ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Survey on the Security Features of Cryptographic Techniques in Mobile Devices

Dr. Mani[1,] A. Mullai [2]

Associate Professor, Department of Computer Science, Puthanampatti, Affiliated to Bharathidasan University, Trichy, Tamil Nadu, India[1]

PhD Research Scholar, Department of Computer Science, Puthanampatti, Affiliated to Bharathidasan University, Trichy, Tamil Nadu, India [2]

ABSTRACT: A revolution of technological advancement has taken place in the field of Communication Technology with the introduction of Wireless Mobile Devices by introducing multifunctional applications embedded in a small device by replacing the traditional and fixed wired technology. Mobile devices play a vital role in everyday life since they provide variety of ubiquitous services. In recent years, the availability of these devices and their ubiquitous services has increased significantly. This is because various forms of connectivity such as Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Bluetooth and Wi-Fi (Wireless Fidelity) etc. are provided to them. Even though some challenges in mobile computing devices cater the needs of the users, the transmission of information can be done very easily, quickly without having any previous knowledge because they are user friendly. The information transmitted through the air by the mobile devices may sometimes being hacked by the hackers. To avoid hacking Security plays a vital role in transmitting the information and it can be achieved by using various cryptographic algorithms to prevent from such attacks. This paper gives a comprehensive survey of cryptographic algorithms and techniques which are being used in mobile devices.

KEYWORDS: Mobile Devices, challenges, hackers, Cryptographic algorithms, techniques.

I. INTRODUCTION

Mobile Computing Portable devices like laptop, palmtop etc. gives an easy access to the people with diverse sources of global information instantaneously anywhere at any place and at any time. It is a technology constantly developing towards the needs of human expectations by using the concept of Bring Your Own Device – Bring Your Own Technology (BYOD – BYOT). A mobile device may be a Personal Digital Assistant (PDA), a handy Cell phone or Web phone, a laptop, or any one of the above numerous devices that allow the user to complete the tasks without being tethered, or connected, to a network. The environment of wireless and mobile bring about different challenges to the users and service providers. The physical constraints like the weight of the device, the battery, the size of the screen, portability, quality of radio transmission, and error rates become more important. Even though the facility of the devices include the mobility of the user, the device, the network, the service provider and also some additional uncertainties, they give opportunities to the users the provision of new services and supplementary information. The major challenges in mobile computing are low bandwidth, high error rate, power restrictions, security, limited capabilities, disconnection and the problems created due to the mobility of the client. Inspite of these challenges security becomes a major concern, because they are connected anonymously. By the application of cryptographic algorithms in mobile computing, the hackers don't get the chance to access the mobile units. Various cryptographic algorithms have been used to maintain security in mobile devices and they provide confidentiality, integrity, availability, non-repudiation, authorization and trust and accounting (CIANATA). This paper gives an overview of various cryptographic techniques which are used to provide such security services in mobile devices.

II. RELATED WORKS

Mavridis I., Pangalos G. [1], in their paper, have discussed the operational and security issues of mobile components in distributed environments. Further they illustrated to eliminate the intrinsic problem of wireless networking using the mobile agents. They applied some security mechanism in their model which is to be implemented in a healthcare paradigm, with some special conditions.

In 2000, Erik Olson and Woojin Yu, [2] surveyed various symmetric key algorithms viz., RC5, RC6, Twofish, and Triple-DES and their usage in mobile computing, specifically in the Palm Pilot, which uses Motorola's Dragon Ball-EZ processor. They illustrated that the architecture used in the processor is similar to the 68K processor and it does not provide the power and versatility of current processors.

In 2000, Wendy Chou [3], surveyed the explosive growth in the usage of mobile and wireless devices demands a new generation of Public Key Cryptography (PKC) schemes, and the limitations on power, bandwidth to provide security in mobile devices, use of Elliptic Curve Cryptography (ECC), its security, performance and also its applications.

