An Efficient Implementation For Key Management Technique Using Smart Card And ECIES Cryptography

Neha gupta[1] and Harsh Kumar Singh[2] and Anurag jain[3]

[1,2,3]Department of Computer Science, RITS Bhopal, M.P(India)

ABSTRACT

A Elliptic curve cryptosystem are become popular because of the reduced number of keys bits required in Comparision to other cryptosystem. In existing work ECC technique are used to describe the encryption data to provide a security over a network. ECC satisfy the Smart cards requirements in term of memory, processing and cost. In existing work ECC cryptographic Algorithm work with a smart card technique. Many existing approaches work with smart card with various Technique and produce a better efficient result. In these review paper, we Define a smart card technique using a ECIES cryptographic algorithm. So These Technique key management using smart card and ECIES.ECC basically based on a discrete logarithm over appoint on an elliptic curve. The ECIES is standard elliptic curve that is totally based on encryption algorithm. Smart Card using ECIES technique in key management technique.

KEYWORDS

ECIES, elliptic curve, encryption, Decryption, public key cryptography, Smart card, java card.

1. INTRODUCTION

In Public key cryptography several cryptosystems have been proposed. Mainly Security and efficiency are the most important features to be requested to any cryptosystem. Generally both characteristics depend on the mathematical problem on which it is based The most extended encryption scheme in ECC is the Elliptic Curve Integrated Encryption Scheme (ECIES). In other word Smart card is a plastic card that contain a microchip in which a lot of information about the user. Generally Smart Card have their stored data can be protected against unauthorized access and tampering. Smart card is considered to be ideal cryptographic token. Smart Card based on key management and key authentication .It consider a registration phase, login phase, Authentication/verification phase, password change phase. To generate a smart card we follow a some step In first stage ,first is registration phase, Login phase, verification phase, password change phase. In registration phase we generate a hash value through a hash function, that is a master key. In login phase user provide a facility a to secure a login, through a user id and password which generate by a registration phase. In verification phase user receiving a login request message. In password change phase if user want to change the password PW with a new password PW new, then user U insert the smart card to the card reader/client machine and keys in ID* and PW* and request to change password. The most extended encryption scheme in ECC is the Elliptic curve integrated encryption Scheme (ECIES). The Elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. ECIES is a public key encryption algorithm like ECDSA.ECIES for portable devices, Application and for the future

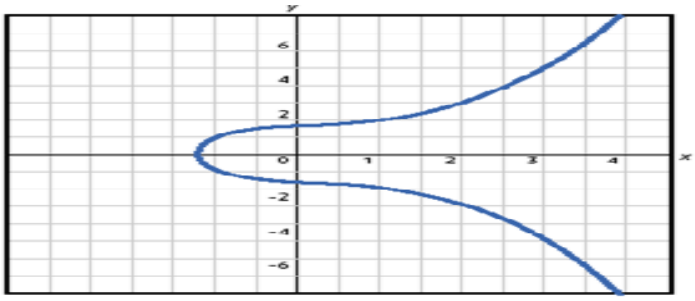
DOI : 10.5121/ijctcm.2013.3603

and this, in the end, is the reason ECIES is a stronger option than the RSA and discrete logarithm systems for the future.

1.1. Characteristics Of ECIES

(a). ECIES provide a security for a given key size.
(b). ECIES provides secure and efficient hash techniques.
(c). ECIES are totally based on the elliptic curve, in which the smaller key size make also possible combination. it provide a faster cryptographic operations run on smaller chip, that is smart card.

An elliptic curve is defined in a standard mathematical form. It define a two dimensional x, y Cartesian coordinate system by an standard elliptic equation of the form: $y^2 = x^3 + ax + b$. The graph turns out to be gently looping lines of various forms. Generally key management scheme based on a encryption key for secure the channel over the network. Mainly Communication parties used a pair wise key used to secure a channel, for direct and indirect communication .In Cryptography, almost all of the encryption techniques are dependent on the key, so key management is the basis for a security mechanism. Key management is the vital component but it is also a weak link. Key management Life cycle generally includes User registration, user initialization, key generation key installation, key registration, key backup, key update, key recovery, key revocation.



