A Novel M-Commerce Data Security Mechanism using Elliptic Curve Cryptography

Balasubramanian Prabhu Kavin, Sannasi Ganapathy

Abstract*: Cryptography is a mathematical science which permits only the authorized users to access the data. Today, it is necessary for our routine life to safeguard online data like credit card numbers, bank transactions, etc. Many cryptographic algorithm-based data security mechanisms have been introduced by various researchers for protecting the online / M-Commerce data. Even though, no data security algorithms achieved the required security level with less time. For overcoming these issues, we propose a new data security algorithm called Elliptic-Curve Cryptography and Diffie-Hellman based data security algorithm for securing the M-Commerce data. Here, the key size of the Elliptic Curve Cryptography is less than RSA that will be helpful to improve the efficiency and reduce the storage space. This algorithm is able to establish a secure session key through a server over an insecure channel and also handle various illegitimate users. In addition, this new algorithm is more secure, efficient and suitable for mobile commerce environments than existing data security algorithms. For evaluating the data security mechanism, many experiments conducted with M-Commerce data that are collected from the Internet which are freely available and also proved the efficiency of the data security algorithm.

Index Terms*: Cryptography, Encryption, Decryption, Elliptic Curve Cryptography (ECC), Diffie-Hellman, Private Key, Public Key.

I. INTRODUCTION

Mobile commerce (M-Commerce) is one of the procedures to buy and sell the materials, all kind of things, including eatable and electronic goods and services using the internet enabled the mobile applications. M-Commerce has also become a mode of payment for the goods and services. With the change in technology most of the electronic commerce has been transformed to mobile commerce. In present time, mobiles phones are widely used for the payment mechanism through a communication medium. There are many positive aspects of mobile commerce transactions but on the other hand it has several issues related to its security and privacy which cannot be neglected. Elliptic Curve Cryptography (ECC) is one of the public key encryption techniques that work according to the mathematical elliptic curve equation given in equation (1).

$$Y^2=X^3+aX+b \quad (1)$$

Elliptic Curve is the type of equation formed using the points where the line intersects the axis. If we multiply a point with a number, another point can be produced on the curve. Even if you are familiar with the original point and the result, you cannot find what number is used. Elliptic Curve equations are simple to generate curve points, but quite difficult to reverse back and find the original point.

Elliptic Curve Cryptography (ECC) provides a same level of security in a less key size compared to other cryptographic algorithms. If it uses a key size of 164-bit, the other requires 1024-bit key size for the same level of security. Because of this reason it is the most widely used algorithm for the security with lower computing power and less resource usage.

Diffie-Hellman (DH) is a manner of producing a shared secret between two people in a way that the key is not seen by observing the information in communication. This is most helpful because it is used to generate an encryption key with somebody, and then begin encrypting your circulation with that key. And though the circulation is logged and later examined, there is not at all chance to find the key, even if the connections which are made, may be visible. The exact confidentiality comes from this place. Nobody can analyse the circulation at a later date to disrupt the key is neither saved nor conveyed, and cannot be detected at anyplace.

The major contribution of this paper is to apply a new security algorithm which is useful for enhancing the business strategy, profit and also make it easy to buy and sell the products in the market. For this purpose, a standard cryptographic method which uses the standard Elliptic Curve and Diffie-Hellman is used for protecting the M-commerce data that are stored and transferred from our own office/home. Remaining of this work is organized as below: In section 2, the various cryptographic algorithms and the relevant works of M-Commerce were discussed. The working flow of the proposed model is explained in Section 3. In section 4, the performance of the proposed system is demonstrated with the highlight of achievement. Section 5 concludes the work and also suggested few new directions.

