BBRC
Bioscience Biotechnology Research Communications

A Secure and Efficient Authentication in E-Commerce

Dulal Kumbhakar[1], Kanchan Sanyal[2] and Sunil Karforma[3]
[1]SACT-I, Department of BCA, Vivekananda Mahavidyalaya, Haripal, Hooghly, West Bengal, India
[2]Computer Application, Bhadrapur M.N.K High School, Birbhum, West Bengal, India
[3]Department of Computer Science, The University of Burdwan, Golapbag, Bardhaman, West Bengal, India

ABSTRACT

E-commerce is the technique to conduct commercial transactions using wireless devices. More precisely, E-commerce is defined as the new emerging applications and services that people can access through internet enabled mobile devices such as smartphones, PDAs, i-pads and laptops anytime & anywhere. Nowadays, E-commerce transactions have exploded around the world due to the advancement of Internet technology. But E-commerce transactions are suffered by many attacks due to the lack of secured and efficient security infrastructure. Therefore, secure and effective security requirements are required to prevent E-commerce transactions from the malicious attacks. However, this paper represents the authentication based secure framework for E-commerce applications & services. This paper is also proposed a secure and efficient authentication technique using ECDSA algorithm to ensure the confirming services of E-Commerce to the end customers.

KEY WORDS: E-COMMERCE, FRAMEWORK AND AUTHENTICATION USING ECDSA.

INTRODUCTION

The term E-Commerce was coined by Dr. Robert Jacobson, Principal Consultant to the California State Assembly's Utilities & Commerce Committee, in 1984, to define online transaction processing between customers and businesses organization or between one business organization and another. E-Commerce is the part of new business model that exchanges the valuable services (buying and selling goods) among the business organizations and consumers using wireless electronic devices such as hand-held computers (tablets), mobile phones or laptops without needing to find a place to plug in, which is based on the Wireless Application Protocol (WAP). The integration of Internet, Wireless and E-Commerce produces a successful E-Commerce. With E-Commerce, countries around the world are tried to improve their business volume, education, security, retail management and economic infrastructure, etc. These are achieved by using Wireless Sensor Networks (WSN) and technologies such as Radio-Frequency Identification (RFID).

E-Commerce can be B2B (business to business) or B2C (business to customer) oriented. The term B2B is the exchange of products & services or information between business organizations rather than business organizations & customers whereas B2C refers to the process of selling to individual customers directly through online. These models are used to improve the efficiency & effectiveness of the organization's sales report & better delivery status also. With rapid development of E-Commerce combined with smart technology, the security concerns related to E-commerce infrastructure is also increased simultaneously. Smart technology not only gathers user's credentials, but can also monitor user's activities. However, the scope of this paper relies on a secure authentication technique regarding B2C where the information is shared between business organizations and customers for improving the efficiency of selling and buying process without any fear of attacks.

Biosc Biotech Res Comm P-ISSN: 0974-6455 E-ISSN: 2321-4007

Identifiers and Pagination
Year: 2021 Vol: 14 No (5) Special Issue
Pages: 93-99

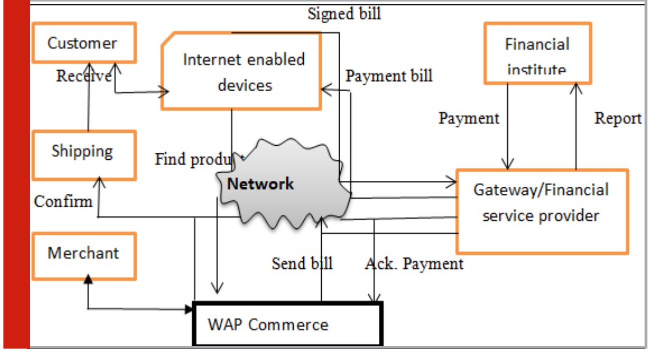
Article Information
Received: 14th Jan 2021
Accepted after revision: 27th Mar 2021

