Novel Secured Digital Payment Gateway with Dynamic Password on Multiple Private Keys (PIN) connecting SET Protocol on ECC in E-Commerce Applications

Anjaneyulu G.S.G.N[1], Narendra Mohan. L[2*]
[1, 2] Department of Mathematics, SAS, VIT University, Vellore, Tamilanadu-14, India
Corresponding Author*: mohannarendra3@gmail.com, ,

ABSTRACT: In this paper, secured online digital payment gateway model for e-commerce applications is intended and fabricated. This depicts a real time application scheme on Elliptic Curve Cryptography under the structure of SET protocol, which includes both digital signature and cryptosystem. The novelty in this gateway is dynamic password, which will be generated on again a dynamic PIN, which in turn is initiated by the customer for each transaction. This dynamic password finally completes the transaction. And also, this improvement includes two Confirmation algorithms for implementation of ECC that assures complexity and security. At the end, secure implementation of SET protocol over ECC for online payment gateway is presented, which ensures the validity, confidentiality, integrity and non-repudiation of transaction. Security analysis like attack on DLP, attack on Hash function is also given to strengthen the architecture.

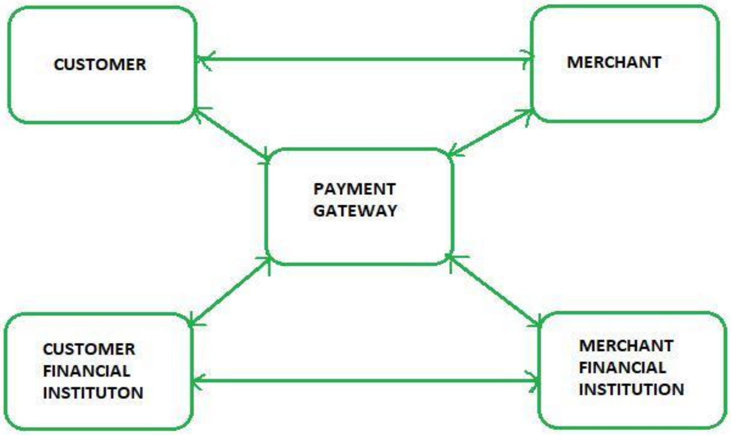
Keywords: Secure Electronic Transaction Protocol, Elliptic Curve Cryptography, Digital Signature, Secure Transaction.

1. INTRODUCTION

E-commerce is basically the concept of exchanging online authenticated information to sell their products or render the services to their clients, so the security of transaction is more and more significant. The businesses and consumers are both draw at most attention to build a security E-commerce platform. And SET (Secure Electronic Transaction) protocol is a security protocol adopted in Ecommerce [1], it's more important to provide the confidentiality and security of information by suitable encryption algorithm and digital signature. SET protocol is designed to settle the transaction by bank cards between consumers and Digital Merchants. It involves the encryption [15, 16, and 17], digital signature and envelope. And the encryption and signature is usually used in every phase. The operation patterns of purchasing commodity online as follows: When Users find the commodity and want to shopping by SET, Merchant will require the Users to place order, then users exchange information with Merchant by password in order to verify the validity of Merchant; Users send order and require of payment to Merchant, and Merchant transfer his information and SET certificate to Bank, then waiting for the request; The bank check these certificates to verify the validity of Users and Merchant; Finally, Merchant confirms the order, then require the bank to withdraw these transaction [5,12,13]. Certificate is a core in the process of transaction, and the certificate is issued by CA (Certificate Authority). In this paper we also introduce new authenticated technique as dynamic password and multiple pins for transaction of money and online transaction. This pin is instant pin that can be changed multiple times and password can be generating once with less period of time in each transaction. This technique is additional security is given in this paper comparative to exiting algorithm. Here we also implement ECC, ECDSA for ordering and transacting commodities through SET protocol in E-commerce.

1.1 SECURE ELECTRONIC TRANSACTION (SET) PROTOCOL

Secure Electronic Transaction or SET is a system, which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Master Card, Microsoft which provided its Secure Transaction Technology (STT) and Netscape which provided technology of Secure Socket Layer (SSL). SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification of Authorities for making use of standard Digital Certificates like X.509 Certificate [18, 19, and 20]. Before discussing SET further; let‟s see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.



1.2.1. Requirements in SET:

SET protocol has some requirements to meet, some of the important requirements are:

i. It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.

ISSN: 2233-7857 IJFGCN

ii. It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
iii. It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
iv. SET also needs to provide interoperability and make use of best security mechanisms.

1.2.2. Participants in SET :

In the general scenario of online transaction, SET includes similar participants:

i. Cardholder: customer
ii. Issuer: customer financial institution
iii. Merchant
iv. Acquirer: Merchant financial Department
v. Certificate authority: Authority which follows certain standards and issues certificates (like X.509V3) to all other participants [24, 25].

1.2.3. SET Functionalities :

(a) Provide Authentication

i. Merchant Authentication: To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.