II. LITERATURE SURVEY

Many cryptographic algorithms-based data security models have been introduced by various researchers in the last two decades to protect the data from attacker in online and offline. Among them, Muthurajkumar et al proposed different kinds of security approaches for secured log management, detection of malware, intrusion detection, and also scheduling in cloud environment [18-21]. Jayanthi et al have done a detailed survey on different types encryption techniques in images. In addition, she has presented a new image encryption and an efficient transmission technique [24-26].Subbulakshmi Padmanabhan et al have suggested secured shopping system by employing RFID in cloud [22].

Revised Manuscript Received on August 07, 2019.

Balasubramanian Prabhu kavin, School of Computing Science and Engineering, VIT University-Chennai Campus, Chennai, India.

Sannasi Ganapathy, School of Computing Science and Engineering, VIT University-Chennai Campus, Chennai, India.

Thangaramya Kalidoss et al have used a map reducing techniques for identifying the data that are vertically partitioned [23]. Deepak Kumar et al tried to cover the safety concern for online transactions. The difficulties like privacy, verification, secret writing and authorization is mentioned to create secure transactions over the wireless devices [1]. Himja Agarwal and Badadapure defined that Elliptic curve Cryptography authentication scheme offers much higher data security for a defined size of key. If the size of key is smaller it is also possible to implement for a given level of security so that it consumes less power and less heat production. The smaller key size makes faster cryptographic operations, which runs on smaller chip and on much dense software [3]. Khaleel Ahmed and Shoaib Alam focused on SET security. The aim of the paper is to enhance security in E-commerce with PGP with dual signature. Their projected model aimed on important keys like the SET security, the time consumption and cost. They used ECC algorithm which is most protected and less time engrossing. With the help of private and public key of sender and receiver, it can control all the encryption and the decryption [6],[10]. Christina Thomas et al discussed the security issues and drawbacks in the existing encryption techniques. In the survey paper, a better way of scalar multiplication is done for the two fields (prime fields and binary fields) [4]. Susantio and Muchtadi-Alamsyah et al defined how elliptic curves are implemented on binary fields. They recognized numerous algorithms for implementation of the shortened ECIES on binary part. Many situations can be dealt once by considering and adding the points, that area unit wherever the purpose of one or both the points area unit points at a particular time period and it also the situation wherever the points area unit an equivalent. Using Theorems, the point can be generated efficiently. The provided algorithm can also encrypt and decrypt the information efficiently [7]. Prabhu and Ganapathy proposed a new task scheduling method by utilizing A* Search and IPSO algorithm in cloud environment [15]. Deepika et al proposed a scalar multiplication on elliptic curve for improving the security level[5],[11]. Argyris et al presented an illustration methodology which is depended over the adaptive interactive system for checking out the process of M-Commerce and also introduced the persona check process. Especially, this system has been organized and processed in a way that the users will be visually sophisticated as per their expectation. There are mainly three components in the persona check system they are 1) an environment to create and manage the designs of the checkout process, 2) a component for a user model that holds the data collection methods of the users, and 3) An adaptive user interface that follows a rule-based mechanism to identify the perfect fit for decision making and communication [14]. Subbulakshmi developed a secured Point Of Sale system which is completely secured over the cloud and for the purpose of improving the security level RFID technology have been used by the author [13].Samaneh et al discussed in depth about the available and serious attacks including the new attacks that comes newly, Sybil, reputation score, Sybil and the proposal of a new and a system that takes care the multi-factor trust values according to the confidence. They have implemented their work in a simulator which maintains less means absolute error rate [12]. Preethika et al developed an effective authentication methodology by utilizing the Diffie-Hellman key exchange approach in wireless sensor network [9].