DOI: *http://dx.doi.org/10.21786/bbrc/14.5/19*

In this context, we will briefly explain about related works regarding security mechanisms in respect of E-commerce transactions. A new mobile payment system based on mobile traveller's check (MTC) for mobile commerce is recommend by Shaik Shakeel Ahamad & others. MTC uses elliptic curve digital signature algorithm (ECDSA) for generating and verifying digital signatures. Robert Pinheiro analyzes a well-designed three factor authentication scheme that combines a biometric with a PIN and a registered cell phone acts as a token would offer strong security in E-Commerce. Sanwar ALI et al. have discussed different security measures and the application of the cryptography for key generation, authentication, digital signature and digital certificate in E-Commerce. Seema Nambiar et al. have discussed the framework of public key infrastructure as a basis for security in different mobile technologies, and also analyzed the security measures in mobile security technologies. An implementation of 1024-bit RSA encryption/decryption algorithm using VB.NET for securing ecommerce payment transaction is proposed by Chinedu J. Nwoye. Ibrahim Sayed Abdelwahab Mohamed discusses the E-Commerce security issues and the use of digital signature in different applications of E-Commerce.

It is concerned that online transactions through internet enabled devices are still suffered by challenges although many researchers have proposed different authentication mechanisms. Since, Public key digital signature algorithms are used to eliminate authentication issue regarding E-commerce transactions. For this we have recommended a secure end-to-end authentication mechanism using elliptic curve digital signature algorithm (ECDSA). Its security is based on the difficulty of the elliptic curve discrete logarithm problem and works on significantly smaller key size with same level of security which offers faster computations and less storage space related to other public key digital signature algorithms. The paper is organized as follows. Section 2 represents a secure authentication based E-commerce framework. Section 3 depicts a secure end-to-end authentication technique using ECDSA with summary performances compared to RSA & DSA algorithms. Section 4 concludes the paper.

Figure 1: Secure E-commerce framework



Authentication Based E-Commerce Framework: The authentication based E-commerce framework consists of some sub modules based on the working flows of customer's order regarding products or services. E-commerce addresses electronic commerce via internet enabled devices, where the customer must not be physical or eye contact with the purchased products [5]. The following Figure-1 shows that how to interact the sub systems of the framework to each other in securely & effectively. Here, the Wireless Application Protocol (WAP) is a standard protocol for the presentation and delivery of wireless information and telephony services on different internet enabled devices and wireless terminals.

Any transaction based on the above secure E-Commerce framework between two parties (B2C), the following corresponding steps are listed below:

1. The customer searches E-commerce sites for buying products & services through online.
2. Selects item(s) for own interest.
3. Customer sends request to the system (WAP portal) for buying the selected item(s). Here system checks access right of the item(s).
4. If the item(s) is available to the customer, the system redirects the payment transaction process to the trusted financial organization. The transaction through electronic payment card elaborates the following steps.

1. Customer enters information (electronic payment card details) on the device as per instructions are provided by FSP (financial service provider).
2. Entered information is encrypted by the customer using digital signature algorithm & sends to the service provider.
3. Sharing information between service provider & third party (gateway).
4. Third party decrypts the encrypted information & authenticates using verifier algorithm.
5. After successful authentication, payments done between customer & bank.
6. If payment transaction is successfully done, the financial institute sends payment report to the financial service provider (FSP).
7. FSP sends payment acknowledgment (ACK) to the WAP commerce portal.
8. After that FSP approves the buying product(s) & directs to the shipping department.
9. Shipping department delivers the product(s) to the customer.

Therefore, E-Commerce framework delivers applications & services to the end users with relatively low cost. But the process of B2C is attacked by several attackers such as Man-In-The-Browser (MITB) attack [15]. MITB is the attack that resides in a user's browser and can be programmed to trigger when a user want to access specific sites, such as an on-line shipping site. To mitigate such issues a strong authentication technique based on B2C communication channel is required.