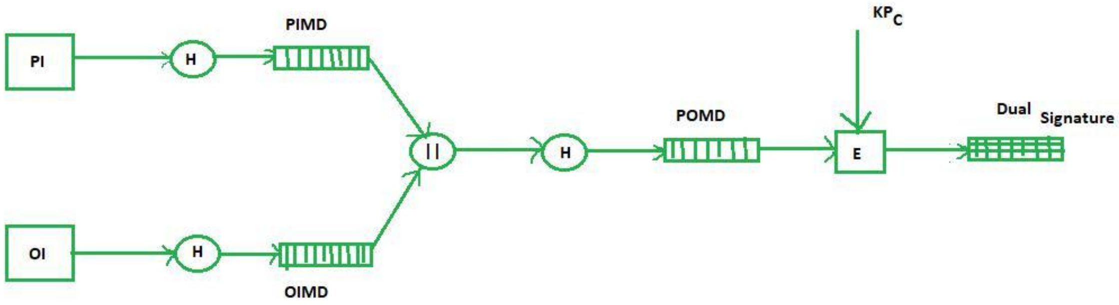
ii. Customer / Cardholder Authentication: SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.

iii. Provide Message Confidentiality: Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.

iv. Provide Message Integrity: SET doesn‟t allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1 [26, 27].

(b) Dual Signature:

The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers: Order Information (OI) for merchant Payment Information (PI) for bank You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible [12,15] . Here is the generation of dual signature:



Where,

PI stands for payment information
OI stands for order information
PIMD stands for Payment Information Message Digest
OIMD stands for Order Information Message Digest
POMD stands for Payment Order Message Digest
H stands for Hashing
E stands for Public Key encryption
KPc is customer‟s private key
||stands for append/Concatenation operation

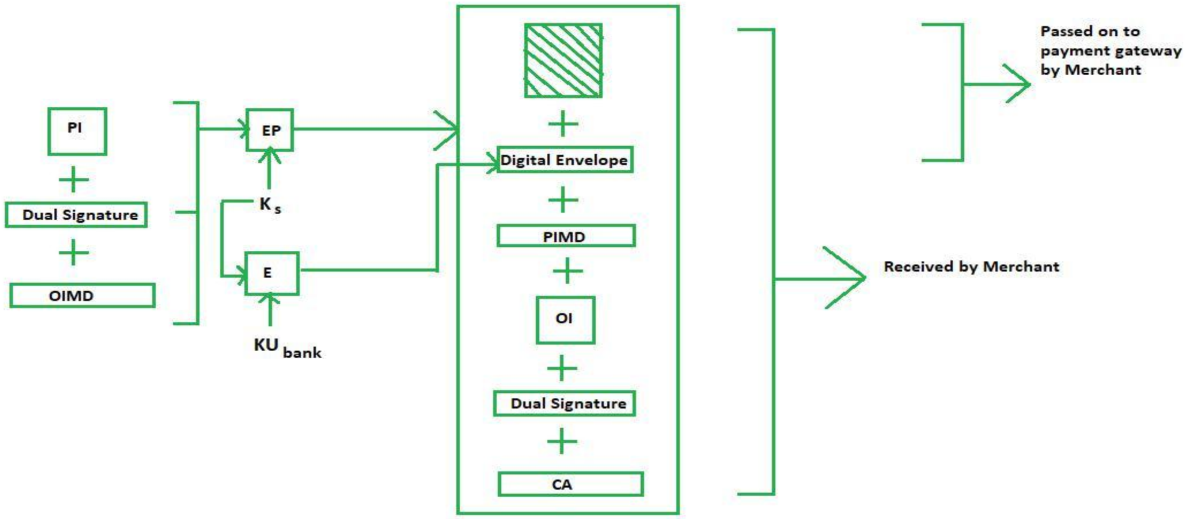
Dual signature is DS = E (KPc, [H (H (PI) || H (OI))])

(c) Purchase Request Generation:

The process of purchase request generation requires three inputs:

- Payment Information (PI)
- Dual Signature
- Order Information Message Digest (OIMD)

The purchase request is generated as follows:



Where,

PI, OIMD, OI all have the same meanings as before

The new things are:

EP which is symmetric key encryption

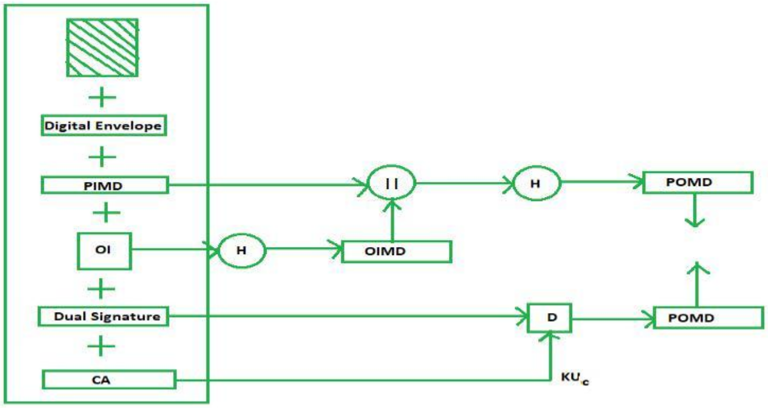
Ks is a temporary symmetric key

KU bank is Public key of bank

CA is Cardholder or customer Certificate

Digital Envelope = E (KU bank, Ks) [21, 23, 29]

(d) Purchase Request Validation on Merchant Side:



4

ISSN: 2233-7857 IJFGCN

The Merchant verifies by comparing POMD generated through PIMD hashing with POMD generated through decryption of Dual Signature as follows:
Since we used Customer private key in encryption here we use KUc which is public key of customer or cardholder for decryption„D‟ [22, 28, 30].