Balasubramanian and Sannasi et al proposed a mechanism for the purpose of safeguarding the data in the cloud database. In their work, they have used the Chinese Remainder Theorem for building this new mechanism. In addition, the author has also developed a new scheme for group key management by using Chinese Remainder Theorem for providing the access to the group users. In this the authors have used two different formulas for encryption and decryption of user data in cloud, and for group key generation also a new formula has been introduced. It has been proven that the new mechanism performs well while comparing with the classical security mechanisms [17]. Md Shoaib et al addresses the security and privacy of user and wireless infrastructure through cryptography. He proposed a model called McEliece cryptosystem to perform the encryption and decryption processes on the M-Commerce data by applying an unbreakable quantum cryptosystem. All the existing systems are not able to achieve the required accuracy in less time. For this purpose, a new security mechanism is proposed to protect the data on the cloud platform. Moreover, it is helpful for enhancing the M-Commerce [16].

III. PROPOSED DATA SECURITY MODEL

The proposed security model is explained in this section with necessary justification briefly. The proposed system uses the standard cryptographic algorithm called Elliptic Curve Cryptography (ECC) and Diffie Hellman (DH) based for improving the M-Commerce by protecting the M-Commerce data in network from the attackers. Here, this work creates a secret that is communal on an insecure channel and there must be an unknown key protocol which allows two users to have key pairs with the combination of private and public keys that are generated by using elliptic curve cryptographic algorithm and Diffie-Hellman [2], [8]. Moreover, this communal secret message is used as a key directly or to derive another one key. In addition, the data (information) is encrypted by using the secret key or the derived key with a symmetric-key cipher.

Generally, the Diffie-Hellman algorithm is a key exchange algorithm but it also acts as an encryption algorithm when it is incorporate with elliptic curves. In addition, the ECDH is an encryption algorithm as well as a key agreement protocol. The Diffie-Hellman approach is incorporated with elliptic curves. The ECDH defines the way of generating key and the exchange of keys between the parties. That secret key is used for encryption and information is sent to the other party secretly. However, we need to share the information securely to the other party in such a way the middle man or any third party may interrupt them but not be able to decode the information. The steps of the proposed Elliptic-Curve and Diffie-Hellman based Data Security Algorithm are works as follows:

Elliptic-Curve and Diffie-Hellman based Data Security Algorithm (ECDH-DSA)

Input: E-Commerce Data

Output: Secured Data

Step 1: Firstly, both the parties (Customer & Company) create their own private and public keys.

Step 2: For Customer, the private key is $\mathbf{d_a}$ and public key is $\mathbf{H_a=d_aG}$.
Step 3: Similarly, for the company applies keys $\mathbf{d_b}$ and $\mathbf{H_b}$ as private and public keys. $\mathbf{H_b=d_aG}$.
Step 4: Where. **G**= the similar base point over the same elliptic curve over the finite field which is similar to the same.
Step 5: **d**= an integer number is chosen randomly from the set 1 to n-1 and n is considered as a sequence of the subgroup.
Step 6: Both the parties i.e. Customer and Company share their public keys such as $\mathbf{H_a}$ and $\mathbf{H_b}$ over the channel that is insecure.
Step 7: The middle man can perform the interception between the $\mathbf{H_a}$ and $\mathbf{H_b}$ and it will not be available for finding out the $\mathbf{d_a}$ or the $\mathbf{d_b}$.
Step 8: Customer computes the S value by applying the formula $\mathbf{S=d_aH_b}$ and the company admin computes the S value by using the formula $\mathbf{S=d_bH_a}$.
Step 9: S is same for both customer and company admin.
$\mathbf{S=d_aH_b=d_a(d_bG)=d_b(d_aG)=d_bH_a}$
Step 10: Now, the third party or the middle man (server) who only knows the $\mathbf{H_a}$ & $\mathbf{H_b}$ will not be able to compute the secret key S without knowing the private keys.

Fig.1 shows the private key structure which is used in this work.