In 2002, Limor Elbaz [4], implemented PKC in security of wireless devices and the use of Public Key Infrastructure (PKI) in current as well as in the future applications of mobile phones. Further he showed that the Discretix Crypto Cell implementation of cryptographic algorithms which enable wireless devices to become PKI-enabled cum efficient, lightweight and standard-compliant.

In 2003, Dharma P. Agrawal et al.[5], discussed the technology in mobile computing users by combining wireless networking and mobility which serves anytime and anywhere with of various new applications and also services. They had also analyzed some security issues and various threats in the existing countermeasures. They concluded that encryption plays an important role for secured communication in mobile computing environments.

In 2006, Hanping Lufei and Weisong Shi [6], discussed the emergence of heterogeneous devices and diverse networks, and the difficulty in using a one-size-fits-all encryption algorithm. They also explained the deployment of encryption algorithms to choose an appropriate encryption algorithm from multiple algorithms based on the characteristics of heterogeneous mobile computing environments. They proposed an adaptive encryption protocol, to choose a proper encryption algorithm dynamically which enhances security from the candidate algorithms, and minimizes the time overhead.

In 2008, Abhishek Kumar Gupta [7], discussed the need for information as a driving force for the incoming growth in Web technology, wireless communication, and portable computing devices and also explained the field of mobile computing (computing and communication) with the aim of providing seamless computing environment for mobile users, which are all dependent on information and it is available only by accessing a network. Further they discussed that the mobility can also cause wireless connections to be lost or degraded when the users travel beyond the limitations of network transceivers or enter areas of high interference.

In [2009], S. Krishna Mohan Rao and Dr. A Venugopal Reddy [8], discussed Data dissemination in asymmetrical communication environment, where the capacity of the downlink communication is much greater than the uplink communication capacity and it is best suited for mobile environment. The important issue discussed in this paper is that the data dissemination which illustrates quickly access of the data item in mobile devices with minimum access time so that the mobile clients save the precious battery power while they are moving from one place to another.

In [2009], widespread growth in applications for resource-limited Wireless Sensor Networks (WSN), and also the need for reliable and efficient security mechanisms using two potential block ciphers, namely the RC5 and AES-Rijindael discussed and analyzed the suitability of the algorithm for resource-limited wireless network security by M. Razvi Doomun, and KMS Soyjaudah [9].

In [2009], Kar and Banshidhar Majhi[10], proposed an efficient password security of Multi-Party key exchange protocol based on elliptic curve discrete logarithm problem (ECDLP), and these protocols allow a group of parties communicating over a public network to establish a common secret key called Session Key and also build protocol for password authentication model, where group members were assumed to hold an individual password rather than a common password and two one-way hash functions to build the security level high.

In [2009], Mooseeop Kim et.al. [11], proposed a compact architecture for a cryptographic engine on a mobile platform, which has very stringent limitations with respect to the circuit area and the consuming power .It is highly effective to implement the scalable RSA and unified SHA algorithms with a minimum resource usage. The combined performance results of circuit area, power efficiency, throughput, and functionality strongly indicate that the proposed architecture for cryptographic hardware is suitable for mobile computing systems.

In [2010], Bruno P.S. Rocha et. al [12], demonstrated a security service, which works as a middleware, to dynamically change the security protocols used between two peers and these changes can occur based on variations on wireless medium parameters, system resource usage, available hardware resources, application-defined Quality of Service (QoS) metrics, and desired data security levels. They provide the solution to some static security protocols and adaptability of middleware in different conditions of medium and system, and shows performance gain in the execution of cryptographic primitives, through the use of data semantics.

In [2010], Sathish Alampalayam Kumar [13], suggested a mobile agent based mobile computing system, the classification of various types of security attacks, the security solutions for those types of attacks proposed by various schemes and the open research issues in providing security for mobile agent based computing systems.