Payment Authorization and Payment Capture:

Payment authorization as the name suggests is the authorization of payment information by merchant which ensures payment will be received by merchant. Payment capture is the process by which merchant receives payment which includes again generating some request blocks to gateway and payment gateway in turn issues payment to merchant [31].

1.2. DIGITAL SIGNATURE

The term digital signatures encompass many varieties of "signatures". Electronic signatures are simply an electronic confirmation of identity. This definition is deliberately broad enough to encompass all forms of electronic identification, from biometric signatures such as iris scans and fingerprints to non-biometric signatures, such as digital signatures. Electronic signatures can be further subdivided into the highly secure and the insecure. Digital signature must serve the same essential functions that we expect of documents signed by handwritten signatures, namely integrity, nonrepudiation, authentication and confidentiality. In the digital realm, integrity means ensuring that a communication has not been altered in the course of transmission. It is concerned with the accuracy and completeness of the communication. The recipient of an electronic communication must be confident of a communication's integrity before she can rely on and act on the communication. Integrity is critical to ecommerce transactions, especially where contracts are formed electronically. The process of digitally signing starts by taking a mathematical summary (called a hash code) of the check. This hash code is a uniquely-identifying digital fingerprint of the check. If even a single bit of the check changes, the hash code will dramatically change. The next step in creating a digital signature is to sign the hash code with your private key. This signed hash code is then appended to the check. How is this signature? Well, the recipient of your check can verify the hash code sent by you, using your public key. At the same time, a new hash code can be created from the received check and compared with the original signed hash code. If the hash codes match, then the recipient has verified that the check has not been altered. The recipient also knows that only you could have sent the check because only you have the private key that signed the original hash code.

1.3. DEFINITION OF ELLIPTIC CURVE CRYPTOGRAPHY

Since the discovery of RSA (and El-Gamal) their ability to withstand attacks has meant that these two cryptographic systems have become widespread in use. They are being used every day both for authentication purposes as well as encryption/decryption. Both systems cover the current security standards–so why invent a new system? Even though ECC [2, 8] is relatively new, the use of elliptic curves as a base for a cryptographic system was independently proposed by Victor Miller and Neil Koblitz [4, 7]. What makes it stand apart from RSA and El-Gamal is its ability to be more efficient that those two. The reason why this is important is the developments in information technology–most importantly hand held, mobile devices, sensor networks, etc. Somehow, there must be a way to secure communications generated by these devices; however their computing power and memory are not nearly as abundant as on their desktop and laptop counterparts. A contemporary desktop or laptop system has no problems working with 2048 bit keys and higher, but these small embedded devices do since we do not want to spend a lot of their resources and bandwidth securing traffic.

The operations on which RSA are founded are modular exponentiation in integer rings. The security of RSA depends on the difficulty of factoring large integers which can be done in sub-exponential times. For the ECDLP however, only exponential algorithms are known which means we can use shorter keys for security levels where RSA and El-Gamal would need much bigger keys. For example, a 160 bit ECC key and a 1024 bit RSA key offer a similar level of security. To reach the same level of security than a 15360 bit RSA key, one only needs 512 bit ECC key. There are many communications in SET protocol, usually, the data will be encrypted by symmetrical encryption algorithm, and adopt public encryption algorithm to digital signature and envelop, finally, convey the information by public encryption algorithm. Public key systems depend on the use of some sort of invertible mathematical function. The complexity of calculating these functions may not scale linearly with the number of bits in the key but grow more rapidly than that. Thus, the key size must be large enough to make brute-force attack impractical but small enough for practical encryption and decryption. In SSLlTLS protocol, RSA is recommended. As we have seen, the bit length for secure RSA use has increased over recent years, and has put a heavier processing load on applications using RSA. There are several ways of defining equations for elliptic curves [9], which depend on whether the field is a prime finite field or a characteristic two finite field. In this paper, we will only discuss elliptic curve cryptography based on a prime finite field which is defined as follows.

Let Fp be a prime finite field so that p is an odd prime number, and let a, b ∈ Fp, satisfy $4a^3 + 27b^2 \neq 0 \pmod{p}$. Then an elliptic curve E (Fp) over Fp defined by the parameters a,b ∈ Fp consists of the set of solutions or points P = (x, y) for x, y ∈ Fp to the equation:

$$y^2 = x^3 + ax + b \pmod{p}$$

Together with an extra point 0 called the point at infinity. For a given point P = (x_p, y_p), x_p is called the x - coordinate of P, and y_p is called the y - coordinate of P.

The addition operation in E (Fp) is specified as follows:

(l) P+O = O+P = P for all P ∈ E (Fp).
(2) If P = (x, y) ∈ E (Fp), then (x, y) + (x,-y) =O.
(3) Let P = (x_1, y_1) ∈ E (Fp) and Q = (x_2, y_2) ∈ E (Fp), Where P ≠ ± Q, Then P + Q = (x_3, y_3)

where $x_3 = \lambda^2 - x_1 - x_2 \pmod{p}$, $y_3 = \lambda (x_1 - x_3) - y_1 \pmod{p}$ and $\lambda =$ ——.