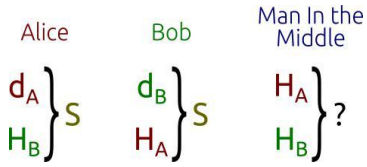

Fig.1. Key Format

The proposed algorithm is used to secure the E-Commerce data that have been collected from the social networks. Moreover, it provides the security to the individual user's data who is utilizing the online purchase frequently. These kinds of user's personal information and their purchase and sales details are also stored securely. Even though, it provides security to the transmission data while communicating between the company and the customers. The particular product feedbacks also stored and maintained securely and it will be protected from the attackers. The proposed algorithm is used to encrypt the user's data and also secure the keys like private and public keys that are useful for protecting the data.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed data security algorithm is used to secure the M-Commerce data that have been collected from the social networks. Moreover, it provides the security to the individual user's data who is utilizing the online purchase frequently. These kinds of user's personal information and their purchase and sales details are also stored securely. Even though, it provides security to the transmission data while communicating between the company and the customers. The particular product feedbacks also stored and maintained securely and it will be protected from the attackers. The proposed algorithm is used to encrypt the user's data and also secure the keys like private and public keys that are useful for protecting the data.

Fig.2 shows the time analysis which expresses the efficiency of the encryption process and the decryption process for the proposed ECDH based data security algorithm. Here, the six experiments have been carried out with various sizes of files including 100, 200, 400, 600, 800 and 1000 Mbs. Here, the encryption and decryption time is increasing gradually in both processes.

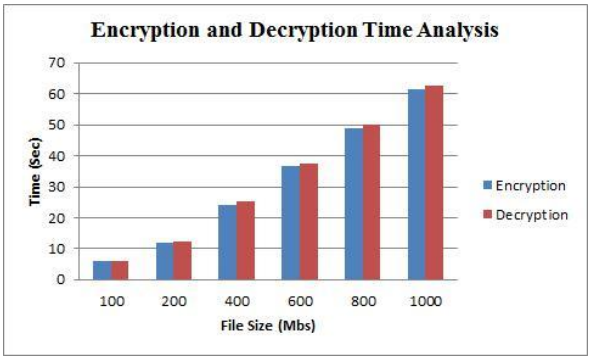

Fig.2 Time Analysis of Encryption and Decryption

Fig.3 shows the comparative analysis between the proposed ECDH based data security algorithm and the existing cryptography algorithms namely BF, AES and DES that are used for providing data security in this application. Here, six experiments have been carried out with the consideration of various file sizes like 100, 200, 400, 600, 800 and 1000 Mbs. Here, the encryption and decryption time is increasing gradually in both processes.

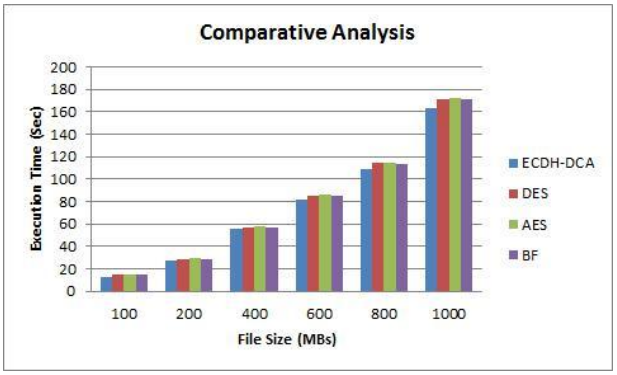

Fig.3 Comparative Analysis with respect to Execution Time

In Figure 3, the performance of the ECDH based M-Commerce data security model is better when map with the standard cryptographic techniques like BF, AES and DES.

The security level analysis is demonstrated in Fig. 4 which compares the performance of the proposed ECDH and the standard cryptographic algorithms including DES, AES and Brute Force. Here, various sizes of files were used for performing encryption and decryption techniques. Here, the encryption and decryption time is increasing gradually in both processes. The better security level is achieved by the proposed data security mechanism than other cryptographic algorithms which demonstrates in fig.4. The reason for the achievement is to the use of Diffie-Hellman along with Elliptic Curve Cryptography.

