A New Security System Using Elliptic Curves Cryptosystem (ECC) And Md5

Ms Manorama Chouhan*
ME Student of IT
Department of Information Technology, Institute of Engineering & Technology, DAVV
Indore, India

Dr Vivek Kapoor
Assistant Professor
Department of Information Technology, Institute of Engineering & Technology, DAVV
Indore, India

***Abstract*—— Need of data security is an essential issue in the domain of computing traditionally. There are various algorithms are developed in order to improve the security of data, but they having their own issues. Now in these days the traditional algorithms are not much suitable for providing security over the untrusted communications and data exchange. Therefore a new encryption standard is required that can fulfill the current need of security meanwhile that is extendable according to the need. The proposed work includes the development of new hybrid algorithm using ECC and MD5 hash generation technology.**

Keywords: ***Security, Elliptic curve cryptography, MD5.***

INTRODUCTION

Cryptography is the art of hiding data to keep the data more secured and private. This process involves two processes encryption and decryption, where encryption is method to hide data and decryption involve the recovery of the original data. It is capable of keeping the data in secret while saving the information or passing it over the unsafe networks, like internet. These methods are works as safeguard from hackers and make it understandable only to intended receiver. It is a very ancient methodology for hiding private messages from others, but these methods are significantly improved in modern days. In various application confidential data involved and it is transmitted over internet, but these data are not much secure. Therefore to protect data in these applications, it is highly recommended to use the cryptographic methods. The general process of cryptography involving both encryption and decryption is illustrated below in the Figure 1 [1]

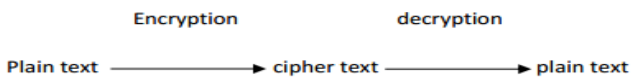

Figure 1 shows Cryptography process

In this proposed work we are evaluating the effectiveness of ECC encryption process and their effect on the encrypted files. In addition of that using the MD5 the ECC cryptographic process is enhanced for fulfilling the need of the hybrid technology development. The proposed encryption architecture is enhanced to provide the strength over the developed cypher text.

II BACKGROUND

Due to fast life style time is much precious than money therefore, to preserve the time banking like services are now becomes mobile. Mobile and internet banking is a way by which banking customers perform banking operations and transactions on his or her cell phone or their laptops. Now in these days this becomes a much popular method of banking, which fits in well with a busy, technical lifestyle. Log on from home computer, or make a phone call is more comfortable for the consumer than having to physically go into a bank.

In the domain of internet and web access phishing is more a kind of attack but due to this attack to a large amount of money and reputation is compromised by the victim. This proposed study work is a study around various kinds of anti-phishing toolbars available over internet and promises to provide the security against phishing attack. In addition of that document includes different aspects of phishing attack, detection techniques, and their solutions and attack types.

Therefore, security issues are very essential for information technology applications (e-commerce application, and Smart

cards). In e-commerce applications the mobile agent can complete the tasks which are assigned by the users. These qualities help physique the mobile agent becomes the most suitable for e-commerce applications. Confidential information is always risky to transfer over an open Internet environment [3]. Therefore a literature collection is provided in the next section of given paper for investigating the security schemes and methodologies that are previously proposed and implemented by various different authors.

III. LITERATURE STUDY

This section includes the various research papers and articles that are providing us guidelines for designing the security system for mobile banking applications.

ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. One of the other recent public key cryptosystems is Elliptic Curves Cryptography use for security. In recent times, the majority of e-commerce applications are designed using asymmetric cryptography to assure the authentication of the concerned parties. ***Sultan et al*** [1] developed a security system and according to that, The Elliptic curve asymmetric cryptography and the results demonstrate that the performance achieved is good. Conversely, an increasing requirement for mobile devices has geared a shift towards mobile e-commerce applications. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC propose equivalent security with smaller key sizes; these result in faster calculation, lower power expenditure, as well as memory and bandwidth savings. ECC is peculiarly useful for mobile devices, which are typically particular in terms of their CPU, power and network connectivity. Elliptic curve-based zero-knowledge proof techniques are powerful tools in such critical applications for providing both security and privacy at the same time in e-commerce applications. The improvement of security is due to the higher complexity of solving the discrete logarithm problem over elliptic curves than over the multiplicative group Zn. This advantage is applicable to all applications, in which the zero-knowledge proof is based on the discrete logarithm over an elliptic curve [1].

