Analysis of Cryptography Algorithms for Security in Mobile Devices

Dr. Y. Angeline Christobel [1], Usha Rani Sridhar [2]

[1]Assistant Professor, Department of Computer Science, Hindustan College of Arts and Science, Chennai

[2] Assistant Professor, AMA International University, Bahrain

---***---

Abstract - *The* security issues of mobile devices have increased to a great extent due to the drastic increase of mobile devices. In this paper, an elaborate study of the cryptographic algorithms like symmetric, asymmetric, finger print recognition and voice recognition have been done and a hybrid algorithm is proposed to obtain a high level of security,

Keywords: Symmetry, Asymmetry, Bio-centric, Finger Print, IRIS

1. INTRODUCTION

In recent years, due to the rapid development of technology, the work style and lifestyle both as individual and society is prudent to foresee what impact this new technologies will bring tomorrow that will be disruptive in nature. The usage of mobile devices is further extended to portable technologies including but not limited to mobile phones, ipods, MP3 players, notebooks, and tablets. It provides various chances and facilities which also result in threats associated with privacy and security [18]. In view of the wide availability of the resources used by mobiles, the requirement of security is eminent which is increasing to a larger extent. The threat to mobile devices will enlarge in order that the bad elements will invade the infrastructure to gain entry into the communications of corporate world [18]. Mobile devices are vulnerable to security threats like loss of data, device crash, malware and external breaches. Since the manpower resources are crucial to the business transactions, it is inevitable for the mobile devices usage escalation.

The present life is changed by mobility at all levels like professional, personal and social[18]. Most of the workforce use mobile devices for prolonged period a substantial part of the tasks performed on desktops earlier[18]. The dependence of mobile devices is phenomenal with increasing pace and the mobile atmosphere is both wide and never- ending [18]. Mobile computing [1] is predominantly vital in view of the increase of portable [1] computers and the urge to have un-interrupted network connection to the internet and matter where the node is physically located [1]. This study of research is aimed at knowing the requirement of the security, the hurdles involved in the availability of security with any bottle necks to the available data and to safeguard the mobile devices from all kinds of risks.

2. RELATED WORKS

Review has been done on various journals to understand on mobile security threats and methods to safeguard the devices. The review has helped in understanding the different types of mobile security attacks and the management techniques that can be used to protect the mobile devices from all sorts of threats.

The authors of paper [1] have done a study on the characteristics, applications, limitations and issues of computing in mobile devices. The first section has given an introduction to computing with mobility. The second section has done a study on the technologies that can be used for communication. The next sections explain about the importance of mobile computing, its limitations and problems and conclude saying the advantages of mobile devices. Since this research is about the study of security challenges of mobile devices, the study of this article has given an idea about the security issues.

The paper [2] is an analysis of the different approaches on how to address the mobile security challenges. The various security threats associated with mobile devices are identified and the multilayered collaborative technique has been recommended as a solution to protect mobile devices from threats. This paper is of more value as this research is also to recommend a method to enhance the security of mobile devices.

The paper [3] has analyzed all the security problems that are challenging while designing mobile devices. The author has done an elaborate study on the requirements of communication security needed to protect devices that are mobile and use networking with immobile devices.

In [4] the authors have taken into account the advancement in the technical advancement of the mobile devices. Each and every day new features are being introduced in mobile devices to extend their computing capability which again leads to new security threats. The article has made a thorough study of the challenges in both the hardware and software of the mobile devices. It has also analyzed the differences in the environments of mobile devices and fixed computing devices. The article has also done a comparative study of the different security models. Finally the authors have suggested some commandments for future mobile security research.

The paper[5] by Pullela is an elaborate study of the security protocols. The paper has analyzed the differences between the types of security protocols and how to choose a protocol for the security requirement. The paper is concluded saying "As and when new features get added to mobile devices, the security protocols also need to be altered to protect the mobile devices from threats due to added new features".

In [6] the authors have analyzed the various internet security issues and the papers [7,8,9] have done an elaborate analysis on the various security issues and the challenges being faced due to the advancement in the features of mobile devices. The web links [19, 20] are resources of the security problems, security development and test tools, wireless security tips and wireless security critical success factors.

