International Journal of Research in Engineering, Science and Management
Volume-1, Issue-9, September-2018
www.ijresm.com | ISSN (Online): 2581-5782

Identity Protection in Smart Phones Using Hybrid Encryption

J. Sathya[1], C. N. Manokaran[2]
[1]*Student, Department of MCA, VLB Janakiammal College of Arts and Science, Coimbatore, India*
[2]*Assistant Professor, Department of MCA, VLB Janakiammal College of Arts and Science, Coimbatore, India*

Abstract—**Smart phones users are becoming more popular now a days. Privacy and security are the two main concerns in Smart phones. There is a requirement for the structure to offer security with minimum computational speed. We developed the structure to ensure the identity protection in Smart phones by means of cryptography where Blowfish and Elliptic Curve Cryptography are joined together to offer more security and privacy. Random number is used to increase the security and the rounds in the Blowfish also get randomized to make the performance better.**

***Index Terms*—Blowfish, Elliptic Curve Cryptography, Smart phones, Security, Randomization.**

I. Introduction

Cryptography is the Greek word which means secret writing which has the process of converting plain text into cipher text. This process is carried out by means of cryptographic algorithms and the key. Cryptography is of two types namely Symmetric Cryptography and Asymmetric Cryptography. Symmetric Cryptography is the method which uses the same key for both encryption and decryption. Advantages of this using technique are that the data encryption can take place in less time, it uses computer resources. Disadvantages of this technique are that there is a lack of guarantee in ensuring the origin and legitimacy of the messages. Symmetric Cryptography algorithms are DES, 3DES, AES, RC4, RC6 and Blowfish. Asymmetric Cryptography is the technique which involves two keys namely private key and public key .Private key is kept secret and the public key is known to all. Advantages of using this technique are that it solves the problem of distributing the keys; it offers the path for non-repudiation. Disadvantages of using this technique is that is slower in speed encryption compared to Symmetric Cryptography, it utilizes more resources. Asymmetric Cryptographic algorithms are Diffie-Hellman, RSA, Elgamal, and Elliptic Curve Cryptography. Generally, Cryptography involves two process referred as Encryption, Decryption where Encryption is the method making the non-understandable text by converting the understandable text and Decryption is the method of making the non-understandable text from understandable text. Hybrid Approach is the combination of both Symmetric and Asymmetric Cryptography.

Cryptographic services like Encryption, Decryption, and Key Generation are offered by group of API referred as Java Cryptographic Extensions. Cryptographic algorithms specified above are implemented in Java by utilizing the packages referred as java.crypto and java.security.

Cryptographic algorithms are proficient approaches to afford security to the user's data. As based on the comparative analysis, ECC is a kind of asymmetric crypto system which offers equal security level with smaller key size in comparison with other public cryptosystems which uses to reduce the processing overhead. Blowfish algorithm affords more speed, compactness and suppleness of the key size. Data Encryption and key expansion are the two major parts of this algorithm. 16 rounds are totally taken place in this blowfish algorithm whereas in every round there involves a process of key dependent permutation and key, data dependent substitution. Blowfish is more preferable for the application where key does not changes frequently.

II. Related Work

Subasree and Sakthivel (2010) proposed a hybrid approach on the combination of ECC, MD5 and Dual RSA [1].

Kumar (2012) reveals a hybrid approach with the combination with the combination of AES, ECC and MD5.The result shows that encryption takes more long time [2].

Pradap Chandra Mandel et al (2012) offer a fair comparison between the algorithms likely DES, 3DES, AES and Blowfish. The result reveals that Blowfish algorithm is best suited algorithm in terms of rounds, key size, and block size [2].

M Bafandehkar et al (2013) describes an outline of comparing ECC with other public cryptosystem. The result specifies that ECC offers more security with smaller parameters in comparison with others [4].

Gutub and Khan (2015) proposed a hybrid approach with the combination of using DES, RSA and AES [5].

III. Methodology

In this paper we proposed a structure to offer identity protection in smart phones. To deal with more security, there are various cryptographic algorithms but the choice has to made on the basis of security also performance improvement in smart phones. We proposed a hybrid approach with the combination

of Elliptic Curve Cryptography and Blowfish where Blowfish is more appropriate for smart phone because there is no such more possibility to crack the blowfish algorithm. In comparison with others Blowfish will have better performance because the key changes frequently. Some modifications are made in Blowfish to make the key secure.

In the proposed hybrid approach Randomization concept is implemented in each and every encryption process where the attackers could not be capable to decrypt. Blowfish increases 18 sub keys which are reserved as secure by making an XOR operation with plain text by means of random number which minimizes the number of rounds in Blowfish.

In the first step, the key of the Blowfish is exchanged with ECC for more encryption/decryption whereas in every encryption process, a new random number of 64 bit is created which checks whether its least significant bit holds minimum five 1's or not. The function F will be implemented by ensuring the place of 1's in least significant bit. Attackers is not able to attack because we have made the restriction that minimum five rounds need to carry out in Blowfish.

IV. Conclusion

Smart Phones need security for user's identity protection. The proposed structure provides stronger security for smart phone users. By applying randomization in every encryption, attacker could not be able to crack the key. Our proposed scheme reduces execution time in comparison with Original Blowfish algorithm.

References

[1] Subasree, S., Sakthivel, N.K.,"Design of a new security protocol using hybrid cryptography algorithms", IJRRAS 2 (2), PP: 95–103, 2010.
[2] Kumar, N.,"A Secure Communication Wireless Sensor Networks through Hybrid (AES+ECC) Algorithm", vol. 386. Von LAP LAMBERTAcademic Publishing, 2012.
[3] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" ,Journal of Global Research in Computer Science ,Volume 3, No. 8, August 2012.
[4] M. Bafandehkar, S. Yasin, R. Mahmod, and Z. Mohd Hanap,"Comparison of ECC and RSA Algorithm in Resource Constrained Device", Int. Conf. on IT Convergence and Security, PP: 1-3,2013.
[5] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" ,Journal of Global Research in Computer Science ,Volume 3, No. 8, August 2012.
[6] S. Gupta, and J. Sharma, "A Hybrid Encryption Algorithm based on RSA and Diffie Hellman", Computational Intelligence & Computing Research (ICCIC), IEEE International Conference, and PP: 1-4, 2012.
[7] Komal Rege, Nikita Goenka, Pooja Bhutada, Sunil Mane," Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", International Journal of Computer Applications (0975 – 8887) ,Volume 71–No.22, June 2013.
[8] V. Kapoor, Rahul Yadav,"A Hybrid Cryptography Technique for Improving Network Security", International Journal of Computer Applications (0975 – 8887), Volume 141 ,No.11, May 2016.
[9] V. Kapoor, Rahul Yadav,"A Hybrid Cryptography Technique for Improving Network Security", International Journal of Computer Applications (0975 – 8887), Volume 141 ,No.11, May 2016.