(4) Let P = (x_1, y_1) ∈ E (Fp), Then P + P = 2P = (x_3, y_3), where $x_3 = \lambda^2 - 2x_1 \pmod{p}$,

$y_3 = \lambda (x_1 - x_3) - y_1 \pmod{p}$ and $\lambda =$ ——.

1.3.1. Point Multiplication

In point multiplication a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point L on the same elliptic curve, giving kP=L. Point multiplication can be achieved by two basic elliptic curve operations, namely point addition and point doubling. Point addition is defined as adding two points P and L to obtain another point R written as R=P+L. Point doubling is defined as adding a point P to itself to obtain another point L so that L=2P. Point multiplication is hence achieved as follows: let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point L on the curve so that L=kP. I.e. Elliptic curve point multiplication is defined as

$$[k]P = \{P + P + \cdot\cdot\cdot + P\} \text{ for k summands}$$

$$\text{If } k=23 \text{ then } kP=23P=2\,(\,2\,(\,2\,(\,2P\,)+P\,)+P\,)+P.$$

Thus point multiplication uses point addition and point doubling repeatedly to find the result.
The above method is called the 'double and add' method for point multiplication.

There are other, more efficient methods for point multiplication. The main attraction of ECC compared to RSA is that the best algorithm known for solving the elliptic curve discrete logarithm problem takes fully exponential time. On the other hand, the best algorithms known for solving the underlying hard mathematical problems in RSA and DSA (the integer factorization problem, and the discrete logarithm problem, respectively) take sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with equivalent levels of security [10].

1.3.2. Elliptic Curve Example:

Elliptic curve general form:

$$qy^2 = rx^3 + ax + b + sx^2 + ty$$

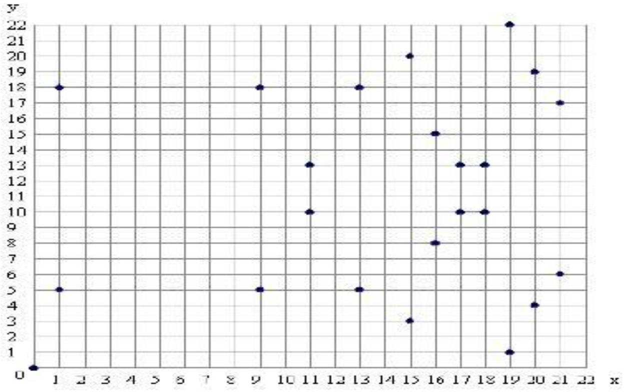
We want the set of solutions (x, y) to the equation

$$y^2 = x^3 + ax + b \text{ where } 4\,a^3 + 27\,b^2 \neq 0$$

Example: (p=23, n=2, a=1, b=0) and Set p = 23, y^2 mod p = x^3 + 1x + 0 mod p.
Observe $4a^3 + 27b^2$ mod p = 4 ≠ 0
Choose G = (9, 5) (on curve: 25 mod 23 = 729+9 mod 23)

There are 23 points on this curve:

(0, 0) (1, 5) (1, 18) (9, 5) (9, 18)
(11, 10) (11, 13) (13, 5) (13, 18)
(15, 3) (15, 20) (16, 8) (16, 15)
(17, 10) (17, 13) (18, 10) (18, 13)
(19, 1) (19, 22) (20, 4) (20, 19)
(21, 6) (21, 17)



Elliptic Curve Equation: $y^2 = x^3 + x$

1.3.3. Notations & Operations used in ECC:

GROUP	**F $_P$ ***	**E(F $_P$)**
Group Elements	Integers{0,1,2,----- , n-1}	Points (x , y) on Elliptic curve and operation +
Group Operation	Multiplication modulo P	Addition of point in pairs
Notation	Elements : g , h	Elements : P , Q
	Multiplication : g.h	Addition : P + Q
	Inverse : g^{-1}	Negative : -P
	Division : g/h	Subtraction : P - Q
	Exponentiation : g^K	Multiple : kP
Discrete Logarithm Problem	Given g ∈ Fp and	Given P ∈ E (Fp) and
	$y = g^K$ mod n then find k	L = kP then find k

1.4 OUTLINE OF THE PAPER

In this paper we discuss concept of digital signature in section-1.2 and information of Elliptic Curve Cryptography in section-1.3 [10] and then we go for implementation ECDSA [11]. We should select suitable encryption algorithm to provide the confidentiality, integrity, authentication and non-repudiation of information. In this paper, the main idea of applications using elliptic curve cryptography for payment gate way through ECC for secure transaction in section-3. Then, we will discuss algorithm for payment gateway with flowchart in section-3.3, and presented soundness of algorithm in section-4. Finally we have given security attacks like attacks on ECC; attacks on ECDSA are given in section-5 to strengthen architecture.