In [2011], Sameer Hasan et. al. [14], proposed a non-server (that is P2P) architecture PKC to secure the mobile communications. They have discussed and implemented various security services needed for mobile communication. Compared with server based architecture, this architecture has low risk and the security has been improved to avoid many attacks. They used NTRU algorithm for public key cryptography in non-server architecture and tested on real equipment, the solution security and potential risks.

In [2011], Rahat Afreen and S.C. Mehrotra [15], discussed the ECC emerged in its proper implementation in various directions to analyze in hardware as well as software platforms. Helena Rifa-Pous and Jordi Herrera-Joancomarti [16], discussed the performances of different cryptographic algorithms in PDAs and compared it with device's basic costs in terms of operating system, screen, and network interfaces to determine the overhead and the results were used to estimate the costs of network security protocols design.

In [2011], Jagdish Bhatta and Lok Prakash Pandey [17], proposed a software level cryptographic protocol implementations to measure the energy level through the device's serial port, running them and measuring their power consumption. The results show that the proposed cryptographic protocol provides a guaranteed better security and acquires very less consumption of energy than the existing cryptographic protocols. The performance analysis are compared and proved that the proposed scheme is to be more simple, secure and efficient.

In [2012], K. Sathish Kumar et. al. [18], explained the mobile hand-held device in an efficient way to deliver real time data to users. They designed and implemented an energy efficient authentication protocol that accomplishes a high level security with minimum energy consumption for mobile devices.

In [2012], Masoud Nosrati et. al. [19], proposed an algorithm for security mechanism in different types of mobile devices and the operation systems. This security mechanism uses some algorithms to scramble data into unreadable text which can be only decoded or decrypted by those who possess the associated key and these algorithms consume a significant amount of computing resources such as CPU time, memory, battery power and computation time.

In [2012], Ravinder Singh Mann et. al. [20], presented the comparative analysis of ECC, AES and RSA algorithms experimentally with parameters such as computation time and complexity of the algorithms. Based on the result it was concluded that ECC has more complexity when compared to AES and RSA in mobile devices.

In [2013], Giripunje et al. [21], discussed many differences in mobile devices, their capabilities, computational powers and security requirements in networking environments. The security of mobile communication is concerned with mobile confidentiality, authentication, integrity and non-repudiation. They have mentioned that the currently available network security mechanisms are inadequate. They provided effective security solution using PKC and its implementation in two parts: first, design for API for ECC which generates shared key for secure communication and secondly, a web service is created which distributes this key to validate the mobile user.

In [2013], Ameya Nayak [22], discussed the growing android community, its malware attacks, security concerns, aid in serving as the continuous challenges of identifying current, future vulnerabilities as well as incorporating security strategies against them and this focus on mobile devices.

In [2013], Srikanth Pullela [23], discussed the performance issues like handoffs, routing etc. Then he further addressed that security is another key issue, which needs to be considered when the communication channel is set up. Also protocols are being proposed for different applications like wireless application protocol, 802.11 etc. Most of them are based on the public and private key cryptography.

In [2013], V. Gayoaso Martinez and L. Hernandez Encinas [24], have discussed the ECC, one of the best options for protecting sensitive information. The latest version of the JAVA platform includes a cryptographic provider - SunEC which implements EC operations and protocols. They have explained the complete code of three applications to generate key pairs, perform key exchanges, and produce digital signatures with EC in JAVA.

In [2013], Muhammad Waseem Khan [25], explained that short message service (SMS) is one of the frequently used mobile services with universal availability in all GSM networks but the SMS facility has not achieved secure transmission of plaintext between different mobile phone devices. However, SMS does not have its own built-in mechanism to secure the transmitted data because security is not considered as a priority application for mobile devices. The existing schemes provide room for the secure SMS message communication. The effect of each security scheme on mobile device’s performance was also observed. Finally summary of all security schemes with their limitations was presented.

