International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195223

Secure Transmission of Data through Electronic Devices using ECC Algorithm

G. BanuPriya, K. Dharani
Assistant Professor, Department of Computer Science, SNMV College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT

In recent days securing the data while transferring through electronic devices from one end to the other has became a challenging task to both sender and the receiver. During the transmission of private data over the electronic devices may be hacked some times by the hackers. The data can be secured by using the cryptographic concept. This paper is about how the data are protected while transferring the data from one electronics devices to another using the ECC algorithm. Cryptographic algorithms plays an important role in securing the data against malicious attacks. The main goal of cryptography is not only to secure data from being hacked or attacked also it can be used for authentication of users. There are two types of cryptographic algorithms namely Symmetric key cryptographic algorithms and Asymmetric key cryptographic algorithms. Symmetric key cryptographic algorithm uses the only one key for both encryption and decryption process, where as Asymmetric cryptographic algorithm uses two different keys for encrypting and decrypting the messages. The public key is made publicly available and can be used to encrypt messages. The private key is kept secret and can be used to decrypt the received messages. Nowadays, many electronic devices like electronic phones, tablets, personal computers are in the workplace for transferring the data. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create privacy, integrity and confidentiality, faster, smaller, and more efficient cryptographic keys.

Keywords : Cryptography, Encryption, Decryption, ECC Algorithm, Privacy, Integrity and Confidentiality.

I. INTRODUCTION

Computer data transfer plays a very important role in daily life. The security to a system is essential nowadays ! with the growth of the Information Technology and with the emergence of new techniques, the number of threats a user is supposed to deal with grew exponentially. The process of transfer data is to focus on finding answers for life problem by transfer information from one person to another. The importance of the transfer data can range from business, schools, companies, and government documents. In order to analysis how data is being transfer from the electronic device and to prevent private data from getting out there, we need to simulate several different ways how data can be transferred on the electronic device. Data transfer is achieving by safely copying or moving important data from one location to another. Some examples are, computer to computer, computer to electronic device, electronic device to electronic device, electronic device to the server, and computer to the server. Now it is much easier and faster to transfer data today than it was in the past few decades. Nevertheless, it is even easier for hackers to get private data from the users. As a result, many researches are needed to find safer ways to transfer data and information on the electronic devices.

II. RELIABLE DATA TRANSMISSION AND USAGE IN ELECTRONIC GADGETS

Understanding where you hold private data internally is essential, but it does not provide a complete view of where

your data resides. Understanding data flows is a complicated task, and technology can help to provide transparency into network based data transfers. However, you must additionally understand third-party data access, business-driven data exchange and end- user data transmission capabilities.

A. Third-party data access

Data identification should include obtaining an understanding of private data that is accessible by third parties. This includes data that is exchanged with third parties and third parties that have direct access to internal systems. Once an inventory of third parties with access to private data exists, controls should be implemented to safeguard third-party access. Focus areas should include:

- Secure data transmissions
- Controlled access to data
- Monitoring of third-party access to private data.
- Third-party due information security assurance

B. Design the Policies and standards

Once private data is classified and identified, data protection policies should be developed and/or customized to document security requirements that are specific to the type of private data held by the organization. A high-level policy specifying the requirements for protecting private data should exist and clearly link to the data classification policy.

- Transmission of private data through email and the internet.
- Storage of private data on electronic devices, laptops, Tablets, Pc's, CD, workstations.
- Appropriate use of remote access technologies.
- User responsibilities for classifying data at the point of creation and ensuring that private data users create is included in relevant data/information inventories.
- Private data may not be transmitted through public networks without adequate encryption.
- Approved technologies may be used to exchange data with third parties.
- Private data may not be shared with third parties without sufficient contracts in place specifying information security requirements, their obligations to protect company data, their responsibilities for monitoring their own third parties and the company's right to audit and monitor.
- Access to private data must be logged and monitored where appropriate.
- Private data must be anonym zed before being stored in less controlled environments, such as 0test and development environments.
- Private data must be adequately protected through all stages of the data lifecycle and the systems development lifecycle.

C. How to Protect the Electronic gadgets?

- Harden Electronic gadgets.
- Configurations and enable.
- Features such as password protection and remote wipe facilities.

III. TECHNICAL DATA SECURITY THREATS TO INFORMATION SYSTEMS

1. Android: Changing the Electronic Landscape

Android devices have been well received by the market vendors who are now delivering them across a broad range of price from high end products to low end one that is from HTC, SAMSUNG to MICROMAX. This describes the marketing analysis of Android device in the world & gives the layout of working and performance management of the OS.

2. Mobile Devices.

Use of electronic devices, such as laptops or handheld devices including smart phones, is exploding; however, the security of electronic devices are lagging behind. The situation is complicated by the fact that these devices are often used to conduct work outside the organization's to breaches can occur in a number of ways: devices can be lost, stolen, or their security can be compromised by malicious code invading the operating system and applications.

Mitigation: To promote data security in case a device is lost or stolen, encrypt data on all mobile devices

storing private information. Until more data encryption, user authentication, anti-malware solutions become available and for mobile devices, the best protection and for mobile devices, the best protection policy and monitor the network for malicious activity.

2. Mobile Devices.

Use of electronic devices, such as laptops or handheld devices including smart phones, is exploding; however, the security of electronic devices are lagging behind. The situation is complicated by the fact that these devices are often used to conduct work outside the organization's to breaches can occur in a number of ways: devices can be lost, stolen, or their security can be compromised by malicious code invading the operating system and applications.

Mitigation: To promote data security in case a device is lost or stolen, encrypt data on all mobile devices storing private information. Until more data encryption, user authentication, anti-malware solutions become available and for mobile devices, the best protection and for mobile devices, the best protection policy and monitor the network for malicious activity.

3. Removable media
The use of removable media (e.g., flash drives, CDs, and external hard drives) on an organization's network poses a significant security threat. Without proper protection, these types of media provide a pathway for malware to move between networks or hosts. proper security measures when using removable media devices is necessary to decrease the risk of infecting organization's machines or the entire network.

Mitigation: To minimize the security risks, apply simple preventative steps. These include disabling the "auto run" feature of the operating system on the organization's machines and training users to scan removable media for viruses before opening the files.

4. Poor Passwords
It is especially important for users with access to the most private information. Modern password-cracking programs can easily break weak passwords, such as those containing common words or word groups found in a dictionary. For this reason, user-selected passwords are generally considered to be weaker than randomly-generated passwords.

5. Viruses and worms
Terminology is emerging such as "malware" (or malicious software). Instant Messaging (IM) is very popular because it provides flexibility, speed and ease of communication, but it is also very vulnerable to attacks because of its flexibility. Attacks are not limited to personal computers (PC). They now include cell phones and other processor-based electronics and will only increase and become more sophisticated. To protect the security system database from unwanted electronic intruders requires that no software be introduced into the security network without the Security management's approval.

7. Backup
Backups are kept for several reasons: a computer crash, documentation, employee/contractor investigation, and file corruption. For these reasons, there must be several levels of backup available. The requirements will vary depending upon a specific application.

8. Physical protection
The purpose of physical protection is to prevent access and detect unauthorized surreptitious access. Protection can be in the form of conduit, sealed cable trays, locked rooms, and alarms that indicate potential tampering or unauthorized access.

IV. CRYPTOGRAPHY

Cryptography is the art and science of achieving security by encoding the simple message to make it unreadable. The message to send is in simple or ordinary language understood by all, it is called a plaintext. The process of converting plaintext into a form which cannot be understood without having special information is called encryption. This unreadable form is called cipher text and this special information is called encryption key. The conversion of cipher text again into plaintext with a special knowledge is called decryption, whereas special

knowledge for decryption is called decryption key. Only the receiver has this special knowledge and only receiver can decrypt a cipher text with this knowledge called decryption key.

There are basically two types of cryptography based on the techniques for converting plaintext to cipher and vice versa which are namely called as symmetric and asymmetric cryptography. In symmetric cryptography sender and receiver use the same key for encryption and decryption of test whereas in asymmetric cryptography systems two keys namely public and private keys are used for encryption and decryption process. By keeping the private key safe, you can assure that the data remain safe. But the disadvantage of asymmetric algorithm is that they are computationally intensive. Therefore, in this proposed system symmetric key cryptography is used with the intension of less computation but high data security. Cryptography mechanisms are depending on the degree of randomness and uncertainty in the generation of the cipher text from the plain text. Hence depend on the phenomenon of nature there are various types of cryptography such as: Modern Cryptography is based on the difficult mathematical problems such as prime factorization, matrix manipulation.

A. ECC Algorithm

ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry and network security products. Elliptical curve cryptography is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. The small key size in ECC provides greater security. For faster cryptographic operations and reliability, ECC can be implemented in hardware chips. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very.

Large prime numbers. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve and to establish equivalent security with lower computing power and battery resource usage; it is becoming widely used for mobile applications. Many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone have included support for ECC in their products.

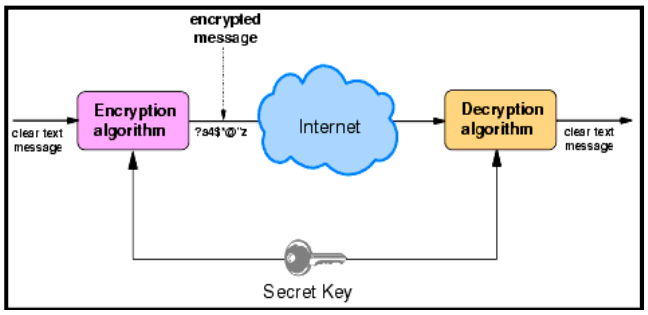

Fig 1 : File Encryption and Decryption Using Secure ECC

1. Features of the ECC algorithm
   - Secrecy and Privacy
   - Integrity
   - Authentication
   - Non repudiation

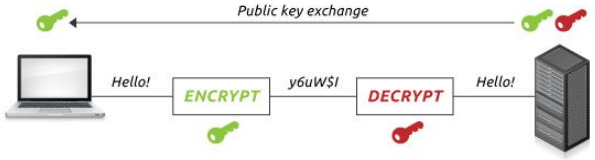

Fig 2 : Encryption and decryption using public key

D. Encryption algorithm

procedure ENCRYPT_MSG

- Consider 'm' has the point 'M' on the curve 'E'.
- Randomly select 'k' in the interval 1 to (n-1).
- 'q' is the prime number in the interval 1 to (n-1).
- Cipher text C will be generated using the equation

  $C = mQ \bmod q$
- Cipher text C will be sent.

E. Decryption algorithm

procedure DECRYPT_MSG

- Plaintext M will be generated using the equation

  $M = Cd \bmod q$
- Where M is the original message.
- 'q' is the prime number in the interval 1 to (n-1).
- 'd' is the private key.

V. THE DESIGN AND IMPLEMENTATION OF DATABASE ENCRYPTION

Information inside the database is shared by multiple parties such as internal users, partners, contractors and others. Private data stored in database could be a target to attackers. The attacker for data stored in database not only from external but also from within the organization. Adding the database encryption, valuable information in database becomes more secure since the encrypted data ensure the confidentiality of the data. System is built and implemented into existing system for protecting user password, where the data is decrypted and produced the similar output as the original plain text.

VI. FUTURE SCOPE

Some future problems will arise in the field of business world that how to protect the private data or the organization data from the attackers. Since most private data is protected from the hackers to get your personal information. Even though, it is difficult to tell how the private data will treat in the future and how it will change the electronic gadgets. Future work will involve more conscious in protecting the private data on electronic gadgets by implementing the better software, methods and efficient algorithms for secure transmission of data through electronic devices. We will focus on the asymmetric cryptographic algorithms such RSA, Elliptic curve algorithms for encrypting and decrypting the data with high speed when comparing to the existing system and implementing in the electronic gadgets for protecting the private data.

VII.CONCLUSION

Technological innovations have put an end to traditional working process. Today's business world is mainly depending upon the electronic gadgets for their working process such online business, e-commerce, and for file transferring through electronic gadgets over the network. This new technology is supposed to occur some serious threats to information security. So, keeping this in mind necessary planning activities should be done to safe guard the information at all levels within a corporation or organization, to secure the data. It is also important to standardize working process; to determine, which procedures are in compliance with information security standards; and safety policies to be set for the usage of electronic devices and wireless networks. The proposed algorithm reduces the effectiveness of intrusion attacks as only a part of the message will be available even if the intruder interrupts any message and decrypts it. Also decrypting part of a message is not very easy. It uses RSA Algorithm, one of the most effective and commonly used cryptographic algorithms and adds more steps to it to reduce attacks A crucial part of information security, is the privacy issue the standards for this issue should also be defined within an organization.

VIII. REFERENCES

[1]. Zhiyong Peng Xiaojuan Li, "The improvement and simulation of LEACHprotocolforWSNs,"Software Engineering and Service Sciences (ICSESS), 2010 IEEE International Conference on , vol., no., pp.500-503, 16-18 July2011.

[2]. Bahadori, M.; Mali, M.R. Sarbishei, O.,Atarodi, M.;Sharifkhani, M. , "A novel approach for secure and fast generation of RSA public and privatekeysonSmartCard," NEWCAS Conference (NEWCAS), 2010 8th IEEE International , vol., no., pp.265-268, 20-23 June 2010.

[3]. Massey, J.L, "An Introduction to Contemporary Cryptology", Proceedings of the IEEE, Special Section on Cryptography, 533-549, May 2011.

[4]. Manikandan.G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G, "A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.

[5]. Wang, X., "Cryptanalysis for Hash Functions and Some Potential Dangers," RSA Conference 2010, Cryptographer's Track, 2010.

[6]. Dr. Sandeep Sharma and Rishabh Arora "Performance Analysis of Cryptography Algorithms" International Journal of Computer Applications (0975 – 8887) Volume 48– No.21, June 2012.

[7]. A. Lazou., and G. R. Weir, "Perceived Risk and Sensitive Data on Mobile Devices", UK. University of Strathclyde Publishing., pp. 183-196, 2011.

[8]. William Stallings, "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition.

[9]. Atul Kahate, "Computer and Network Security", Third Edition,Tata McGraw Hill Publication Company Limited,2013

[10]. Ambedkar, B. R., Gupta, A., Gautam, P., & Bedi, S. S. (2011, June). An Efficient Method to Factorize the RSA Public Key Encryption. In Communication Systems and Network Technologies (CSNT), 2011 International Conference on (pp. 108-111). IEEE.

[11]. NeetuSettia. "Cryptanalysis of modern Cryptography Algorithms". International Journal of Computer Science and Technology. December 2010.

[12]. Nentawe Y.Goshwe(2013) Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS International Journal of Computer Science and Network Security, VOL.13No.7.

Cite this article as :

G. Banu Priya, K. Dharani, "Secure Transmission of Data through Electronic Devices using ECC Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 130-135, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT195223
Journal URL : http://ijsrcseit.com/CSEIT195223