2. MATHEMATICAL INFRASTRUCTURE FOR PROPOSED PROTOCOL

2.1. Complement Operator (~): Let x_1 be an integer in Z_p. Now, this integer x_1 is converted in to binary system and then apply bitwise compliment operator which is a unary operator (works on only one operand). It changes 1 to 0 and 0 to 1 in the binary form of $x_{1.}$ This binary number will be again converted in decimal form, which is also an integer and is defined as complement of $x_{1.}$ This is denoted by .

2.2. Pin Generation: Let Z $_p$ = {1, 2, 3, ----, Pp1} be a Group with respect to mltiplication modulo P. Let a, b, c ε Z_p , now we define "d" as private parameter along with a,b, c and define as follows. Definitely this insertion in to the algorithm will provide more security for on line payment gateway. This is novel on line secured payment gateway on multiple private keys a, b, c, d ε Z $_p$.

d = {

2.3 Auto Generated Pin: This is completely new and highly secured for ATM based transaction. In this based on our random input of this three digits a , b , c instant PIN will be communicated to our registered mobile number. This PIN only valid for one transaction and it is also valid for limited period of time. The computation of this instant PIN over Z $_p$ based on previo~~us se~~lection a , b , c and d as follows

p_1 = {

p_2 = {

Similarly p_3 and p_4 will be calculated in a similar way for the combinations (b, c, d) and (a , b , d) respectively. Finally the instant PIN will be computed as steps given below

Step: 1. If p_1 is single digit number than $d_1 = p_1$

Otherwise d_1 = sum of the digits in p_1

Step: 2. If d_1 is single digit number than $d_2 = d_1$

Otherwise step: 2 is repeated till we obtain single digit number

This will be 1st digit of the PIN i.e., n_1

Step: 3. Compute step: 1, and step: 2 for p_2 , p_3 and p_4 .

To evaluate 2nd , 3rd and 4th digits of the PIN

Step: 4. At the end, the PIN will be n_1 n_2 n_3 n_4 , which will be communicated to client registered mobile number. The time and validity are restricted to little period and only one transaction respectively.

Step: 5. Stop.

Note: Integral Part of x: Integral part of x for x ε R, the largest integer not exceeding x. i.e.

[x] ≤ x, symbol is [x]: The integral part of x, Ex: [1.736] = 1.

3. PROPOSED PAYMENT GATEWAY WITH SET PROTOCOL OVER ECC

3.1 NEW DIGITAL SIGNATURE ON PUBLIC KEY ELLIPTIC CURVE CRYPTOGRAPHY:

ECDSA Key Generation:

Elliptic curve domain parameters over Fp are a sixtuple: T = (p, a, b, P, n, h)

(1) T = (p, a, b, P, n, h) consisting of an integer p and two elements a, b, a base point P = (x, y) is a point on Elliptic curve E (Fp), select the number n as n-1 must be a prime number of order p and an integer h which is the cofactor h= # E (Fp)/n.

(2) Select a secret key [d] which is a random integer in the interval [1, n-1].

(3) Select an elliptic curve public key L = [d] P.

(1) Select a key pair ([d] , L) with L = (x_0, y_0) associated with the elliptic curve domain parameters T established during the setup procedure.

(2) Select c ∈ [1, n - 1], cP = (x1, y1), and convert x1 to an integer from definition of bitwise compliment operator, set α = (mod n).

(3) Use the hash function selected to compute the hash value: e = hash (M) where hash is a cryptographic hash function and z = e_n is bit length of hash function with order n.

(4) Compute: $\beta = c^{-1}([d] \alpha + z) \bmod n$

(5) The signature code of message is: γ = (α, β)

ECDSA Signature Verification:

(1) Given L and T to verify α and β, if α and β are not both integers in the interval [1, n-1], the signature is invalid.

(2) Use the hash function to compute the hash value: e = hash (M) and bit length of hash function z = e_n. Evaluate $J= \beta^{-1} \bmod n$

(3) Compute $v_1 =$ z (mod n) and $v_2 =$ (mod n)

(4) Compute R = [v_1] P + [v_2] L = (x_2, y_2)

(5) Convert the element x_1 to an integer using the conversion routine, and set

θ =(mod n)

(6) Accept the signature if and only if $\theta = \alpha$

3.2 CONFIRMATION THEOREMS AND CORRECTNESS OF THE ALGORITHM:

(1) $R = [v_1] P + [v_2] L$

Where public key $L = [d] P$

(2) $R = [v_1] P + [v_2] [d] P$

From elliptic curve property

(3) $R = \{ [v_1] + [v_2] [d] \} P$

(4) $R = \{ z \beta^{-1} + [d] \beta^{-1} \} P$

From terms of β^{-1} we do as follows

(5) $R = \{ z + [d] \} \beta^{-1} P$

By using definition of β from signature generation

(6) $R = (z + [d]) (c^{-1})^{-1} ([d] \alpha + z)^{-1} P$

By adjusting product we get

(7) $R = (z + [d] \alpha) (z + [d] \alpha)^{-1} (c^{-1})^{-1} P$

Here multiplication of an element with its inverse is identity, but we neglect identity and inverse of inverse of an element is equal to itself.

(8) $R = cP$. i.e. $(x_1, y_1) = (x_2, y_2)$. From definition of α in step (2) of signature generation, the above algorithm is correct.