2. WORK ACCOMPLISHED SO FAR

Researcher are continuously working on **Key management scheme using Smart card,** Very few of them are described here:-

(a) Patrick George states that[2],Smart card are provide a separation between a platform and user. It provide a trustworthiness relationship between a user and server.TPM(trusted platform module) authorization protocol in order to implement smart card based user access control to TPM protected resources.

The TPM or smart card demonstrate physically separate the platform credentials stored in TPM which stored in smart card, then generate a TPM and smart card cooperative model. The first model generally introduced a general purpose model. and provide a same service as smart card. Other model simply the implement TPM with smart card. But TPM or Smart card are provide a single storage point both user and platform. These "*TPM-and-smartcard*" model is based on the strict separation between user and platform credentials, and on the tight integration of smart cards into TPM user authorization protocols. The "*TPM-and-smartcard*" model is based on the strict

separation between user and platform credentials, and on the tight integration This model presents the TPM working together with smart cards. In their day-to-day activities, users are interacting more and more with many different computing environments, even to perform the same operation. For example, a user may send business e-mails from different PCs (business, home, Internet-cafe) or from different types of devices (PC, PDA); under these circumstances the user will use the same credential on different platforms, the ones attached to e-mail digital signature issued by the corporate MIS. It is clear that, in this case, storing this credential inside a non-removable device, such as the platform TPM, is impracticable and will raise issues when the user switches to different platforms. User authentication in TCG in which authorization the data and protocol. In these paper future work defined a additional synergies in TPM and Smart Card. These smart card stored a user secret information and credential, and enhanced the digital signature to secure a communication.

(b)A.K. Awasthi & Sundar lal States that[3] it proposed a new remote user authentication scheme using smart card. Masquerade Attack is successful in this scheme. Some researchers point out a different type of attack on this scheme & presented a modified scheme to remove these effects. Recent research have suggested idea of check digit to overcome the above attack. A no. of remote password authentication scheme with smart card have been proposed since then. These new remote user authentication scheme based on a cryptosystem. in these scheme it allow a valid user login on remote server and access the services which provided by a remote server. The researcher Awasthi and Lal also proposed scheme which also remove a threats. In these proposed work it proposed a Initial phase, registration phase, login phase and authentication phase. Firstly user registered and login through a user id and password and issues a smart card. These smart card holding user related information through a secure channel. user insert a smart card into a device and keys the password. Some attack are described in these paper. Such as Chan & Cheng's attack, Shen-lin-Hwang's attack and Chang & Hwang's attack:

Chan & Cheng equation is :

$$IDj = (IDb \; \square IDb) \bmod p.$$

Is modified to

$$IDj = (IDb)r \bmod p.$$

Where r is a arbitrary integer.

These new remote user authentication scheme is modified form of Hwang-li's scheme and uses one more function CK to generate a check bits for registered identity. If customer id and check digit are same(XOR) then condition processed otherwise rejects. in this paper result is incomplete still it is essential to obtain the check bits corresponding the ID. In these conclusion These scheme is more essential then the other scheme. It provide a secure scheme against a both type of attacks: Attack via registration phase and attack via authentication phase.