A new security requirement for semantically secure encryption strategy, ***Chia-Hui Liu et al*** [3] analyze the security against chosen cipher-text attack. A mobile agent key management and access control scheme with a hierarchy structure. The scheme is based on bilinear pairings over elliptic curves. The advantages of the scheme are: (1) a hierarchy structure which makes it easier to construct Mobile agent; (2) in comparison to Volker and Mehrdad's scheme, repetitive storage of keys is effectively reduced; (3) derivation of the decryption key is relatively simple; (4) effective protection against malicious attack. Therefore, it can effectively provide mobile agents with a secure runtime environment [3].

One of the other Elliptic Curve based key generation for stream cipher is proposed by ***S. Maria Celestin Vigila et al*** [5] for security in e-commerce Application. The key streams are

generated based on the combination of LFSR and cyclic EC over a finite prime field are designed and investigated. The input image and the respective cipher image histograms are conversing. It is seen that cipher image does not have residual information and the histogram is nearly smooth and uniform, offering good security for images. The entropy and the correlation between two neighboring pixels in the input and cipher images are computed and analyzed. The proposed schemes key space is sufficient to resist all sorts of brute-force attacks. Hence the proposed EC based image encryption algorithm is secure against brute force, statistical and correlation attacks. The key file parameters are also encrypted using ECC based technique and sends along with the cipher image. It is difficult for an adversary to determine the key file parameters since the Elliptic Curve Discrete Logarithmic Problem is considered difficult. These factors are used to enhance the security of proposed EC based stream cipher [5].

Ion et al in 2012 examining the security, implementation and performance of ECC applications on various mobile devices, we can conclude that ECC is the most suitable PKC scheme for use in a constrained environment. ECC efficiency and security makes them an attractive alternative to conventional crypto systems, like RSA and DSA, not just in constrained devices, but also on powerful computers. Elliptic curve crypto systems are expected to become the next-generation public key cryptosystems. ECCs require a shorter key length than RSA cryptosystems, which are the actual standards of public key cryptosystems, but provide similar security levels. Because of the small key length, ECCs is fast and can be implemented with less hardware. Although ECC's security has not been completely estimated, it is required to come into widespread use in various fields in the future because of its compactness and high performance when it is hardware-imp lamented. So author examined the security, implementation and performance of some ECC applications on various mobile devices and to compare ECC and conventional PKC performances. That's opinion is ECC could become the next-generation of PKC [6].

Ali Makki in 2012 provides a study according to their studies, there is a computational advantage to be used ECC with a shorter key length than other secure cipher such as RSA. These techniques are more efficient than all ElGamal encryption/decryption scheme and MVECC technique, where it never needs to calculate the inverse operations, by producing one multiplication operation in the encryption and one multiplication operation in the decryption, also it never needs to embed the plaintext as points in the elliptic curve such as used in ElGamal technique [7].

IV LITERATURE SUMMARY

There are various techniques and methods are previously available for providing security in e-commerce applications. Most of them are using the cryptographic schemes for securing the transactions between client and server. This investigation is derived for the mobile banking application. Therefore more security and light weight execution of algorithms are required for designing the security system for mobile applications.

Devices are built with the processing units, memory and power management options. Therefore, the basic computational need can be satisfied using the smart mobile devices. But they are not much capable for execution of large processes and applications that are consuming more battery life and CPU.

V PROPOSED SYSTEM

The proposed work is design and implementation of the security scheme for providing the secure data for security system. In order to secure data there are various cryptographic and hybrid cryptographic schemes are available. But most of the methods are not working in all formats of the data therefore some improvements of the traditional computing is required; therefore some key issues are listed. 1. The problem with the data formats for incorporating with cryptographic approaches. 2. Stenographic approach is not much strong for security point of view; these are easily breakable using small hints. 3. other hand the cryptographic approaches are developed for specific data formats.