3. A Secure And Efficient End-To-End Authentication Technique Using Ecdsa Algorithm: Communication and sending sensitive information through network is one of the most important activities of E-Commerce services; hence this is a vital security segment to protect customer's credentials of internet enabled devices. In this context, this authentication technique works more effectively and securely.

3.1 Proposed Work: We have proposed a secure and efficient authentication technique using ECDSA during transaction between the customer at the sender end & FSP at the receiver end. The following steps are taken at the customer end during E-Commerce transaction.

1. Customer enters information (electronic payment card details) through internet enabled device.
2. The message digest (MD) of entered information is calculated using SHA-1 hash function by the customer.
3. This MD is encrypted by using a private key that is generated by customer to form a signature.
4. The signature is appended with the original information and sent to the FSP.

The following steps are taken at the FSP end during E-Commerce transaction.

1. The FSP decrypts the signature by using a public key which is known to form MD1.
2. The FSP now computes the message digest (MD2) from message representing an E-Commerce transaction which is sent with the signature using SHA-1 hash function.
3. Then MD1 & MD2 are compared.
4. If MD1 is same as MD2, then the transaction between customer & FSP is successfully done. Otherwise it will be rejected.

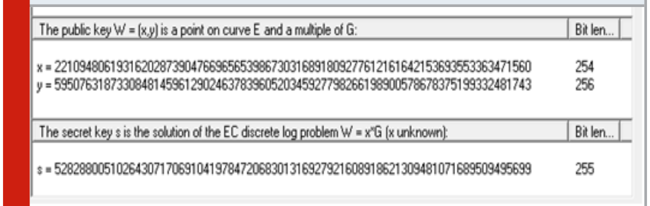
Therefore, the private key of the customer is only used to encrypt & public key is used to decrypt that ensures the authenticity. The proposed technique is able to prevent the M-commerce transactions from the intruders. The implementation of ECDSA is done by Crypto tool. There are three processes namely key pair generation, digital signature creation, verification & extraction.

A. Key pair generation

Before functioning of authentication using ECDSA, the customer needs to know its private key. So the following steps are followed by the customer.

1. Take an Elliptic curve E described through the curve equation: y2 = x3 + ax + b (mod p).
2. Set point G on curve E (through its (x, y) coordinates): G has the prime order n and the cofactor k (n*k is the number of points on E).
3. Set the public key W=(x, y) is a point on curve E and multiple of G. The public key is derived from the private key and the domain parameters (E, G, and n).
4. Set secret key's which is the solution of the EC discrete log problem W=x*G where x is the selected random number in the interval [1, n-1] by the customer.
5. After calculating by Crypto tool, the following key values are generated.

Figure 2: Key value generation



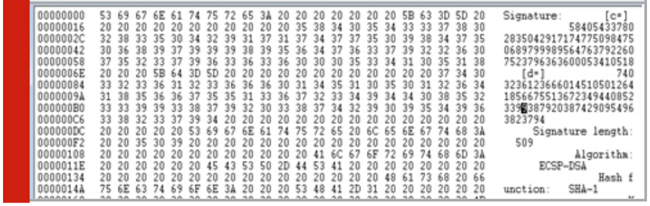
```
The public key W = (x,y) is a point on curve E and a multiple of G:                     Bit len...

x = 22109480619316202873904766965653986730316891809277612161642153693553363471560      254
y = 59507631873308481459612902463783960520345927798266198900578678375199332481743      256

The secret key s is the solution of the EC discrete log problem W = x*G (x unknown):    Bit len...

s = 52828800510264307170691041978472068301316927921608918621309481071689509495699      255
```

B. Digital signature creation: The customer creates signature which will be verified by the FSP using public key which is known. For signature creation of the information, the following steps are followed by the customer.

1. Compute e= SHA-1 (message representing an M-commerce transaction is converted in to an integer).
2. Select a random integer k, 1≤ k ≤ n-1.
3. Calculate the curve point (x1, y1) =k*G.
4. Calculate c=x1 mod n. If c=0, go to step 2.
5. Calculate d= k-1 (z+ cx) mod n, where z is left most bit of e. If d=0, go to step-2.
6. The signature is the (c, d) pair.