3. Cryptographic Algorithms

Cryptography [11] is a technical term that refers to hiding information. In cryptography mathematics is used to scramble the information that is to be sent over unsecured channel which is encryption[11].As the information is scrambled unauthorized persons will not be able to understand the sent data. Decryption [11] is the reverse of encryption where in which the mathematically scrambled data will be unscrambled to retrieve the original information [11]. Any mathematical function that works in combination with a key, used to encrypt and decrypt data can be referred to as cryptographic algorithm [11].The strength of the algorithm depends on the techniques used for encryption and the key secrecy [11].The two types of cryptographic techniques are symmetric [11] and asymmetric[11].

Symmetric Algorithm

In symmetric algorithm the same secret key is used at the transmitting and receiving end. As the secret key needs to be disclosed at the receiving end and need to be a secret it is also known as Private-key algorithm. It becomes unsafe if anybody gets to know the secret key. It is the oldest technique and the advantage is, it consumes very less computing power[15].There are two different techniques used by symmetric algorithms. The AES, RC6 and Blowfish symmetric algorithms use block cipher [14]. A block cipher divides data into chunks, pads the last chunk if necessary, and then encrypts each chunk in its turn [14]. The RC4 algorithm uses the Stream Cipher. A streaming cipher uses a series of random numbers seeded with a cipher key to encrypt a stream of bits [14].

Asymmetric Algorithm

In asymmetric algorithm the secret key at the transmitting end is different from the secret key at the receiving end. This algorithm uses a key pair-one public key and one private key[11].The private and the public keys are needed for encryption and decryption[11]. RSA, DSA, ELGAMAL [15] . Symmetric algorithms use identical key for encryption and decryption whereas the asymmetric algorithms use different keys for encryption and decryption [14].Asymmetric algorithms need a very large bit size to obtain similar level of security which can be achieved with a very small bit size using symmetric algorithm [14].Asymmetric algorithms are very slow and need large computing power compared to symmetric algorithms an hence cannot be used to encrypt huge amounts of data.

When the symmetric and asymmetric algorithm are combined and used together, use of the best features of both the algorithmic types can be combined and the new algorithm can be named as an hybrid algorithm. A public key algorithm can be used to encrypt a randomly generated encryption key, and the random key can be used to encrypt the actual message using a symmetric algorithm [14].

Bio-Centric Algorithms

Fingerprint Recognition algorithms [10]

A template of the finger print of the owner is saved in the mobile phone and when the user puts his finger on the mobile the recognition algorithm tries to match the live finger print with the template saved in the phone. If it is matched then the mobile is ready for use. The finger print recognition works on identifying the minutiae which is the intersection point of the ridges and valleys on the finger [10]. The minutiae, ridges and valleys are unique to every human being and hence the security level is effectively good.

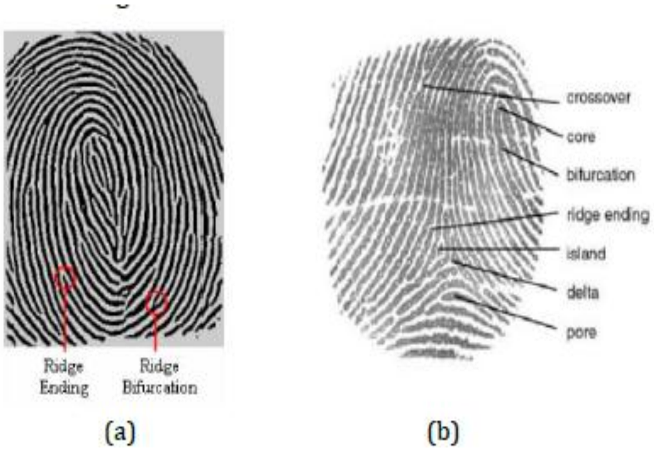

Fig 1[21] : a)Two minutia featuresb)Other minutia features

Voice Recognition algorithm

This algorithm recognizes the voice tone of a person and tries to match with the voice sample which is prerecorded and saved in the mobile by the owner. If the two matches then the mobile is authenticated for use. Hence there is a very minimum security threat.