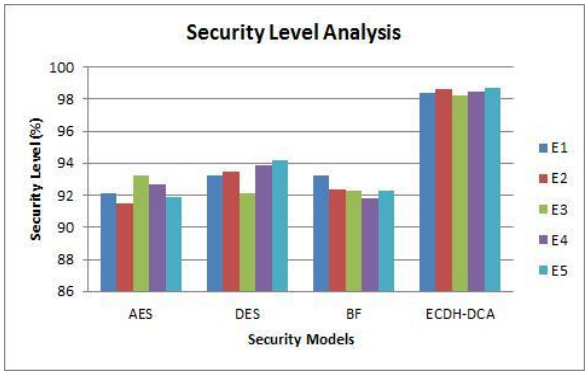

Fig.4 Security Level Analysis

The reason for the achievement is to the use of Diffie-Hellman along with Elliptic Curve Cryptography. This combination is able to provide more security than others.

V. CONCLUSIONS AND FUTURE DIRECTIONS

A novel Elliptic Curve Cryptography and Diffie-Hellman based data security algorithm that is used to provide M-Commerce data on Internet or Cloud environments. The M-Commerce data can be protected by performing encryption and decryption process over the M-Commerce data and also protect the user's keys such as private and public key that are used for enhancing key security. Here, keys are protected by applying the encryption process and the decryption process. The pro-posed work achieved more than 98% data security with less time. This work can be extended by the introduction of new and lightweight cryptography algorithms for achieving more security level and minimizes the time taken.

