1 Use case diagram



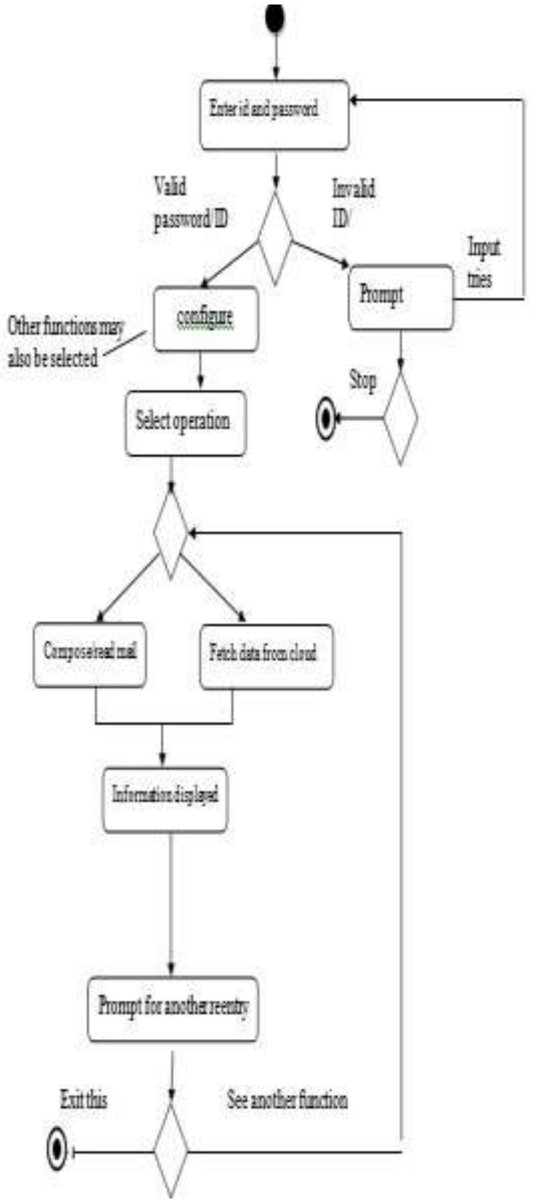
Here admin is nothing but the server who is having the authority to

- Change private key and
- Configure user account details.

But the user has been given a chance to

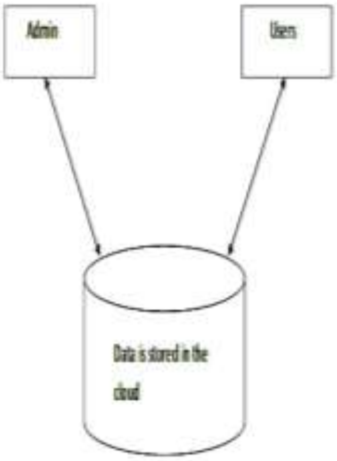
- Compose a mail.
- Check his inbox.
- Configure his/her account details.
- Access his/her drafts.
- Change his/her private key.

7.2 Activity Diagram



- User must enter user id and password for logging in, here maximum of three trials are given in a single session for correct login if not achieved application will be closed abruptly.
- Once successful login is done home page is displayed with many options such as compose mail, drafts, algorithm change ,key generator and help.
- If mail composing is chosen then a separate tab will be created for mail composition and allows the user to attach files.
- Once mail is composed user has to specify private key of receiver and send it.
- Once mail sent user will be allowed to access his/her home page options.
- And hence the process continues till he /she feels that complete work has been done by logging out from them application.

7.3 Data Centered Architecture



- Here we make use of data centered architecture I.e., cloud for storing our secured data in encrypted format.
- Hence Client and server can interact with each other in an efficient and secured way.

VIII. CONCLUSION

Here the main focus of data security is being successfully achieved with the help of secured cryptographic techniques such as RSA, Message digest. And our second focus of secured data transmission is also achieved with the help of this technique.

The application have fairly good success market probability and can be able to provide a security for the data to be stored locally (on device) or globally (cloud) due to its function to encrypt and then store data.

REFERENCES

[1] Milan Markovic, Goran Dordevic, On implementation Aspects of Standard Asymmetric and Symmetric Cryptographic Algorithms on T1 Signal processors.

[2] F.Ayoub, K.Singh, Cryptographic techniques and network security.

[3] Mohammad Zakir Hossain Sarkar, Md Shafir Parvlz,a cost efficient symmetric key cryptographic algorithm for small amount of data.

[4] Sean O'Melia, Adam J. Elbirt, Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions.

[5] HoWon Kim, Sunggu Lee, Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System.

[6] Ying-Yu Cao,Chong Fu,An efficient implementation of RSA digital Signature Algorithm.

[7] Min-Shiang Hwang, Eric Jui-Lin Lu and Iuon-Chang Lin, A Practical (t, n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem.

[8] FIPS PUB 197: Advanced Encryption Standard (AES).

[9] ISO/IEC 18033-3: Information technology — Security techniques.

[10] 2008 International Conference on Intelligent Computation technology and Automation.