Fig 2: Voice recognition

Face recognition algorithm

As almost all mobile phones are equipped with a camera, face recognition [10] can be used for security. A photo can be captured and saved in the mobile and whenever the user shows his face on the mobile, the algorithm will try to match it with the captured image. Only, if a perfect match is found between the two images the mobile will be authenticated for use.

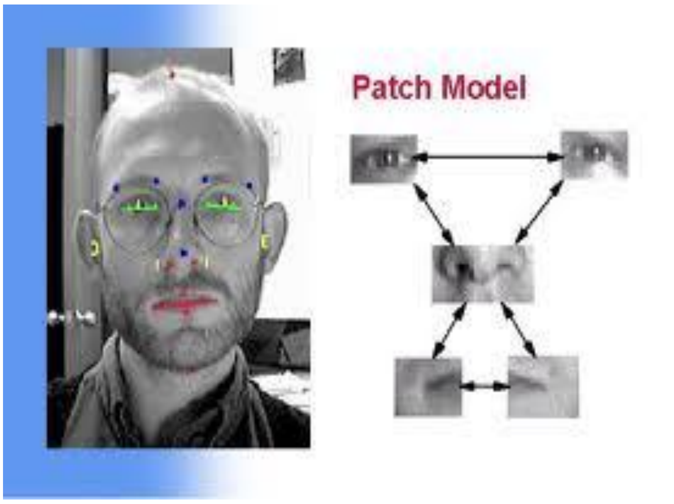

Fig 3: Face recognition pattern

Iris Recognition Algorithm

Another effective biometric security approach is Iris recognition. Situated at the back of the cornea, covering the pupil, Iris is a part in the eye which is colored. The technology using Iris recognition is centered around iris's uniqueness. Even in the case of twins which are identical, the irises are entirely different. Certain characteristics like pits, fibres, freckles, rings are captured by Iris. All the information about these characteristics can be read by the iris which is stored in 'Iris Code' [10]. While scanning, a still picture of the eye and the live eye can be differentiated by the current technology. Small and continuous fluctuations are undergone by the pupil in the live eye while it is not so in the case of the pupil in the picture of an eye. Hence, more reliance is considered for iris recognition in order to secure mobile phones. Multiple images of a user's iris are being captured during an enrollment process. The 'Iris Code' image is stored in an image database with the user's approval. Under the verification process, the iris code stored in the database and the user's iris are scanned again and compared. This technology of iris recognition security , provides a choice of storing iris code for both irises, and during verification, both eyes are required to be scanned. A mismatch of both irises will lead to a security alarm in the mobile phone.

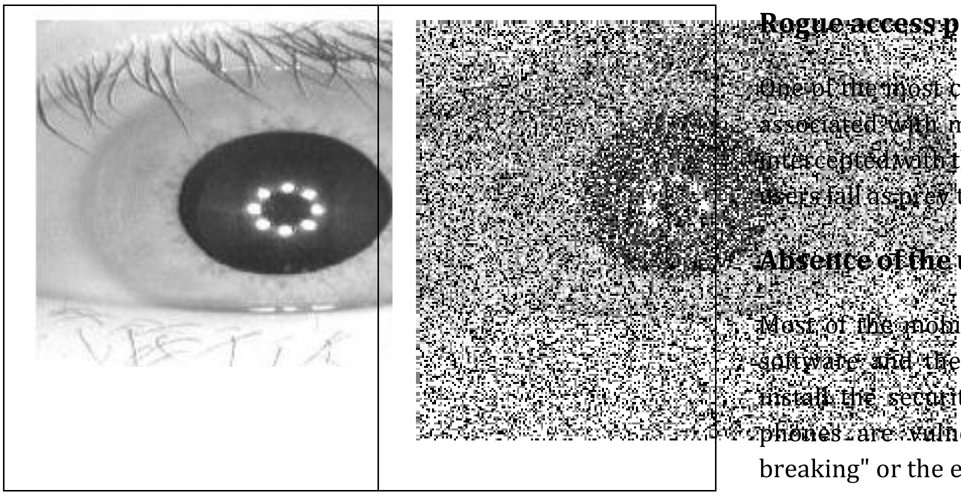

Fig 4[22]: a. IRIS image b. Encrypted IRIS image

4. Results and Recommendations

As the usage of mobiles has increased the security issues of mobile devices has also increased to a very great extent. The users need to be concerned about the following five of the top mobile security issues:

Mobile apps[13]

Mobile apps are very convenient and enhance value to the mobile experience. Many rogue apps with malware get downloaded into mobile devices. For many years, the computer users were concerned about Trojans, malicious programs [10] function under the pretext of being interesting or useful .Apps that appear to be useful are not so in the age of mobile.

Mobile banking is going to rein the business world. Already most of the online banking users do their banking through mobile phones though the security is at stake. Most of the users are not cautious about using legitimate apps[10] without the developers being updating the apps. Further the users perform online banking, mobile shopping social networks, mailing etc without running security software.

Data security

Though the mobile users look at the convenience, they do not envisage the risks involved. The operating systems are not updated by the vendors in the mobile devices. Further the manufacturers will not support the older devices which are required to run update operating systems. Malicious and critical software used are vulnerable to many risks that are posed to the users.

Rogue access points and Insecure Wi-Fi

One of the most convenient modes of transmissions is but associated with many security risks. The data are always intercepted with the transmissions not being encrypted. The users fall as prey to the rogue access exploiters.

Absence of the use of security software or firewalls

Most of the mobile devices are not with built-in security software and the users ignore the fact that they should install the security software. It is also common that the phones are vulnerable to threats by “rooting” or “jail breaking" or the exploitation by cybercriminals.

Apart from the above security threats, absence of password-protecting phones leads to the data being mis-used from stolen phones.

The security issues can be tackled by combining the features of both the cryptographic algorithmic technique and bio-centric algorithmic technique.

Proposed Hybrid Algorithm

The proposed hybrid algorithm is a fusion [10] of symmetric, asymmetric and a biometric fingerprint algorithm which can be referred a bio-hybrid algorithm.

The algorithm has two phases

1. The biometric authentication
2. Hybrid authentication

The advantage of this algorithm is accuracy as the biometric signals are used which are unique for every person and then we authenticate with hybrid cryptography which is combination of the symmetric and asymmetric cryptography. At the first stage the biometric module will accept or reject. If accepted then the hybrid level authentication starts.

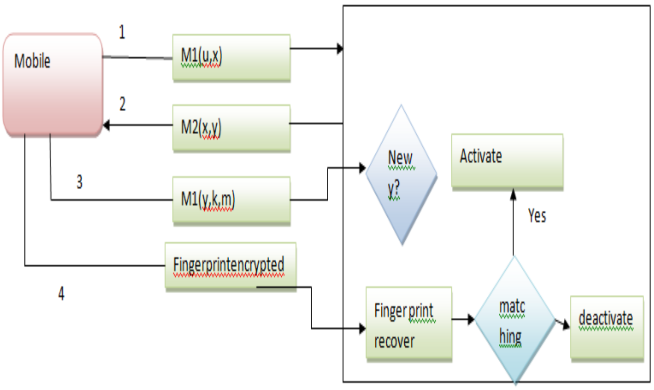

Fig 5: Hybrid Algorithm with Fingerprint recognition

Registration, Login and Authentication are the three security checks that will be carried before you can access the mobile. In the registration phase[15] the finger print recognition works on identifying the minutiae[10]which is the intersection point of the ridges[10] and valleys[10] on the finger in the database.

In the login phase when the user keeps his finger on the mobile, the minutiae from the database tries to match minutiae of the finger placed on the mobile with the one in the database. If they match then it goes to the next level of security check which is the hybrid cryptographic algorithm. The authentication is carried out with the help of message 1 and message2 as follows:

1. User sends message 1[16] M1(U, Random) to recognize the user M1 along with a random number x, by using the principal[16] M2's public key[16]
2. The private key of principal M2 can only read message1.Principal M2 generates a random number y and sends it together with x in message 2 M2(x,y) encrypted with the sender's public key. When the user recognizes x inside message2, the user gets ensured that message 2 is responding[16] and that only message 2 can open message 1 with M2's private key.
3. Fingerprint is incorporated to finish the process of mutual authentication [16] which is confirmed by Messages 3,4 .
4. The user has to provide her finger print, which will then be encrypted. The encryption key k will be generated from the raw fingerprint image which will sent to the central server through a secure channel.

5. CONCLUSION

In this study, it is found that traditional algorithms will not protect the current internet information security with the emergence of hackers even though Fingerprint algorithms has many advantages like increased accuracy, advanced biometrics, user friendly, requiring less storage space. So a hybrid cryptography algorithm along the finger print recognition is proposed. This will obtain a high level security.

6. REFERENCES

1. Deepak G , Dr. Pradeep B S "Challenging Issues and Limitations of Mobile Computing" International Journal Computer Technology & Applications, Feb 2012,Vol 3 (1),Pages 177-181
2. Sathyan.J, Sadasivan "Multilayered collaborative approach to address enterprise mobile security challenges" Mobility Practice,I nfosys Technology Ltd, India, Collaborative Security Technologies(CoSec) IEEE Workshop 15 December 2010,Pages 1-6
3. Audun Josang, Gunnar Sandererud "Security in Mobile Communications:Challenges and Opportunities" Australian Information Security workshop(AISW2003)Adelaide, Australia.Conferences in Research and Practice in Information Technology, Vol 21
4. Jon Oberheide, Farnam Jahanian "When Mobile is Harder than Fixed:Demystifying Security Challenges in Mobile Environments"Electrical Engineering and Computer Science, University of Michigan,Ann Arbor. The Eleventh International Workshop on Mobile Computing Systems and Applications, ACM978-1-4503-0005, 22 February,2010, Annapolis,MD ,USA
5. Srikanth Pullela "Security Issues in Mobile Computing" Department of Computer Science University of Texas at Arlington Technical report, 2002.
6. Vipul Gupta and Sumit Gupta "Securing the Wireless Internet" IEEE Communications 2001
7. Mavridis I Pangalos G "Security Issues in a Mobile Computing Paradigm" Communications and Multimedia Security, Vol 3, S.Katsikas(Ed),IFIP 1997, published by Chapman & Hall
8. M.Satyanarayanan "Fundamental Challenges in Mobile Computing" School of Computer Science, Carnegie Mellon University, Fifteenth ACM Symposium on Principles of Distributed Computing , May 1996, Philadelphia, PA
9. PA Artjom Vassiljev " Enhancing the hierarchical Framework Model of Mobile Security" June 2010
10. Nirav Jobanputra "Emerging Security Technologies for Mobile User Accesses" San Jose State University, Volume 2, Issue 4, eJETA.org, Jan 2009.
11. Ayushi "A Symmetric Key Cryptographic Algorithm" IJCA, Volume1,No.15,2010
12. Hatem Mohamed, Diaa Salama "Evaluating the Performance of Symmetric Algorithms",International Journal of Network Security, Vol.10,No 3,PP.213-219,May 2010.
13. http://digitaljournal.com/article/345824#ixzz2YLBbeOqL
14. http://www.omnisecu.com/security/public-key-infrastructure/symmetric-encryption-algorithms.htm
15. http://www.omnisecu.com/security/public-key-infrastructure/symmetric-encryption-algorithms.htm
16. http://users.suse.com/~garloff/Writings/mutt_gpg/node3.html
17. Kai Xi, Tohari Ahmad, Fengling Han and Jiankun Hu "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment", Security Comm. Networks (2010),Published in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.225

18. Wang Tianfu, K. Ramesh Babu "Design of a Hybrid Cryptographic Algorithm" International Journal of Computer Science & Communication Networks, 2012, Vol 2(2), 277-283, ISSN:2249-5789
19. http://www.mcafee.com/us/resources/reports/rp-cylab-mobile- security.pdf(old11)
20. http://www.mobileinfo.com/Security
21. http://digitaljournal.com/article/345824#ixzz2YLBbeOq
22. Sangram Bana " Fingerprint Recognition using Image Segmentation" (IJAEST) International Journal of Advanced Engineering Sciences and Technologies, 2011, Vol No. 5, Issue No. 1, 012 – 023
23. Abdullah Sharaf Alghamdi, Hanif Ullah "A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm" (IJCNS) International Journal of Computer and Network Security, Vol. 2, No. 4, April 2010
24. Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni, " Enhancing Data Security by using Hybrid Cryptographic Algorithm" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013