(c)B. Baker[4] states that The world wide web has become the de facto interface for consumer oriented electronic commerce. So the interaction between consumer and merchants is mostly limited to providing information about product and credit card based payments for mail orders. These scheme describe the design of new three party authentication and key distribution protocols. The authentication protocol features three parties: A client(Consumer), A server(the service provider), and a trusted third party(the smart card issuer. e.g bank).Some elements are describe such as Identificators (both client and user use to prove their identity), trusted third

party(the issuer of identificators), Semi trusted computing based(secure application runs in this environment).A trusted third party not need to give a any response before both client and server not authenticated. The kryptoknight protocol need to calculate the authentication code over messages. The kryptoknight protocol all the TTP(trusted third party) generate session key and distribute it to a server and client over a network. In these new algorithm scheme, a different distribution scheme, in which proposed party A generate a session key, transports it encrypted (via party B) to the TTP, which decrypts the key and finally send to party B, and then party B Reencrypted with a key known to B. So in this case the session key is transported (from A to B) rather than distributed (from the TTP to A and B). A and B generate cryptographic proofs before contacting the trusted third party. In the same effort the session key can be generated as well: party A generates session key KAB with the same parameters as proof PAK it sends to the TTP. The basic KLOMP protocol has been designed to be implementable with any challenges/response capable Identificator. With some Identificators the protocol can be enhanced for better security. In this scheme for testing purpose also a password based challenge/response identificator has been built. The smart card access code has been applied in project for the LISV. User easily register and login to the HTTP based application by entering their chipper and chip knip card.

(d) Rajaram Ramasamy and Amutha prabakar Muniyandi states that[5] In this scheme it proposed that efficient password authentication with smart card applying RSA. These proposed scheme define a maximun attacks with minimum computational cost. Remote user authenticaton using smart card is a good solution for any e-based applications.To access resources at remote system, user should have proper access rights. One of the simplest and efficient mechanism is the use of a password authentication scheme. To access the resources user should have own user ID and PASSWORD. This work propose an efficient password authentication scheme with smart card using RSA. In these proposed scheme has three phase Registration phase, Authentication Phase, and login Phase.In these proposed scheme security issues The attacker cannot create or update the false information for login. In proposed scheme, if login request is rejected three time then automatically the user account is locked and the user has contact server to unlock the account. The proposed protocol overcomes the DOS attack over the computation power of the server. In these proposed scheme if the smart card of user are lost the adversary cannot use this card without knowing the password of the user. if any case adversary want to change the password he/she must know the original password.

Some Security Analysis in these scheme:

(i) Denial of service attack
(ii) Parallel Session Attack
(iii) Smart card loss attack.

These proposed scheme has high time complexity and that improved security level from already existing scheme. The proposed scheme restricts most of the well known attacks with the reasonable Computational cost. Server not need to maintain a password table,instead it to maintain onlt registration time of every user. This work reduce the server overhead of maintaining large user data for authentication.

3. PROPOSED METHODOLOGY

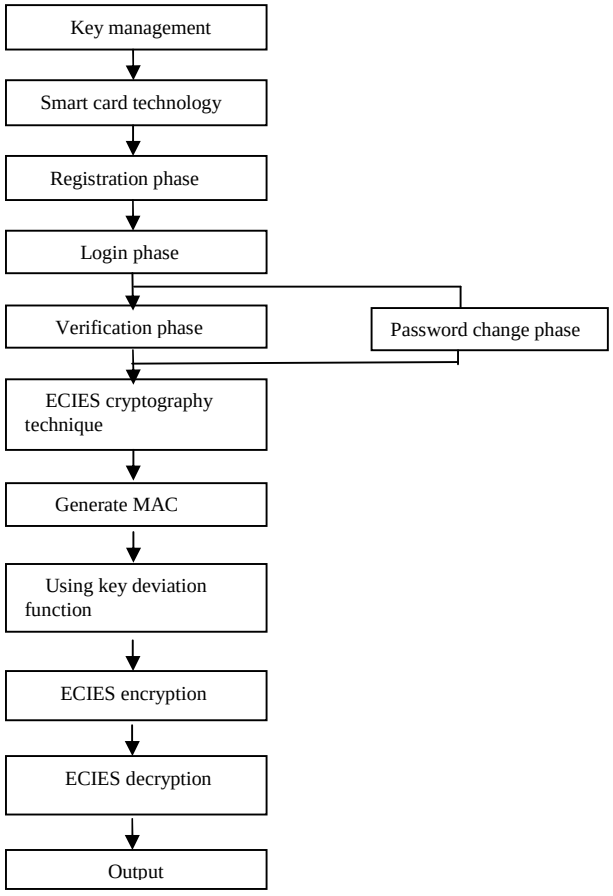
3.1. KEY MANAGEMENT LIFE CYCLE:

1. user registration
2. user initialization

3. key generation
4. key installation
5. key registration
6. key update
7. key de-registration and destruction
8. key recovery
9. key revocation

3.2. Smart Card based key management and authentication

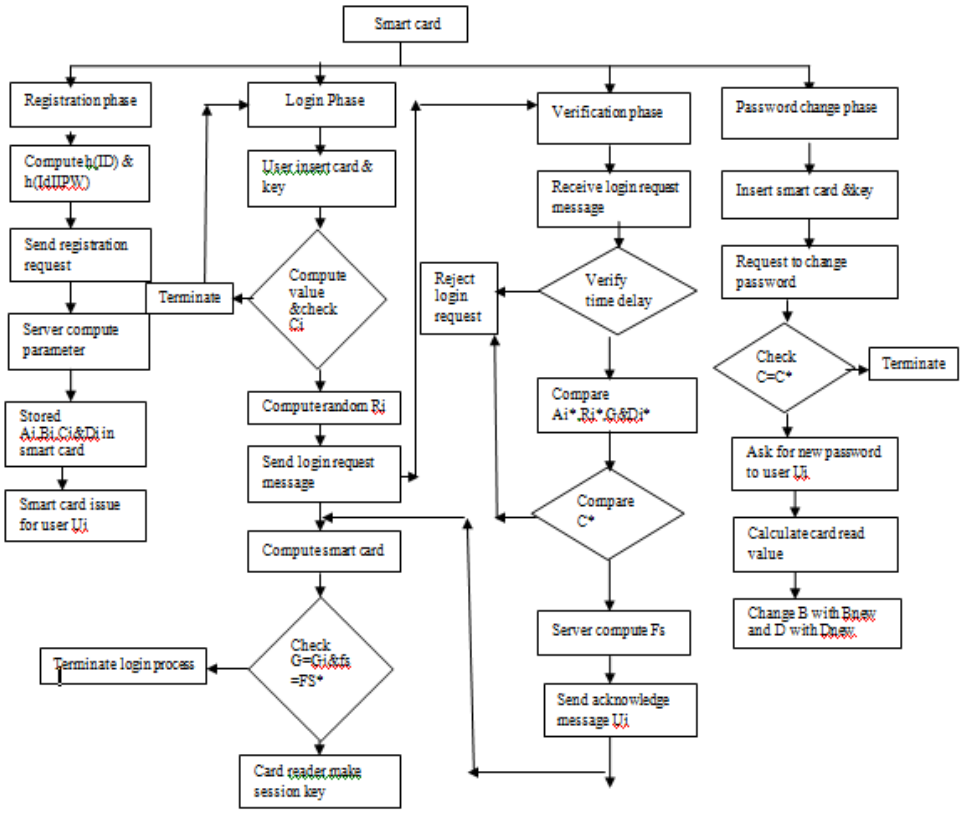
1-Registration phase
2-Login phase
3- authentication/verification phase and
4-password change phase.



Fig(b):Key management process using smart card

The notations use in proposed scheme and phases are describe below-The Notations are:

U – Remote User
ID – Identity of User
PW– password chosen by User
S– Remote authentication Server
X– Permanent secret key of S
H (·) – One-way hash Function
xor – Bitwise XOR operation
|| – concatena



Fig(c):Flowchart of phases smart card

3.3. ECIES

ECIES is a public-key encryption algorithm where there is assumed to be a set of domain parameters(K,E,q,h,G).with these parameters, we also add a choice of symmetric encryption/decryption functions which we shall denote Ek(m) and Dk(c).The use of a symmetric Encryption function makes it easy to encrypt long messages. in addition instead of a simple hash function. we require two special Types of hash function: A message authentication code MAC k(c)

MAC: {0.1}^n * {0,1}^* → {0,1}^m

This Acts precisely like a standard hash function expect that it has a Secret key passed to it as well as a message to be hashed

A key derivation function KD(T,1)

KD : E * N → {0,1}^*

A key derivation function acts precisely like a hash function except that output length could be quite large. The output is used as a key to to encrypt a message hence if the key is to be used in a xor-based encryption algorithm the output needs to be as long as the message is being encrypted. The x-or based encryption requires key derivation and the MAC function to encrypt the message on the basis of x-or operation on bits. The ECIES scheme works like a one-pass Diffie Hellman key transport, where one of the parties is using a fixed long term rather than an ephemeral one. This is followed by symmetric encryption of the actual message. For example the combined length of the required MAC key and the required key for the symmetric encryption is given by l. The recipient is assumed to have a long-term public /private key pair

(Y,x) where Y=[x]G

3.3.1. ECIES Encryption:

INPUT: Message m and public key OUTPUT: The ciphertext (U,c,r)
1. Choose k € R(1…….q-1)
2. U ← [k]G
3. T ← [k]Y
4. (k1||k2) ← KD(T,l)
5. Encrypt the message c ← Ek1(m)
6. Compute the MAC on the ciphertext r ← MACk2(c)
7. Output (U,c,r)

3.3.2. ECIES Decryption:

INPUT: Ciphertext (U,c,r) and a private key r. OUTPUT: The message m or an 'invalid ciphetext' message.
1. T ← [x]U
2. (k1||k2) ← KD(T,l)
3. Decrypt the message m ← Dk(c).
4. if r ≠ MACk2(c) then output 'Invalid Ciphertext'
5. output m.

4. COMPARISION BETWEEN EXISTING WORK AND PROPOSED WORK

In existing work,it use a smart card technology based on remote user authentication scheme. In proposed work, we use a smart card technology based on ECIES cryptography algorithm. Both existing and proposed work using a one way hash function which generate a hash value and bitwise exclusive OR operation. Generally smart card key management and authentication have four phase: registration phase, login phase, authentication phase/verification phase & password change phase. In existing work, it used a remote user authentication scheme against a denial attack and stolen smart card etc. In other word proposed work consist a ECIES algorithm to provide a encryption and decryption technique. It convert a plain text into a cipher text & vice versa. ECIES a public key encryption technique. It provide a secure message passing between a

network. ECIES encryption algorithm provide a secure and efficient hash technique. It is based on elliptic curve & it contain a smaller key size make possible combination.

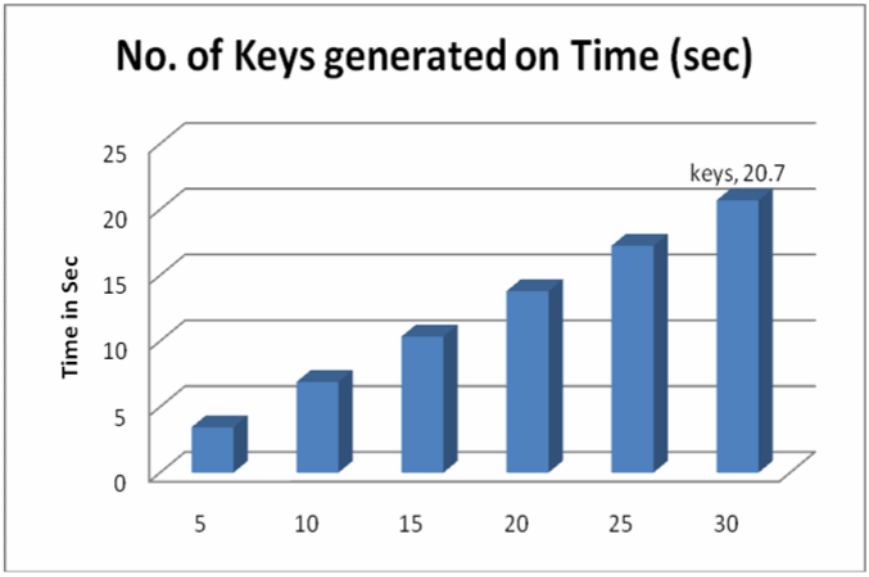
5. RESULT ANALYSIS

Public key	Signature time	Time to encrypt	Time to decrypt	Storage
0.53 sec	0.64 sec	4.9 sec	3.82 sec	63 bytes