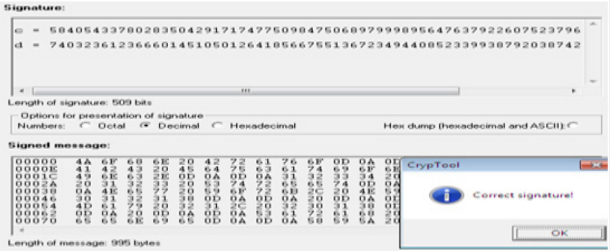
Following figure shows the generated signature.

Figure 3: Signature generation



```
00000000  53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 5B 63 3D 5D 20   Signature:      [c=]
00000016  20 20 20 20 20 20 20 20 20 20 20 35 38 34 30 35 34 33 33 37 38 30            58405433780
0000002C  32 38 33 35 30 34 32 39 31 37 31 37 34 37 37 35 30 39 38 34 37 35   2835042917174775098475
00000042  30 36 38 39 37 39 39 39 38 39 35 36 34 37 36 33 37 39 32 32 36 30   0689799989564763792260
00000058  37 35 32 33 37 39 36 33 36 33 36 30 30 30 35 33 34 31 30 35 31 38   7523796363600053410518
0000006E  20 20 20 5B 64 3D 5D 20 20 20 20 20 20 20 20 20 20 20 20 37 34 30      [d=]             740
00000084  33 32 33 36 31 32 33 36 36 36 30 31 34 35 31 30 35 30 31 32 36 34   3236123666014510501264
0000009A  31 38 35 36 36 37 35 35 31 33 36 37 32 33 34 39 34 34 30 38 35 32   1856675513672349440852
000000B0  33 33 39 39 33 38 37 39 32 30 33 38 37 34 32 39 30 39 35 34 39 36   3393387920387429095496
000000C6  33 38 32 33 37 39 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   3823794
000000DC  20 20 20 20 20 53 69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A        Signature length:
000000F2  20 20 35 30 39 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20     509
00000108  20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6F 72 69 74 68 6D 3A              Algorithm:
0000011E  20 20 20 20 20 20 45 43 53 50 2D 44 53 41 20 20 20 20 20 20 20 20         ECSP-DSA
00000134  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 48 61 73 68 20 66                 Hash f
0000014A  75 6E 63 74 69 6F 6E 3A 20 20 20 53 48 41 2D 31 20 20 20 20 20 20   unction:   SHA-1
```

Figure 4: Verification of signed document



```
Signature:
c = 58405433780283504291717477509847506897999895647637922607523796
d = 74032361236660145105012641856675513672349440852339938792038742
Length of signature: 509 bits
Options for presentation of signature
Numbers: ○ Octal  ● Decimal  ○ Hexadecimal        Hex dump (hexadecimal and ASCII): ○
Signed message:
00000   4A 6F 68 6E 20 42 72 61 76 6F 0D 0A 0D
0000E   41 42 43 20 45 64 75 63 61 74 69 6F 6E
0001C   49 6E 63 2E 0D 0A 0D 0A 31 32 33 34 20
0002A   20 31 32 33 20 53 74 72 65 65 74 0D 0A
00038   0A 4E 65 77 20 59 6F 72 6B 2C 20 4E 59
00046   30 31 32 31 38 0D 0A 0D 0A 20 0D 0A 0D
00054   4D 61 79 20 32 31 2C 20 32 30 31 38 0D
00062   0D 0A 20 0D 0A 0D 0A 53 61 72 61 68 20
00070   65 65 6E 69 65 0D 0A 0D 0A 58 59 5A 20
Length of message: 995 bytes
```

CrypTool

Correct signature!

C. Verification & Extraction: FSP verifies authenticity of the signed document using public key curve point W. Hence the following steps are followed by the FSP.