In [2013], Ram Ratan Ahirwal and Manoj Ahke [26], explained the Diffie-Hellman scheme as one of the key exchanging cryptosystem, and no messages are involved in this scheme and using this key and ECC for encryption and decryption. Two different methods to encrypt and decrypt the message were proposed by them. They pointed out that the second method supports the system with more security than the first method because the sender computes the exponentiation function between the coordinates of the encryption algorithm and the receiver computes the inverse of the exponentiation function between the coordinates of the key in the decryption algorithm, While in the first method, the sender compute the multiplication between the coordinates of the key in the encryption algorithm, the receiver compute the multiplication between the coordinates of the key in decryption algorithm and forward secrecy in HTTPS protocol.

In [2014], Sathish Kumar et. al. [27], have discussed about the mobile hand-held device are used in an efficient way to deliver real time data to the users in the battle field military applications and the use of security features in military applications such as data confidentiality, authentication etc., which are not readily offered by mobile environment. The energy expenditure in such an environment poses bottleneck while achieving privacy. Hence it is necessary to design and implement an energy efficient authentication protocol that accomplishes a high level of security with minimum energy consumption. They have proposed the implementation of energy efficient authentication protocol for mobile devices.

In [2014], Hamed Khiabani et. al. [28], explained the extensive deployment of wireless networking, mobile and embedded devices, other pervasive computing technologies that are prone to security threats for which nobody will be prepared for. Security and privacy are the main concerns in mobile computing which can be observed from several perspectives including hardware, operating systems, networks, databases, user interfaces, and applications.

In [2014], Seema P. Nakhate, and R.M. Goudar [29], have implemented a secured password based mutual authentication protocol for client-server computing using ECC framework which provides secure communication between client and server with the help of user email-id and mobile phone authentication device for mobile handheld device. The proposed protocol is best suited for constrained environments where the resources such as computational power, storage capacity are extremely limited. Such devices are Mobile phones, PDA’s, Palmtops and Smart cards.

In [2015], Vishnu V and Shobha R [30], discussed the security in Wireless Sensor Networks (WSN). They have applied dynamic election of Cluster Head (CH) mechanism and two evolutionary approaches SET-IBS and SET-IBOOS, since it provides security in data transmission and reduces data losses due to nodes failure, less residual energy selected in CH. It improves the lifetime of network by increasing time of FND (First Node to die).

In [2015], Tanmoy Kumar Bishoi et. al. [31], proposed an algorithm to encrypt the data using symmetric key encryption technique and now it can be improved by using variable length key.

In [2015], Sujithra M et. al. [32], due to high performance computing techniques, cryptographic algorithms are implemented and tested in Local as well as Cloud environment. They have revealed that storing mobile data in cloud increases efficiently and AES algorithm performs better when compared with other algorithms in Mean processing time but the combination of MD5+ECC+AES algorithms qualify better than Speed-Up ratio.

In [2016], Said Bouchkaren and Saiida Lazaar [33], discussed secure data transmission through Internet. They have designed and implemented a new secret key cryptosystem due to a number of iterations of encryption and decryption of data in blocks, using cellular automata and compared them with AES algorithm and also they proved that the new algorithm resists against statistical attacks, faster than AES-256, achieved good confusion and diffusion tests.

III. CONCLUSION

Mobile Computing is a new technological development due to the magnificent growth of internet community for various applications and variety of tasks that can be performed at the requirement of the users. But the requirement is that the data must be transferred in a very fast, quick and secured manner. Hence the Cryptographic tools and techniques will be more useful to achieve this. An eavesdropper or intruder can catch the information/data during the transmission. In order to prevent this, various types of cryptographic algorithms have been used. From the findings, Elliptic Curve Cryptography (ECC) is more useful and it produces more security with less number of bits compared to RSA algorithm. It has been proved that the ECC can be applied in various levels of applications and hand - held devices.