Table 1: Various Steps take time in sec.

Replay attack	Insider attack	Outsider attack	Eavesdropping	Password based attack	Man-in the middle attack
YES	YES	YES	YES	YES	YES

Table 2: Various Attacks Prevent in technique



Fig(d):No.of key comparision in Sec.

Storage/ scheme	Our scheme	R. song al et.
Smart card	480 bits	320 bits
Server	160 bits	480 bits

Table 3:Comparision between existing and proposed work

6. CONCULSION

In These proposed work smart card work efficiently with the ECIES Cryptography technique. In These paper we use a smart card based key management and authentication technique. In which smart card authentication stage contains a registration phase, login phase, registration phase, and password change phase and using a ECIES public key encryption algorithm. These algorithm define a symmetric encryption and decryption function. These proposed scheme provide a better efficient result and secure a network.

7. REFERENCES

[1] Swarn Sanjay Sonwanshi,Ram ratan ahirwal,Yogendra kumar jain"An efficient smart card based remote user authentication scheme using hash function",IEEE ,conferences on electrical,electronics and computer science,2012.

[2] Patrick george "user authentication with smart card in trusted computing architecture"Gemplus.

[3] A.k.awasthi and S.lal,"A remote user authentication scheme using smart card with forward security",IEEE transactions on consumer Electronics,Vol.49,.no.4,pp,1246-1248,2003.

[4] B.Baker "Mutual Authentication with smart card"Delft university of technology,Chicago,Illinois,USA,may 10-11-1999.

[5] R. ramasamy and Amutha prabakar Muniyandi"An efficient password authentication scheme for smart card",international journal of network security ,vol.14,no.3,pp 180-186,may 2012.

[6] R. ramasamy and Amutha prabakar Muniyandi"new remote Mutual Authentication scheme using smart card"transaction on data Privacy 2(2009) 141-152.

[7] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. Consumer Electron., vol. 46, pp. 992-993, 2000.

[8] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," Computers and Mathematics with applications, vol. 26, No.7, pp. 19-27, 1993.

[9] C. C. Chang and K. F. Hwang, "Some forgery attack on a remote user authentication scheme using smart cards," Infomatics, vol. 14, no. 3, pp.189 - 294, 2003.

[10] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," IEE Proceedings-E, vol. 138, no. 3, pp. 165-168, 1993.

Authors

Neha Gupta received the B.E degree in Computer science from RGPV university, Bhopal, India in 2009,And the M.TECH pursing in Computer science & engineering From RITS, RGPV, Bhopal.

Harsh Kumar Singh received the B.E degree in information technology from RGPV university, Bhopal, India, In 2006,and the M.TECH degree in computer science & engineering from MANIT university, Bhopal, India in 2011.He is a currently a Asst. Prof. in RITS Bhopal, India. His current research interests include wireless sensor network, time synchronization.

Mr.Anurag Jain is a associate Professor and head of the department of CSE in Radharaman institute of technology & science Bhopal.He is also the dean academics RITS. Anurag Jain has completed his M.tech(IT),He is also pursing Phd.in RGPV university. He is 12 year teaching experience and area of interest including network security. TOC, data structure, OOPs, Basic computer, Complier design. He is organized and attend several national and international conferences.He also published 36 international journal paper and 2 national paper. He is also published a book of basic computer engineering.He is life member of CSI(Computer socity of india).

INTENTIONAL BLANK