REFERENCES

1. Deepak Kumar, Nivesh Goyal, "Security Issues In M-Commerce for Online Transactions", IEEE, pp.1-6, 2016.
2. Nan li," Research on Diffie-Hellman Key Exchange Protocol", IEEE, pp.1-4, 2016.
3. Himja Agrawal, P.R.Badadapure, "A Survey on Elliptic Curve Cryptography", International Research Journal of Engineering and Technology 3, pp.1-5, 2016.
4. Christina Thomas et al, "A Survey on Various Algorithms Used for Elliptic Curve Cryptography ", International Journal of Computer Science and Information Technologies 5(6), pp.1-8, 2014.
5. Deepika Kamboj et al,"Efficient Scalar Multiplication Over elliptic curve" International Journal of Computer Networks and Information Security 4, pp.56-61 (2016).
6. Khaleel Ahmad and Shoaib Alam," Ecommerce Security through ECC", Sciencedirect.com, pp.1-7, 2016.
7. R Susantio and I Muchtadi-Alamsyah," Implementation of Elliptic Curve Cryptography in Binary Field",, Journal of physics 4, pp.1-10 (2016).
8. Bhattacharya et al, "Improving the Diffie-Hellman Secure Key", IEEE, pp.1-5, 2015.
9. Preetika Joshi et al, "Secure Authentication Approach Using Diffie-Hellman Key Exchange Algorithm for WSN', IEEE, pp.1-6, 2015.
10. Xiuhua LIU,"The Study on E-Commerce based on ECC and SET", IEEE, pp.1-3, 2011.
11. Gayoso Martinez And L. Hernandez Encinas," Implementing Ecc With Java Standard Edition 7", International Journal of Computer Science and Artificial Intelligence 3(4), pp.1-9, 2013.
12. Samaneh Jafari, Leila Khatibzadeh, Zarrin taj Bornaee, "A Multi-Factor Trust Management System based on Confidence in M-Commerce Environment", Second International Con-gress on Technology, Communication and Knowledge (ICTCK 2015) November, 11-12, 2015 - Mashhad Branch, Islamic Azad University, Mashhad, Iran, pp. 524-529, 2015.
13. Subbulakshmi Padmanabhan, V. Sumathi, S. Ganapathy, "Cloud based POS System for Secured Smart Shopping CART using RFID", Journal of Advanced Research in Dynamical and Control Systems 9(Sp.14), pp.2764-2777, 2017.
14. Argyris Constantinides, Marios Belk, Panagiotis Germanakos, George Samaras, "The Per-sonaCheck System for Personalizing M-Commerce Checkout Processes", 2015 16th IEEE International Conference on Mobile Data Management, pp. 303-306, 2015.
15. Balasubramanian Prabhu Kavin, Sannasi Ganapathy, Arputharaj Kannan, "An Intelligent Task Scheduling Approach for Cloud Using IPSO and A* Search Algorithm", 2018 Eleventh International Conference on Contemporary Computing (IC3), pp.1-5, 2018.
16. Md Shoaib Alam, "Secure M-Commerce Data using Quantum Cryptography", IEEE Inter-national Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017), pp. 649-654, 2017.
17. Balasubramanian Prabhu kavin, Sannasi Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications", Computer Networks 151, pp.181–190, 2019.
18. S.Muthurajkumar, S.Ganapathy, M.Vijayalakshmi, A.Kannana, "Secured Temporal Log Management Techniques for Cloud", Procedia Computer Science, Elsevier, Vol.46, pp.589-595, 2015.
19. S. Muthurajkumar, M. Vijayalakshmi, S. Ganapathy and A. Kannan, "Agent based intelligent approach for the malware detection for infected cloud data storage files", Seventh International Conference on Advanced Computing (ICoAC), pp.1-5, 2015.
20. S Muthurajkumar, S Ganapathy, M Vijayalakshmi, A Kannan, "An Effective Intrusion Detection on Cloud Virtual Machines Using Hybrid Feature Selection and Multiclass Classifier", Australian Journal of Basic and Applied Sciences, Vol.9, No.6, pp.38-41, 2015.
21. S Muthurajkumar, M Vijayalakshmi, A Kannan, S Ganapathy, "Optimal and Energy Efficient Scheduling Techniques for Resource Management in Public Cloud Networks", National Academy Science Letters, Springer, Vol.41, No.4, pp.219-223, 2018.
22. Subbulakshmi Padmanabhan, V. Sumathi, S. Ganapathy, "Cloud based POS System for Secured Smart Shopping CART using RFID", Journal of Advanced Research in Dynamical and Control Systems, Vol.9, No.14, pp.2764-2777, 2017.
23. Thangaramya Kalidoss, Ganapathy Sannasi, Sairamesh Lakshmanan, Kulothungan Kanagasabai, Arputharaj Kannan, "Data anonymisation of vertically partitioned data using Map Reduce techniques on cloud", International Journal of Communication Networks and Distributed Systems, Inderscience Publishers, Vol.20, No.4, pp.519-531, 2018.
24. R.Jayanthi, K.John Singh, "Image encryption techniques for data transmission in networks: a survey", International Journal of Advanced Intelligence Paradigms, Inderscience, Vol.12, No.1-2, pp. 178–191, 2019.
25. R.Jayanthi, K.John Singh, "Encrypted image-based data hiding technique using elliptic curve ElGamal cryptography", International Journal of Reasoning-based Intelligent Systems, Inderscience, Vol.10, No.3-4, pp.279–285, 2018.
26. R.Jayanthi, K.John Singh, " A Public Key based Encryption and Signature Verification Model for Secured Image Transmission in Network ", International Journal of Internet Technology and Secured Transactions, Inderscience,2018(In press).

AUTHORS PROFILE

Prabhu Kavin B, is currently pursuing Ph.D in Computer Science and Engineering, VIT-Chennai Campus, Chennai in the area of Cloud Computing and Security. He has completed his M.E. from Anna University, Chennai. He has published 2 papers in journal and conference. His areas of interest are Cryptography, Cloud Computing and Security.

Sannasi Ganapathy, is currently working as Assistant Professor (Sr. Gr) in VIT University, Chennai. He received his M.E and Ph. D degrees from Anna University, Chennai. He has published more than 60 articles in journals and conferences. His area of interest includes Computer Networks, Soft Computing, Cloud Computing and Security.