The proposed security scheme is based on the cryptographic approach using ECC encryption methodology and the MD5 hash generation algorithm.

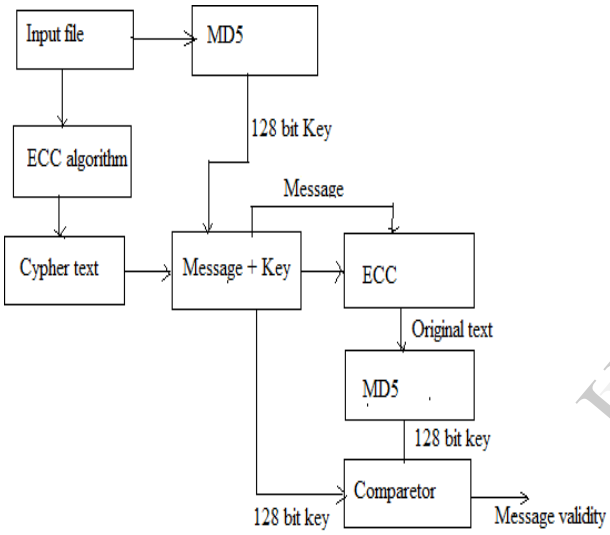

Figure 2 Improved ECC

The propose solution includes the development of security system using traditional encryption scheme (ECC) and the MD5 hash generation algorithm. The private key generation of the ECC algorithm here accept self-generated key for encryption and that key is incorporated with the cypher for secure file exchange.In addition of that the algorithm is able to extract key from the given cypher and cross check the validity of the data.

The diagram figure 2, First of all the system will accept input file and apply on ECC encryption process on the input file and also apply MD5 algorithm that will generate 128 bit key. Both cipher text and 128 bit key will send. Then on decryption side it will get Ciphertext and 128 bit key. Apply ECC decryption process on the cipher text and get original message. Now it will apply MD5 Algo on the message and get 128 bit key. If received 128 bit key and generated 128 bit key are same then massage will accept otherwise massage will discard.

To understand the process of the proposed methodology, first required illustrating the traditional ECC encryption process. The traditional encryption and decryption process is given using figure 3 and 4.

