International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 122 – 125

Securing Data using Hybrid Encryption Technique for Android Devices

Ms. Manju Ahuja
Computer science & Engineering
Nuva College Of Engineering & Technology Nagpur.
manju.ahuja@yahoo.com

Prof.Vishwajeet Bajpayee
Electronics & Communication
Manoharbhai Patel Institute of Engg. & Technology, Gondia ,
bajpayee07@gmail.com

Prof.Shyam Dube
Computer science & Engineering,
Nuva College of Engineering & Technology, Nagpur
Shyam.nuva@gmail.com

***Abstract*—** Security means to secure or to protect the valuable information from the unauthorized person from having access. Cryptography is very important in securing data in terms of integrity and confidentiality. Like desktop computers, mobile devices (e.g., smart phones, tablets, laptops, and notebook computers) are also used to store sensitive information. The data may be text, audio, video, image etc. The android devices can be stolen by the fraud or there is always a possibility of data access without owner's permission. In this case, the protection is required for the data stored in devices. To protect such type of data cryptography only is not the one solution. Symmetric encryption is used when we are dealing with the outsized quantity of information to encrypt. On the other hand Asymmetric encryption is complex than symmetric encryption and not appropriate for huge information to encrypt and does not offer more access. So the data is encrypted using the advantages of both symmetric and asymmetric encryption.

***Keywords*—** *Cryptography, Encryption, Mobile Device Security, Data Security, Image Encryption.*

*****

I. INTRODUCTION

Security is to secure or hide the important data from unwanted operations of unauthorized user. To provide security Cryptography is more important. Cryptography is a technique to safe the data by converting the data into illegible type so that the unauthorized users cannot access it. There are so many cryptographic algorithms are available to secure data. The main terms used in the cryptography are Encryption and Decryption. Encryption means to transform the data into unreadable form and Decryption means to get back that data into its original form.

Now a day, as compared to desktop computer, mobile devices (Smartphone, Tablets) are more used by peoples. As we can carry mobile phones easily anywhere we want. The android devices are nothing but the small wireless computer in our hand. We can capture anything in anywhere. The demand of mobile devices is increasing day by day rapidly. The peoples are now more depending on their cell phones or mobile devices. Mobile devices can be use any time anywhere in the world. Any time we can access internet, video recording, capturing photographs etc.

We can also store the important data into our mobile devices. Important data means some organizational data, company's most important documents or some secret videos captured by devices. But we want to store all these information in encrypted form and also want that these information only decrypted by owner. There is always a risk about stolen of devices. We want to provide strong security to data.

Protection to channel of communication is not sufficient, endpoints of that channel are also is now a major security challenges. For this type of security we are also used cryptography because cryptography is the only one which defends against attacks. Information of any organization is very sensitive because the third party is always in a way to attack on the device and want to get all the information by breaking the security chain. Attacker always follows any potential method to get that information either by using any decryption method or by stolen device. Cryptography is provided to secure the information so that the third party never get the data or he is enable to decrypt that data which is encrypted.

Many cases are there in which the devices are stolen by the unauthorized party and misused the sensitive information stored in the device. To protect the sensitive information held by the device from the attack, it is require that we only store the information which is used and delete those information which is no longer in use. We store the useful information in the device in encrypted form so that attacker never gets the data from the device. If we are talk about mobile devices which are now plays an important role in our life and we move anywhere to it and always keeping it with you. We are storing the information in our device so that in future if we need that data so we can easily access to it and if needed we can also modify it. Some devices are only used for the storage and transfer it to another device for processing. we are using mobile device and we only stores information into it and not perform any changes. These devices do not need processing

the data that is stored in that, but should store the data in secure manner

Cryptography involves encryption and decryption. As we have two types of encryption symmetric and asymmetric. Both have some advantages and disadvantages. Symmetric encryption is used to encrypt large amount of data. If symmetric encryption is used to encrypt the data on device, so its decryption is needed to perform on the same device. It can be happen that the unauthorized party gets the access to the keys by which we encrypt the data and access the data easily. For this purpose we can use asymmetric encryption. If the keys are accessed by the attacker the data is accessed by the attacker and he/she can manipulate the data and we cants do anything to protect by manipulation.

The purpose of this paper is to provide the high degree of security to the device so that the attacker never gets the data in any way. The method we are applying is to securely providing encryption on one device but we can only decrypt it on another device. We are using for this the advantages of both type of encryption techniques i.e. Symmetric and Asymmetric encryption. We are encrypting the whole information or data using symmetric encryption technique. And the keys which are used to encrypt the data are securely encrypted by asymmetric encryption technique. As we are using both type of encryption we called it hybrid encryption (Symmetric and Asymmetric encryption).