REFERENCES

1. Mavridis I., Pangalos G., “Security Issues in Mobile computing Paradigm”. 1997, http://www.researchgate.net.
2. Erik Olson and Woojin Yu, “Encryption   for Mobile computing”, 2000.
3. Wendy Chou, “Elliptic Curve Cryptography and Its applications to Mobile Devices,2000.
4. Limor Elbaz, “Using Public Key Cryptography in Mobile Phones”, White Paper,Discretix Technologies Ltd., Advanced security solutions for constrained environments, October 2002.
5. Dharma P. Agrawal et al., “Secure Mobile Computing”, S.R. Das, S.K. Das (Eds.): IWDC 2003, Springer-Verlag., LNCS 2918, pp.265-278.
6. WHanping Lufei and Weisong Shi, “An Adaptive Encryption Protocol in Mobile Computing”, Wireless/Mobile Network Security, Springer, 2006.
7. WWWWAbhishek Kumar Gupta, “Challenges of Mobile computing”, Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology RIMT – IET, Mandi Gobindgarth, March 29, 2008.
8. S. Krishna Mohan Rao and Dr. A Venugopal Reddy, “Data Dissemination in Mobile Computing Environment”, BIJIT – BVICAM’s International Journal of Information Technology, Bharati Vidyapeeth’s Institute of Computer applications and Management (BVICAM), New Delhi, Vol. 1, No. 1, January 2009.
9. M. Razvi Doomun, and KMS Soyjaudah, “Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security”, International Journal of Network Security, Vol.9, No.1, July 2009, pp. 82–94.
10. Jayaprakash Kar & Banshidhar Majhi, “An Efficient Password Security of Multi-Party key exchange protocol based on ECDLP”, International Journal of Computer Science and Security (IJCSS), Vol.1, Issue 5, Sep. 2009.
11. Mooseeop Kim et.al., “Design of Cryptographic Hardware Architecture for Mobile Computing”, Journal of Information Processing Systems, Vol. 5, No. 4, Dec. 2009.
12. Bruno P.S. Rocha et. al., “Adaptive Security protocol selection for mobile computing”, Journal of Network and Computer Applications 33, 2010, pp. 569.
13. Sathish Alampalayam Kumar, “Classification and Review of Security Schemes in Mobile Computing”, Wireless Sensor Network, June 2010, 2, pp.419-440.
14. Sameer Hasan Al-Bakri, Gazi Mahabubul Alam et. al., “Securing peer-to-peer mobile communications using public key cryptography: New security strategy”, International Journal of the Physical Sciences Vol. 6(4), Feb. 2011, pp. 930-938.