1. Verify that W is not equal to O (identity element); otherwise its coordinates are valid.
2. Verify the W lies on the curve.
3. Verify that pW=O.
4. Verify that c and d are integer in [1, n-1].
5. Calculate e=SHA-1(received message representing an M-commerce transaction converted into integer).
6. Let z be the left most bit of e.
7. Calculate u1=z d-1 mod n and u2=c d-1 mod n.
8. Calculate curve point (x1, y1) =u1.G + u2.W. If (x1,

y1) =0, then the signature is not valid.

9. If c≡x1 (mod p), then the signature is valid. Otherwise it is invalid.
10. The following figure shows the extracted signature

Elliptic curve cryptography works on the equation y2=(x3+ax+b) mod p. The prime modulo (range of 160 bits) allows modular square root and modular multiplicative inverse. Since the possible values of y are between 0 and p-1. Only a smaller subset of those values will be a perfect square which will give N possible points on the curve where N < p where N is the number of perfect squares between 0 and p. Since each x will produce positive and negative values of the square-root of y2. Hence there are N/2 possible x coordinates that are valid and give a point on the curve. So this elliptic curve has a finite number of points on it, and it's all because of the integer calculations and the modulus.

The point multiplication k*n (which is the addition of the point n to itself k times). So, if R=k*n, where R is a symmetric point & there is no way to find out the value of k although R & n are known because there is no point subtraction or point division. The private key is a random number that is generated, and the public key is a point on the curve generated from the point multiplication of G with the private key. If we set 'x' as the private key and 'W' as public key (a point), we have W = x*G (where G is the point of reference in the curve parameters).

Table 1. Time execution of the phases for ECDSA & DSA

Phases	Messages	ECDSA			DSA		
		Sig. size (bits)	Size (bytes)	Time (Sec.)	Sig. size (bits)	Size (bytes)	Time (Sec.)
Key generation	Sample 1	N/A	2050	0.117	N/A	2050	2.309
	Sample 2	N/A	2330	0.056	N/A	2330	1.018
	Sample 3	N/A	2753	0.059	N/A	2753	3.818
	Sample 4	N/A	983	0.047	N/A	983	3.245
	Sample 5	N/A	845	0.046	N/A	845	2.044
	Sample 6	N/A	1379	0.093	N/A	1379	3.261
	Sample 7	N/A	1079	0.047	N/A	1079	1.872
	Sample 8	N/A	919	0.063	N/A	919	4.118
	Sample 9	N/A	720	0.063	N/A	720	0.920
	Sample 10	N/A	414	0.078	N/A	414	3.573
Signature generation	Sample 1	381	2050	0.006	376	2050	0.004
	Sample 2	382	2330	0.006	368	2330	0.006
	Sample 3	384	2753	0.006	368	2753	0.004
	Sample 4	378	983	0.000	376	983	0.000
	Sample 5	383	845	0.000	368	845	0.000
	Sample 6	384	1379	0.056	368	1379	0.000
	Sample 7	375	1079	0.000	368	1079	0.000
	Sample 8	383	919	0.000	376	919	0.014
	Sample 9	380	720	0.000	368	720	0.000
	Sample 10	384	414	0.016	368	414	0.000
Verification & Extraction	Sample 1	381	2050	0.010	376	2050	0.010
	Sample 2	382	2330	0.010	368	2330	0.012
	Sample 3	384	2753	0.012	368	2753	0.012
	Sample 4	378	983	0.014	376	983	0.016
	Sample 5	383	845	0.016	368	845	0.000
	Sample 6	384	1379	0.014	368	1379	0.014
	Sample 7	375	1079	0.000	368	1079	0.016
	Sample 8	383	919	0.000	376	919	0.014
	Sample 9	380	720	0.014	368	720	0.016
	Sample 10	384	414	0.016	368	414	0.014

Now, (c, d) is the signature pair that is mentioned in the signature creation phase and curve point P=k*G (k is a random number). The following equation can be used to compute d. d=k-1(z + c*x) mod n, where z is the hash of the message, x is the private key and c is the x coordinate of k*G. If P is equal to c, the signature is valid. Otherwise it is not . To calculate P using the function P=d-1*z*G+d-1*c*W

Or, P=d-1*z*G + d-1*c*x*G, (where W=x*G)

Or, P=d-1(z + c*x) G,

Or, k*G=d-1(z + c*x) G,
Or, k=d-1(z + c*x), (removing G)
Or d=k-1(z + c*x), (Inverting k & d).