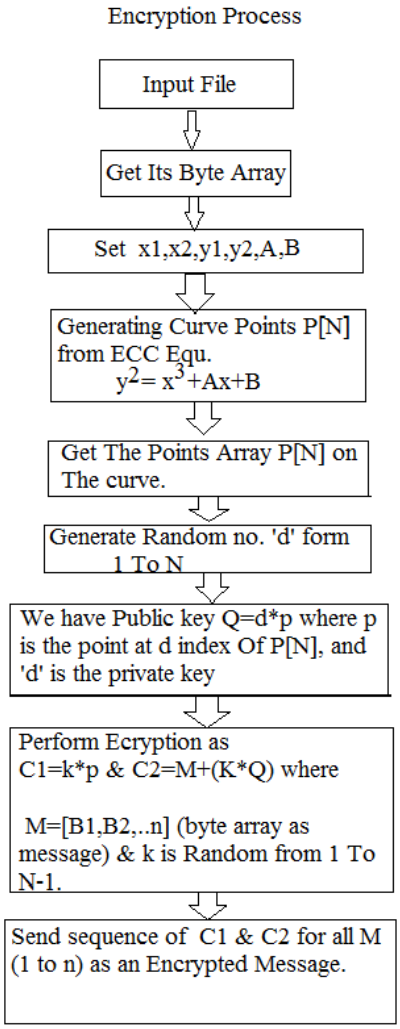

Figure 3 encryption process

If Q= public key

P= a point in curve

d= private key

M= original message

K= random number

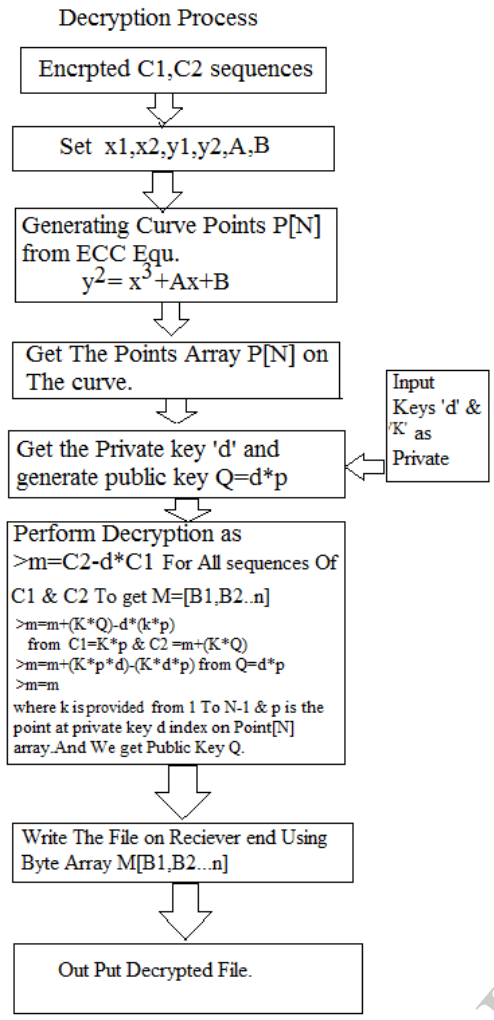

Figure 4 decryption process

Then using above parameters we get the two cypher texts blocks which are denoted using $C_1$and C_2

$$C_1 = K.P$$

$$C_2 = M + KQ$$

Using the above equations the message can be defined as:

$$M = C_2 - d * C_1$$

$$M = C_2 - KQ$$

At the network scenarios the cypher $C_1$and C_2 is sanded on network and the recovery of the original message can be found using the below given expression.

$$M = C_2 - d * C_1$$

$$C_2 - d * C_1 = (M + KQ) - d * (K * p)$$

In next step

$$C_2 - d = M + KQ$$

$$C_2 = M + KQ$$

$$M = M$$

Means the sanded message can be recoverable using the substitution and replacing the cypher context from the delivered messages, where the private key is utilized as the OTP (one time password). The encryption and decryption process for the transaction is given by the figure 2 and 3.

This section of the given paper includes the basic security system design methodology and simple details about the responsibilities of all communicating parties. in the next section draws the conclusion of the given work.

VII CONCLUSION AND FUTURE WORK

In this paper provides an improvement over traditional ECC security algorithm. Using hybrid approach where for enhancing the algorithm ECC and MD5 algorithm is consumed. In place of randomly generation of keys MD5 algorithm is used for key generation. Which enhance the strength of cypher text. In near future the elliptical curve algorithm and proposed hybrid elliptical algorithm is implemented using JAVA framework and the performance analysis is provided using various performance parameters such as storage overhead and computational overhead.

REFERENCES

[1] Better Privacy and Security in E-Commerce: Using Elliptic Curve-Based Zero-Knowledge Proofs, Sultan Almuhammadi, ieeexplore.ieee.org/Xplore/home.jsp
[2] A New Encryption Algorithm over Elliptic Curve, S. Han, E. Chang, W. Liu, ieeexplore.ieee.org/Xplore/home.jsp
[3] Access Control and Key Management Scheme based on Bilinear Pairings over Elliptic Curves for Mobile Agent, 1 Chia-Hui Liu, 2 Yu-Fang Chung, ieeexplore.ieee.org/Xplore/home.jsp
[4] An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography, Mrs. S. Prasanna Ganesan, ieeexplore.ieee.org/Xplore/home.jsp
[5] Elliptic Curve based Key Generation for Symmetric Encryption, S. Maria Celestin Vigila1, K. Muneeswaran2, 2011 IEEE,
[6] Elliptic Curves Cryptosystems Approaches, Ion TUTANESCU, Constantin ANTON, Laurentiu IONESCU, Daniel CARAGATA, 2012 IEEE
[7] Elliptic Curves Cryptographic Techniques, Ali Makki Sagheer 2012 IEEE