15. Rahat Afreen and S.C. Mehrotra, “A Review on Elliptic Curve Cryptography for Embedded Systems”, International Journal of Computer Science & Information Technology Vol. 3, No 3, June 2011.
16. Helena Rifa-Pous and Jordi Herrera-Joancomarti, “Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices”, Future Internet 2011, 3, 31-48; doi: 10.3390/fi3010031, ISSN 1999-5903, www.mdpi.com/journal/futureinternet.
17. Jagdish Bhatta and Lok Prakash Pandey, “Performance Evaluation of RSA Variants and Elliptic Curve Cryptography on Handheld Devices”, IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No. 11, Nov. 2011.
18. K. Sathish Kumar et. al., “An Experimental Study on Energy Consumption of Cryptographic Algorithms for Mobile Hand-Held Devices”, International Journal of Computer Applications, Vol. 40, No.1, Feb. 2012.
19. Masoud Nosrati et. al., “Mobile and Operating Systems”, Computing: Principles, Devices World Applied Programming, Vol. 2, Issue 7, July 2012.
20. Ravinder Singh Mann et al., “A Comparative Evaluation of Cryptographic Algorithms”, Int. J. Computer Technology & Applications, Vol 3(5), Oct. 2012, pp. 1653-1657.
21. Giripunje et al., International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 5, May 2013, pp. 704-713.
22. Ameya Nayak, “Android Mobile Platform Security and Malware Survey”, IJRET: International Journal of Research in Engineering and Technology, Vol. 02 Issue 11, Nov. 2013.
23. Srikanth Pullela, “Security Issues in Mobile computing”, International Journal of Research in Engineering and Technology, Vol. 02, Issue: 11, Nov. 2013.
24. V. Gayoaso Martinez and L. Hernandez Encinas, “Implementing ECC with Java Standard Edition 7”, International Journal of Computer Science and Artificial Intelligence, Dec. 2013, Vol. 3 Issue. 4, pp. 134-142.
25. Muhammad Waseem Khan, “SMS Security in Mobile Devices: A Survey”, Int. J. Advanced Networking and Applications, Vol. 05, Issue 2, pp. 1873 -1882.
26. Ram Ratan Ahirwal and Manoj Ahke, “Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network”, International Journal of Computer Science and Information Technologies, Vol. 4(2), 2013, pp.363 – 368.
27. Sathish Kumar et. al., “An Asymmetric Authentication Protocol for Mobile Hand held Devices using ECC over Point Multiplication Method”, International Journal of Advanced Research in Computer Science & Technology, Vol. 2, Jan.–March 2014.
28. Hamed Khiabani et. al., “A Review on privacy, Security and Trust issues in Mobile Computing”, Collaborative outcome of University of Malaysia and MIMOS Berhad – Information Security Cluster.
29. Seema P. Nakhate and R.M. Goudar, “Secure Authentication Protocol”, International Journal of Computer Networks and Communications Security, Vol. 2, No. 4, April 2014, pp. 142 – 145.
30. Vishnu V and Shobha R, “Dynamic Cluster Head (CH) Node Election and Secure Data Transaction in CWSNs”, International Journal of Engineering Research, Vol. 4, Issue Special 4, May 2015.
31. Tanmoy Kumar Bishoi et. al., “An Algorithm on Text Based Security in Modern Cryptography”, Journal of Computer Networking, Wireless and Mobile Communications (JCNWMC), Vol. 5, Issue 1, Jun 2015, pp. 9-14.
32. Sujithra M et. al., “Mobile Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud”, Procedia Computer Science 47 (2015), pp. 480-485.
33. Said Bouchkaren and Saiida Lazaar, “A New Iterative Secret Key Cryptosystem Based on Reversible and Irreversible Cellular Automata”, International Journal of Network Security, Vol. 18, No. 2, pp. 345-353, Mar 2016.

BIOGRAPHY

Dr. K. Mani is working as an Associate Professor in the Department of Computer Science, Nehru Memorial College, Puthanampatti, Tamil Nadu since 1989. After did his MCA, he got his Graduation in Operations Research from Operational Research Society of India, Kolkatta and obtained his MTech in Advanced Information Technology from Bharathidasan University, Trichy, Tamil Nadu. He has completed his Ph. D degree from Bharathidasan University relating to enhancing security and optimizing the run time in cryptographic algorithms. His current research area includes cryptography, data mining and coding theory. He has published a number of research papers in national and international journals and conferences.

Mrs. A. Mullai is working as an Associate Professor in the Department of Computer Science, Seethalakshmi Ramaswami College, Bharathidasan University, Trichy, Tamil Nadu, India since 2000. She has 15 years of experience in teaching. After did her M.Sc in Physics, MCA in Computer Applications, she got her M.Phil in Computer Science at Bharathidasan University, Trichy, Tamil Nadu. She has cleared National Level Eligibility Test (NET) conducted by University Grants Commission (UGC), New Delhi. She is currently pursuing doctor of philosophy programme at Nehru Memorial College (Autonomous), Puthanampatti and her current area of research is Cryptography in Mobile Computing. She has published research papers in national and international conferences.

DOI: 10.15680/IJIRCCE.2016. 0402186