So, it is matched. Therefore, k (random number) & x (private key) are required to calculate d, but c & W (public key point) are only needed to verify the signature. There is no way to calculate x or k from c & W due to trap door function in ECDSA point multiplication. So, it makes ECDSA algorithm secure. Further, ECDSA works on smaller key size and consuming less memory space. The ECDSA generates d in the interval [1, n-1] by taking the x coordinate of k*G (random point) and reducing it modulo n. These are helpful to make ECDSA algorithm computationally faster. Hence proposed work using ECDSA algorithm enhances the authentication security in E-commerce transactions between customer & FSP.

Table 2. Time execution of the phases for ECDSA & RSA

Phases	Messages	ECDSA			DSA		
		Sig. size (bits)	Size (bytes)	Time (Sec.)	Sig. size (bits)	Size (bytes)	Time (Sec.)
Key generation	Sample 1	N/A	2050	0.117	N/A	2050	0.706
	Sample 2	N/A	2330	0.056	N/A	2330	1.109
	Sample 3	N/A	2753	0.059	N/A	2753	1.234
	Sample 4	N/A	983	0.047	N/A	983	0.702
	Sample 5	N/A	845	0.046	N/A	845	0.717
	Sample 6	N/A	1379	0.093	N/A	1379	0.665
	Sample 7	N/A	1079	0.047	N/A	1079	0.796
	Sample 8	N/A	919	0.063	N/A	919	0.686
	Sample 9	N/A	720	0.063	N/A	720	0.702
	Sample 10	N/A	414	0.078	N/A	414	0.858
Signature generation	Sample 1	381	2050	0.006	1024	2050	0.010
	Sample 2	382	2330	0.006	1024	2330	0.010
	Sample 3	384	2753	0.006	1024	2753	0.010
	Sample 4	378	983	0.000	1024	983	0.000
	Sample 5	383	845	0.000	1024	845	0.014
	Sample 6	384	1379	0.056	1024	1379	0.016
	Sample 7	375	1079	0.000	1024	1079	0.016
	Sample 8	383	919	0.000	1024	919	0.016
	Sample 9	380	720	0.000	1024	720	0.000
	Sample 10	384	414	0.016	1024	414	0.014
Verification & Extraction	Sample 1	381	2050	0.010	1024	2050	0.000
	Sample 2	382	2330	0.010	1024	2330	0.000
	Sample 3	384	2753	0.012	1024	2753	0.000
	Sample 4	378	983	0.014	1024	983	0.000
	Sample 5	383	845	0.016	1024	845	0.000
	Sample 6	384	1379	0.014	1024	1379	0.000
	Sample 7	375	1079	0.000	1024	1079	0.000
	Sample 8	383	919	0.000	1024	919	0.000
	Sample 9	380	720	0.014	1024	720	0.000
	Sample 10	384	414	0.016	1024	414	0.000

Table 3. Time execution summary for ECDSA, RSA & DSA

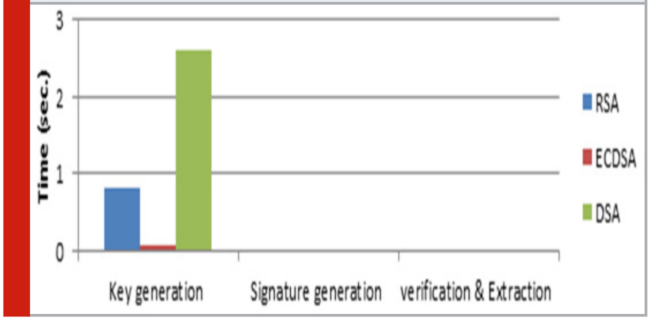
Time(sec.)	ECDSA	RSA	DSA
Key generation	0.0669	0.8175	2.6178
Signature generation	0.009	0.0106	0.0028
Verification & Extraction	0.0106	0	0.0124
Total	0.0865	0.8281	2.6330