II. Literature Survey

In the literature many models are proposed to secure the data of mobile devices. They provides data security but what will happen if the device itself is stolen. These models are used when mobile devices are only used to store data which can be may be public. But what happen when someone have their personal and important details or documents. The strong security is required.

The data security is provided by using two level data hiding technique. In the first level the data is encrypted and securely stored in special records. Second level is a password protection Scheme. As in this the key is generated by using location co-ordinates. Since the password changes according to the location but what if the device is placed for a long time in one location and the password is known to the unauthorized user. There is always a chance of losing mobile. And if the mobile is stolen by someone then the whole information is lost. Neither we can see it nor recover it [1].

The data is treated as a binary bitstream, self-encryption (SE) scheme generates a key stream by randomly extracting bits from the stream. The length of the key stream depends on the user's security requirements. The bit stream is encrypted and the ciphertext is stored on the mobile device, whereas the key stream is stored separately. This makes it computationally not feasible to recover the original data stream from the ciphertext alone. In this the encryption and decryption is performing on the same device that's why whenever the mobile device is stolen by someone, all the important data is not recovered [2].

The data is secured in desktop computers. The first computer device is recording device which is used for encryption and other computer is master which is used to decrypt that data. This model is used only for desktop computer [3].

The data of type image is encrypted by using single unique key. After encryption this unique key is sending to the receiver party for decryption purpose. If the key is received by the receiver successfully then the decryption process is done on that side. The same key is used for encryption and decryption [4].

As we know that today's world is depend on mobile phones. So we propose a system in which we provide the same level of security to the data recorded by the mobile phones. As we record the data from the mobile, that data is stored in the encrypted form so that no one can decrypt it as the decryption process is only done by the master device.

In this paper, we are trying to overcome all this disadvantages by using two devices, one is recording device and other one is master device. The recording device is our android phone and master device is our desktop computer. Recording device is used to store the data in encryption form and Master device is used to decrypt the data. We only the person who have that master device so no one can decrypt our data whatever we recorded in our device. The recording device records all the data and stored it in the encrypted form and then transfers all these information into the master device in which we can decrypt it easily.

Only providing security to the information is not sufficient, the same level of security is required for keys by which we are performing encryption and decryption. So for the encryption of data we are using symmetric key and for encrypting keys we are using asymmetric key. Keys are also protected so that no one can attack on the key. That's why here we are providing encryption technique on keys with data. Both the things are copied into master device but in encrypted form.

So to achieve the highly secured method to protect the data we are using hybrid encryption for our system. Hybrid encryption means both type of encryption techniques we are using here i.e. Symmetric and Asymmetric encryption. We use the advantages of both the techniques. The existing system is based on the desktop system and here we work on mobile

devices. Because now a days mobile devices are very useful in our day to day life.And we can easily move or keep it with you whenever you need them anytime.

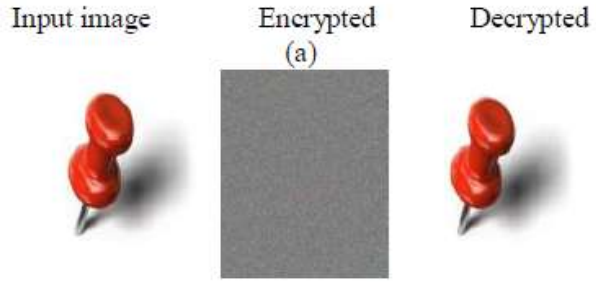

FIG.1.INPUT, ENCRYPTED AND DECRYPTED IMAGE

In the figure above, there are three images as Input image, Encrypted image and Decrypted image. The original image is taken as input in android device and performs encryption on it. Encryption is performed on android device which is used as recording device. After performing encryption, we get encrypted image as shown above in figure. Then the encrypted image is copied in the master device. Here we perform decryption on the encrypted image so that we will get Decrypted image same as input image.

III. PROPOSED WORK

To solve the stated problem, consider two devices one for recording purpose called Recording device and another for processing called Master device. Recording device which is android device encrypt the data and send it to the Master device i.e. desktop computer, where decryption will done. Recording and Master Device will perform some initial communication. In which Master device will generate pair of key i.e. public key Kpub and Private key Kpr.

In this system, there are three modules as Initial setup on recording device, Encryption on recording device and Decryption on master device. Recording device is the mobile device on which we store the information in encrypted form by applying hybrid encryption and master device is a desktop computer system in which we perform decryption. Recording device is only used for storage but storing the information in encrypted form. The steps which we are going to perform in each module are as follows:

Recording device perform some initial operation in secure area.

Setup on Recording device

1. Dividing the storage in blocks.
2. Generating the key and initial vector.
3. Encrypt both using public key and store it into first block of storage.
4. For each block in storage Encrypt (K1; (IV1 XOR i)) and store in block bi Store.

Initial setup is done on recording device. First the storage is divided into blocks. Then generating the key K1 and Initialization vector. Encrypting this key and IV by using public key and storing it into the first two storage block. Now for each remaining blocks other than first three blocks encrypt (IV XOR i) which produces mask and store it into Bi.

Encryption on Recording device

Let Mi be the ith block of data.

1. Recording device will generate key K2 using walsh function and store it after encrypting it using public key.
2. Overwrite block i to n
    a. Encrypt mask using k2.
    b. Overwrite bi with the (mask XOR Ci)

For Encryption on recording device generate random key K2 and now encrypt the data using this key and the produced cipher text is XOR with the mask stored in storage blocks and the result is stored in respective blocks in which their input mask is stored. And the key K2 is encrypted by using public key and store it into third block of the storage.

Decryption on Master device

Decryption of the data is performed by the master device. All the data is copied to the master device. Using private key of master device , decrypt bocks of storage having keys and IV1. Now we remove the mask as :

1. Generating the mask using IV1
2. Encrypt (IV1 XOR i) using K1 which is mask.
   Update bi with the value bi XOR mask.

The blocks are now decrypted as:

1. For each block:
2. Mi = Decrypt (K2; bi)

During decryption Master device will decrypt the blocks that contain the keys and initialization vector. Next step will to remove the mask. To remove the mask, encrypt the Initialization vector using the obtained secrete key and XOR with the content of the block which gives the cipher text. This cipher text is the decrypted using the second secret key which was used during the encryption process, will gives the original data.

The decryption is perform on Master device. First of all decrypt the first three blocks of the storage by using private key because they all are encrypted by using public key. After decryption we get K1, IV and K2. Now Using K1 encrypt(IV XOR i) which will produce mask. Now mask is XOR with Bi which produces Cipher text and stored it into block again of index i. Now decrypt the block Bi using key K2 so finally it produces the original message or data.

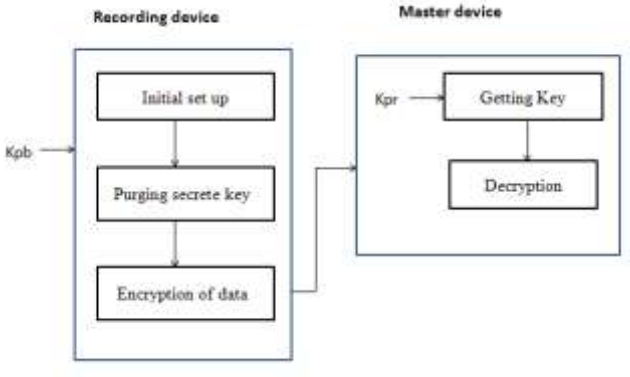

Fig 2. Basic model of Recording and Master device

In the above fig. there are two devices Recording device and Master device. On recording device two out of three modules i.e. initial setup & encryption are performed on recording device and the last module i.e. decryption is done on master device. All the encrypted data then transferred to the master device for decryption. So the encryption is done on one device and decryption is done on another device.

IV. Conclusion

In this paper we want to secure the data by using two devices. One is recording device and other is master device. So the recording device records the data and stores that data in mobile in encrypted form. Then we transfer all the encrypted data into the master device. The mater device is only the device which decrypts that data into its original form. The master device is only accessible by the authorized user. So that if the android device is stolen by someone then there is no loss of data because no one can decrypt it on that device.

References

[1] M Prabu Kumar1 and K Praneesh Kumar Yadav2, "Data Security in Mobile Devices by Geo-Locking, "International Journal of Network Security & Its Applications (IJNSA), Vol.1, No.3, October 2009,

[2] Yu Chen* and Wei-Shinn Ku, "Self-Encryption Scheme for Data Security in Mobile Devices" , CCNC'09, Las Vegas, NV, USA, Jan. 10 – 13, 2009

[3] Ms. Raana Syeda, S.U.Nimbhoekar, "Undecryptable encryptiob against network and forensic ataack" International journal of scientific and research publication,Vol 2, Issue 1, Jan 2012.ISSN 2250-3153.

[4] Kaladharan N , "Unique key using encryption and decryption of image", International journal of Advanced research in computer and communication enginnering.Vol 3,Issue 10. October 2014.

.