This shows that signed message is verified and authenticated.

3.3 ALGORITHM FOR PAYMENT GATEWAY AND EXECUTION

The algorithm for payment gateway is executed by going through the following steps successfully.

Step 1. Initiate system by lodging the smart card or putting order for any commodity in any commercial Website.

Step 2.The order request is encrypted by ECC under SET protocol and is transformed to merchant after Decryption.

Step 3. Once order request is accepted by merchant and SET protocol will enable the payment link, which Requires banking details of customer.

Step 4. In addition to the Name on Card, Expiry date, customer has to enter any three digit instant PIN of his own choice better is other than CVV on Card.

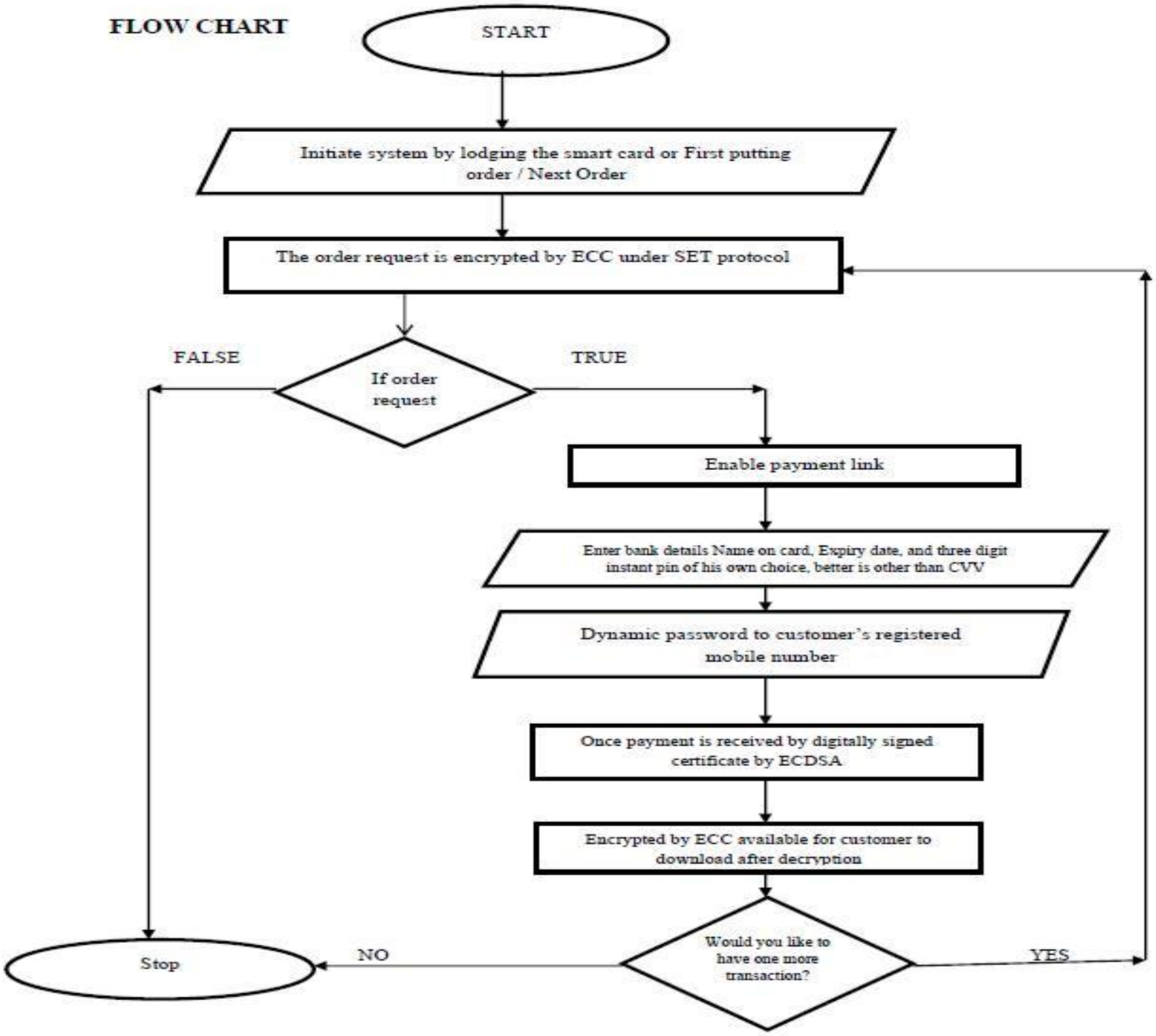
Step 5. A dynamic password will be generated based on customer instant PIN and will be communicated to customer‟s registered mobile number.

Step 6. Customer has to enter this dynamic password on the specified location on the screen, where he has entered instant PIN. By this financial transaction would complete.

Step 7. Once payment is received by merchant, digitally signed certificate by ECDSA will be generated and encrypted by ECC will be made available for customer to download after decryption.

Step 8. Customer can go now for next item or logout.

Step 9. End


FLOW CHART
START
Initiate system by lodging the smart card or First putting order / Next Order
The order request is encrypted by ECC under SET protocol
FALSE
If order request
TRUE
Enable payment link
Enter bank details Name on card, Expiry date, and three digit instant pin of his own choice, better is other than CVV
Dynamic password to customer's registered mobile number
Once payment is received by digitally signed certificate by ECDSA
Encrypted by ECC available for customer to download after decryption
Would you like to have one more transaction?
NO
YES
Stop

4. STRENGTH AND SOUNDNESS OF ALGORITHM

In the current scenario, each person is using more than one smart card and so remembering PINs for each card is very difficult. In this innovation, we have introduced the notion of instant password chosen by cardholder will generate dynamic password, which will transmitted automatically to cardholder registered mobile number. As soon as, once Card holder enters this at specified location on screen, the cycle of transaction is completed successfully. In this notion, the concrete link in between instant PIN and dynamic password. This will not allow any unauthorized person to perform any variety of transaction; even they hold smart card and know static PIN. This will make the people completely free from remembering PINs of distinct smart cards.

In addition to applying this digital tool in e-commerce applications, we can apply even in all ATM operations. This ensures and provides more security of all financial transactions over ATM environment. So this tool shelters all online financial interconnected applications.

5. SECURITY ATTACKS

5.1. Attacks on ECC: ECC allows smaller keys compared to non-EC cryptography to provide equivalent security. Here we explain some attacks on ECC regarding this architecture

(i) Side-channel attacks

In many DLP systems same procedure used for squaring and multiplication, the ECC addition is significantly different for doubling ($P = Q$) and general addition ($P \neq Q$) depending on the coordinate system used. Consequently, it is important to counteract side-channel attacks (timing or simple power analysis attacks) using, for example, fixed pattern window methods (note that this does not increase computation time). In some special family of elliptic curves for which doubling and addition can be done with the same operation. Another worry for ECC-systems is the risk of fault attacks, especially when running on smart cards.

(ii) Invalid curve attack

When ECC is used in virtual machines (kind of software) , an attacker may use an invalid curve to get a complete Platform Diffie Hellman private key. This is defined to be Invalid curve attack.

5.2. Attacks on ECDSA: In this section, we give our results in terms of security analysis of our proposed signature scheme based on ECDLP. The security of the cryptosystems using elliptic curves hinges on the intractability of the discrete logarithm problem in the algebraic system. Over the past ten years this problem has received considerable attention from leading mathematicians around the world. Unlike the case of the discrete logarithm problem in finite fields, there is no sub exponential-time algorithm known for the elliptic curve discrete logarithm problem. The best algorithm known to date takes exponential time. The possible attacks on ECDSA can be classified as follows:

(i) Attacks on the elliptic curve discrete logarithm problem.

(ii) Attacks on the hash function employed.

(iii) Other attacks.

The proposed scheme not only takes full advantage of the difficulty of solving the ECDLP and the security of the proxy scheme but also uses the one-way trapdoor function so the security is higher.

(i) The attacker wishes to obtain secret keys x using all information that is available from the system. In this case, the attacker needs to solve $y = g^x$ (mod p) for x which are clearly infeasible because the difficulty of solving ECDLP. Because the attacker only knows a series of public key, if he wants to gain the private key he has to face the difficulty of solving the ECDLP.

(ii) Attacks on the Hash Function. If SHA-1 is not pre image resistant, then an adversary E may be able to forge A‟s signatures. If SHA-1 is not collision resistant, then an entity E may be able to repudiate signatures. SHA-1 is a 160-bit hash function and is believed to have ideal security.

(iii) The fastest method known for attacking ECDSA by exploiting properties of SHA-1 is to find collisions for SHA-1. Since this is supposed to take minimum steps compared to base paper algorithm attacking ECDSA in this article paper is computationally infeasible.

6. CONCLUSIONS

In this paper, the primal intention of the author to present new notion and dimension of use of instant PIN and dynamic password to perform all financial transactions under secured digital environment. This novel notion facilitated us to design a concrete and secured digital payment gateway infrastructure. This digital infrastructure is fabricated and implemented with the support of SET protocol under the platform of Elliptic Curve Cryptography connecting both Elliptic Curve Cryptosystem and Digital Signature too. This can be applied in all categories of e-commerce applications. We encrypt the payment code using ECC in order to protect the bank account, and the transaction information is encrypted by ECC to avoid any intentional distortion. When we certify the business deals of the card owners, we adopt ECC signature algorithm. Therefore, this ensures the validity, confidentiality, integrity and non-repudiation of information. This paper got weightage by adding the security attacks for ECDLP and hash function applicability to ECDSA algorithm.

REFERENCES

1. S.Brlek,S.Hamadou,l Mullins, "Anonymous and secure electronic transaction protocol,"Annals of Telecommunications,voI.60, pp.530- 557,2005.
2. Certicom Research, "SEC! Elliptic Curve Cryptography Version 1.0, "2000.
3. Yanqin Zhu, Xia Lin, and Gang Wang, "Design of elliptic curve cryptography in GSI,"Current Trends in High Performance Computing and Its Applications, Part II,pp.623-628,2005.
4. Solinas, "Efficient arithmetic on Koblitz curves," Designs, Codes and Cryptography, VoI.19, pp.195-249, 2000.
5. HfCheng, "Privacy protection based on secure electronic transaction protocol in E-Commerce," Communications in Computer and Information Science, I, vol. 153,pp. 449-453.

6. Vanstone, S. A., 1992. Responses to NIST‟s Proposal Communications of the ACM, 35, 50-52.
7. Koblitz, N., 1987.Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.
8. Hankerson, D., Menezes, A., Vanstone, S., 2004. Guide to Elliptic Curve Cryptography. Springer.
9. Botes, J.J., Penzhorn, W.T., 1994. An implementation of an elliptic curve cryptosystem. Communications and SignalProcessing. COMSIG-94. In Proceedings of the 1994 IEEE South African Symposium, 85 -90.
10. Raju, G.V.S., Akbani, R., 2003. Elliptic Curve Cryptosystem and Its Application. In Proceedings of the2003 IEEE International Conference on Systems Man and Cybernetics (IEEE-SMC), 1540-1543.
11. Johnson, D.B., Menezes, A.J., 2007. Elliptic Curve DSA (ECDSA): An Enhanced DSA. Scientific Commons.
12. X. Zhang, Q. Huang and P. Peng, "Implementation of a Suggested E-commerce Model Based on SET Protocol," 2010 Eighth ACIS International Conference on Software Engineering Research, Management and Applications, Montreal, QC, Canada, 2010, pp. 67-73.
13. A.Sun, "Optimization Study for Lightweight Set Protocol," 2012 International Conference on Industrial Control and Electronics Engineering, Xi'an, 2012, pp. 1206-1209.
14. X. Liu,"The Study on E-commerce Security based on ECC and SET,"2011 Third International Conference on Communications and Mobile Computing, Qingdao, 2011, pp. 85-87.
15. X. Zhang and L. Wang, "Key Technologies for Security Enhancing of Payment Gateway," 2008 International Symposium on Electronic Commerce and Security, Guangzhou City, 2008, pp. 743-748.
16. G. Bella, F. Massacci and L. C. Paulson, "Verifying the SET registration protocols," in IEEE Journal on Selected Areas in Communications, vol. 21, no. 1, pp. 77-87, Jan 2003.
17. Z. Hu, "The Study of E-Commerce Security Protocol," 2011 International Conference on Intelligence Science and Information Engineering, Wuhan, 2011, pp. 349-352.
18. Shen Zihao and Wang hui, "An improved SET protocol payment system," 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering, Chengdu, 2010, pp. 400-403.
19. Z. Zhang,"E-Commerce Based Agents over P2P Network," 2008 International Conference on Management of e-Commerce and e-Government, Jiangxi, 2008, pp.77-81.
20. Chin-Ming Hsu and Hui-Mei Chao, "An online fraud-resistant technology for credit card E-transactions, "TENCON 2007 -2007 IEEE Region10 Conference, Taipei, 2007, pp.1-4.
21. P. Venkataram, B. S. Babu, M. K. Naveen and G. H. S. Gungal, "A Method of Fraud & Intrusion Detection for E-payment Systems in Mobile e-Commerce," 2007 IEEE International Performance, Computing, and Communications Conference, New Orleans, LA, 2007, pp. 395-401.
22. Hyun-Seok Kim, Il-Gon Kim and Jin-Young Choi, "Analyzing the Application of E-Commerce in Wireless Network," Second IEEE International Workshop on Mobile Commerce and Services, Munich, 2005, pp. 112-122.
23. Ramakrishna Oruganti, Saurabh Shah, Yohan Pavri, Neelansh Prasad, Prathamesh Churi (2017). JSSecure: A Secured Encryption Strategy for Payment Gateways in E-Commerce. Circulation in Computer Science, 2, 5(June 2017), 13-17.
24. Meadows, Catherine, and Paul Syverson. "A formal specification of requirements for payment transactions in the SET protocol." In International Conference on Financial Cryptography, pp. 122-140. Springer, Berlin, Heidelberg, 1998.
25. Lu, Shiyong, and Scott A. Smolka. "Model checking the secure electronic transaction (SET) protocol." In Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1999. Proceedings. 7th International Symposium on, pp. 358-364. IEEE, 1999.
26. Brlek, Srecko, Sardaouna Hamadou, and John Mullins. "A flaw in the electronic commerce protocol SET." Information Processing Letters 97, no. 3 (2006): 104-108.
27. Shedid, Sabrina M., and Mohamed Kouta. "Modified SET protocol for mobile payment: an empirical analysis." In Software Technology and Engineering (ICSTE), 2010 2nd International Conference on, vol. 1, pp. V1-350. IEEE, 2010.

28. Seo, Moonseog, and Kwangjo Kim. "Electronic funds transfer protocol using domain-verifiable signcryption scheme." In ICISC, vol. 99, pp. 269-277. 1999.
29. Kraft, Theresa A., and Ratika Kakar. "E-commerce security." In Proceedings of the Conference on Information Systems Applied Research, Washington DC, USA. 2009.
30. Marchany, Randy C., and Joseph G. Tront. "E-commerce security issues." In System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on, pp. 2500-2508. IEEE, 2002.
31. Udo, Godwin J. "Privacy and security concerns as major barriers for e-commerce: a survey study." Information Management & Computer Security 9, no. 4 (2001): 165-174.