3.2 Performance Analysis: The entire execution process of proposed model works on the basis of following requirements:

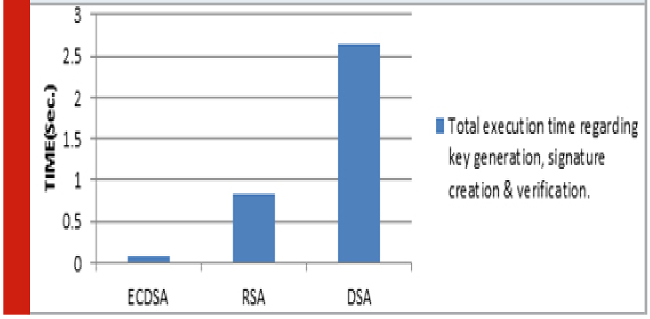
- Operating system: Microsoft windows 7(32 bit) & Processor: Intel(R) Atom(TM) CPU N450, 1.67 GHz, RAM-1GB.
- Crypto tool "CrypTool 1.4.40" is used to compute the proposed model.

A. Evaluation performances of ECDSA compared with DSA: The bit length of the ECDSA for the public key is

Graph 1: Time execution for different phases



Graph 2: Performances of ECDSA, RSA & DSA



the twice of the security level. For instance, the security level of 80 bits(where 280 operations to find the private key), the length of ECDSA public key is 160 bits regarding the size of a DSA public key is at 1024 bits. Therefore we have set bit length prime192v1 for ECDSA & 1024 bits for DSA to achieve the performances of them. So, the following Table-1 represents the summary performances of the entire implementation by ECDSA & DSA. Here SHA – 1 hash function is used for both cases.

B. Evaluation performances of ECDSA compared with RSA: If we compare ECDSA with RSA regarding same level security, then we can say that ECDSA requires smaller key size compared to RSA. For an example, key size of 1024 bits for RSA is equivalent to the key size of 192 bits for ECDSA. Therefore, the following Table-2 represents the summary performances of RSA & ECDSA. Here SHA – 1 hash function is also used and bit length of RSA is 1024 bits which is compared to prime192v1 of ECDSA.

Now, we have calculated the average execution time over 10 samples taken for key generation, signature generation & verification.

We have plotted the summary execution time of different phases in ECDSA, DSA & RSA respectively. This is shown in the following graphical representation.

We have calculated the total execution time for three phases in respect of ECDSA, RSA and DSA. This is shown in the Graph-2. Now we have represented the overall performances of RSA, ECDSA and DSA by combining three phases in terms of execution time as shown below.

After observing the above figure, it is clearly state that the ECDSA algorithm gives more secure and efficient performances for entire set of execution. Although ECDSA is a bit slower than RSA only for verification, but ECDSA with same level of security offers faster implementations by consuming less memory relatively compared to others algorithms like RSA and DSA.

CONCLUSION

ECDSA algorithm uses scalar random in point multiplication k*n (k is the random number) to protect the signature from the attackers. So, strong randomness in ECDSA algorithm increases the authentication security level of E-Commerce transactions. This paper has proposed a secure and efficient end-to-end authentication technique using ECDSA algorithm in E-Commerce transactions. Using this algorithm, we have plotted the summary performances of ECDSA compared to RSA and DSA algorithms respectively. We have observed that the proposed model becomes more secure and faster than the other public key digital signature algorithms in E-Commerce authentication system. However, our future work will be deliver a secure integration technique of cloud computing and IoT technology using machine learning in E-Commerce paradigm.

REFERENCES

A.Deepika, Trends inM-Commerce.” Shanlax International Journals of Commerce, vol. 6, no. S1, 2018, pp. 285–290. /https://doi.org/10.5281/zenodo.1419466.

Al Imem Ali, Comparison And Evaluation Of Digital Signature Schemes Employed In NDN network, International Journal of Embedded systems and Applications(IJESA) Vol.5, No.2, June 2015, PP. 15-30.

Chao-Tsong Fangtsou, Rui-Yang Chen & Ming-Hung Yang, Optimizing Recommendations With An Rfid-Based Approach For The Taiwan Trainquali Document Management System, International Journal of Electronic Commerce Studies, Vol.5, No.1, pp. 1-26, 2014, doi: 10.7903/ijecs.1148.

Chinedu J. Nwoye, Design and Development of an E-Commerce Security Using RSA Cryptosystem, IJIRIS, Issue 2, Volume 6 (June 2015), PP. 1-14.

Don Johnson and Alfred Menezes and Scott Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), PP. 1-56. Retrieved from //www.certicom.com.

G´erard Maze, B.S., M.S., Algebraic Methods For Constructing One-Way Trapdoor Functions, A Dissertation, april 2003.

Ibrahim Sayed Abdelwahab Mohamed, Digital signature in E-Commerce security, Middle East Journal for Scientific Publishing, Vol. 1, Issue No.1, 26-34 (2018).

Ion IVAN, Daniel MILODIN & Alin ZAMFIROIU, Security of M-Commerce transactions, Theoretical and Applied Economics, Volume XX (2013), No. 7(584), pp. 59-76.

KaKaRoTo, blog, How the ECDSA algorithm works, Posted on January 31, 2012, PP. 1-23.

Ljupco Antovski & Marjan Gusev, M-Commerce Services, PP. 15-24, http ://www.ii.edu.mk.

Marko Schuba & Konrad Wrona, Security for Mobile Commerce Applications, Mobility Applications Lab, Ericsson Research, Ericsson Allee 1, 521 Herzogenrath, Germany.

Mishall Al-Zubaidie, Zhongwei Zhang and Ji Zhang, Efficient and Secure ECDSA Algorithm and its Applications: A Survey, improvearXiv:1902.10313v1 [cs.CR] 27 Feb 2019, PP. 1-31.

Prof. Bernhard Esslinger and the CrypTool Team, CRYPTOLOGY WITH CRYPTOOL 1, 19 September 2017, with release CT 1.4.40.

R Jayaraman, A. Srivastava, A. Balgi, A. Kumar , B. Prasad, "A Study of Operating Practices and Supply Chains in the e-Commerce Online Retail Businesses in India", Journal of Supply Chain Management Systems, Volume 2 Issue 3, Pp.1-15, July 2013.

Rania. A. Molla, Imed Romdhani, Bill Buchanan & Etimad. Y. Fadel, Mobile User Authentication System for e-Commerce Applications, PP. 27-34.

Robert Pinheiro, Strong User Authentication For Electronic and Mobile Commerce, SANS Institute 2000 – 2002, GSEC Version 1.4, PP. 1-17.

Sanwar ALI, Waleed FARAG & Mohammad A. ROB, Security Measures in Mobile Commerce: Problems and Solutions, 2015, PP. 1-7.

Seema Nambiar, Chang-Tien Lu and Lily R. Liang, Analysis of Payment Transaction Security in Mobile Commerce, 0-7803-8819 -4/04/$20.0002 004 IEEE, PP. 475-481.

Shaik Shakeel Ahamad, Siba K. Udgata & V.N. Sastry, A new mobile payment system with formal verification, Int. J. Internet Technology and Secured Transactions, Vol. 4, No. 1, 2012, PP. 71-103.

Suchitra.C & Vandana C.P, The Internet of Things and Security Issues, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1, January-2016, pg. 133-139.

Wikipedia, " E-commerce ", Retrieved from https :// en.wikipedia.org/wiki/E-commerce.

Wikipedia, Elliptic Curve Digital Signature Algorithm. Retrieved from:/https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorith.