Developing an Enhanced High-Speed Key Transmission (EHSKT) Technique to Avoid Fraud Activity in E-Commerce

A.B. Hajira Be, R.Balasubramanian
Department of Computer Applications, Karpaga Vinayaga College of Engineering and Technology,
Maduranthagam, India

Article Info

Article history:

Received Jul 30, 2018
Revised Sep 24, 2018
Accepted Oct 11, 2018

Keywords:

Encryption and Decryption
Enhanced High-Speed Key Transmission (EHSKT) Technique
Key Complexity
UUID (Universally Unique Identifier)

ABSTRACT

E-commerce is an emerging and convergence of numerous main information technologies in business practices. E-commerce is an online website where the sale or buys of merchandise ordered electronically. It gives a simple approach to sell items to customers. In the applications suffers payments issues; for example, electronic transactions utilizing Visas or debit cards, net banking, PayPal or different tokens have more consistency problems and are at expanded hazard from being focused than different sites as they suffer more outcomes if there is information loss or modification. An Enhanced High-Speed Key Transmission (EHSKT) Technique is proposed for secure and efficient payment transactions and avoids fraud activity. The proposed system works based UUID (Universally Unique Identifier) to generate a unique id for payment transactions. Proposed system generates Unique id have a combination of number, alphabets, & special character to avoid fraud users. The proposed design reduces the encryption, decryption time and key complexity. Based on Experimental evaluations, proposed methodology reduces 4.73 AD (Average Delay), 23.91 EC (Energy Consumption), 0.95 ET (Encryption Time), 0.85 DT (Decryption Time) and improves 59.8% (Throughput) compared than existing methodologies.

Corresponding Author:

A.B. Hajira Be,
Department of Computer Applications,
Karpaga Vinayaga College of Engineering and Technology,
Maduranthagam, Tamil Nadu.
Email: hajirabe@gmail.com

1. INTRODUCTION

E-commerce is an emerging and convergence technologies in business practices. E-commerce builds everyday life quickly. E-commerce is an online website where the selling or buying of merchandise ordered electronically. It gives a simple approach to sell items to customers. However, there is a lot of competition among different commercial websites sites. At the point when the user interacts on an e-commerce website, they hope to discover what they are searching for rapidly and easily. Additionally, users don't know about the brands or the actual items they want to buy. They have a comprehensive idea of what they need to purchase.

1.1. Problem

E-commerce applications suffer for payments problems; for example, electronic transactions utilizing Visas or debit cards, net banking, PayPal or different tokens have more consistency problems and are at expanded hazard from being focused than different sites as they suffer more outcomes if there is information loss or modification. Although, the government of India has taken positive measures to encourage the fast development of E-commerce by the introduction of cyber laws, decreasing taxes on the framework and so forth. Peoples are hesitating to purchase on lines because of confusions on security and instalment techniques.

There are additionally fakes occurring in credit cards/debit cards which can happen to anyone during online purchasing.

1.2. Background

In Rajan et al [1] exposed the railway ticket reservation system was congested one where the queue for ticket reservation increases and not able to catch train sooner. Dass [2] suggested to audits Indian government initialized unique identity (ID) to all the citizens of India which was a global IT project to provide authority. Yadav [3] described the unique identity innovated to reduce poverty issues, increase the economy, avoids forge identities which emerged process in developing countries like India 2nd place in population. Chander & Kush [4] suggested to a gathering of people's details might be secured in a way to avoid un-authorized person accessing someone's information was a violation, the software tools used to hold these kinds of situations were carried out by administrators keep on tracking network attackers for the security of data. Jadav et al [5] considered about current voting issues in the governance of India where cloud computing technology was providing e-voting procedure that avoided forge identities as well as securing process of linking Aadhaar card for e-voting system.

Bahuguna [6] reviewed on information and security of browsing applications which should be secured and should not allow any other virus or malware into personal computers of users. Varshney & Goyal [7] inspected a solution for money transfer in rural and urban areas where people do not know about online fund transferring, the implemented framework enriched with high security of 3-level authentication allows the user to enter UID, one-time password and fingerprint recognition. Chatterjee & Nath [8] surveyed Indian railway system was a complicated task to manage a large amount of data, the reserved and un-reserved travellers massively high in India whereas seventeen million people travel per day. Anand Shende et al [9] conveyed NoSQL database solution for maintaining millions of UID details securely and retrieve it with minimum time. Henderson-sellers et al [10] examined the electronic signatures of clients gathered on a storage area of central government which ensured authentication service to avoid un-authorized attacker accessing signature records to forge on private assets without any knowledge.

Akhilesh & Srinivasan [11] focused the Indian economic markets of rural areas where every technology depends on the marketer. The agenda was taking innovative technology awareness to the interior of villages, mountain areas for learning new technologies on the market. UIDAI [12] analyzed the importance of Aadhaar card in Indian government to reduce poverty, avoid forge identities and increase economy which ensures efficient in securing public information on secured data-center and innovated for future development of the country. The confidential awareness based on cryptoanalysis for two factor authentication process is presented by [13]. The comparison of various crypto analyses procedures are discussed. In [14], there are three categories of cryptographic algorithms. They are as follows: Hash algorithms, in which hashing functions are used to map data of random or predefined sizes. Symmetric key algorithms, the same cryptographic keys are used for encryption of plain text in the transmitter side and decryption of cipher text in the receiver side. The keys may either be identical or some simple transformations involved between transmitter and receiver sides. An integrated approach combining random key generation and elliptic curver cryptography is discussed [15].

1.3. Objectives:

The paper objectives are following as:

a) To develop an Enhanced High-Speed Key Transmission (EHSKT) Technique for secure and efficient payment transactions and avoids fraud activity.
b) To apply privacy mechanism to maintain traders & customer content profile management
c) To design effective & secure information retrieval in E-commerce for traders and as well as customers.
d) To minimize the encryption and decryption time, average delay, energy consumption & improve the success rate of proposed method compare than existing approaches

2. METHOD

In the section illustrates the proposed methodology details, Implementation pre-processing steps, and implemented algorithm details that provides secure and efficient payment transactions and avoids fraud activity and minimizes the average delay, encryption time, decryption time, energy consumption and key complexities and improve throughput. Figure 1 demonstrates the working principle of the proposed algorithm with implementation processing steps and mathematical evaluation details. The pre-processing implementation steps are explained below in details. The research aims to design a Web-based secure framework for an Enhanced High-Speed Key Transmission (EHSKT) Technique is proposed for secure and efficient payment transactions and avoids fraud activity. In the current scenario, E-shopping is rapidly going to increase day-day. The proposed framework takes care the privacy of the user, trader, trader information and payment process.

The technique also dedicates to offer effective smart way privacy to avoid the complexity of applications & burden of customers. The proposed system works based UUID (Universally Unique Identifier) to generate a unique id for payment transactions. Proposed system generates. Unique id has a combination of number, alphabets, & special character to avoid fraud users. In the technique provides facility to user for utilizing multi-banking account transaction at single place. The proposed system highly dedicated to avoiding fraud entry and un-authorized users. The secret key is used to reflect the access mechanisms so that the authorized user can be able to validate the transaction if and only if the transaction attributes to fulfill the criteria of secret key access.

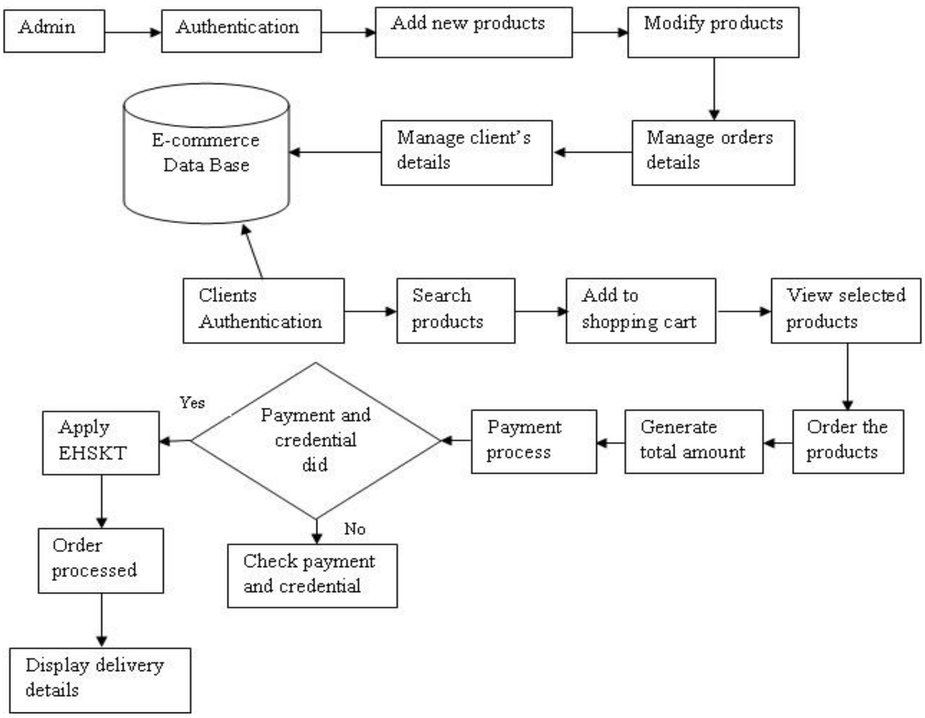

Figure 1. Working Principle of the Proposed Algorithm

2.1. Implementation Pre-processing Steps

2.1.1 Admin Module

In the admin module, adding the new products, different kinds of products and what are all the products offered in that store. The admin changes the products and deletes the products, and it maintains everything day by day. The admin can manage the order information and client information.

2.1.2 Searching Process

In the module, the client will permit to search the shopping store products before login. It displays the name and other related data concerning the online shopping store and when the clients choose the ordering choice in ordering segment, and it illustrates the criteria of exhibiting the products.

2.1.3 User Authentication

Login: The client will be permitted to log on at the initiating the shopping application or at the shopping giving their e-mail address as username and password. The client logs on to starting the application; the client provided the selection of ordering the equal to the last time with a total view of the shopping and also to modify if needed by the client to make a new order. Adding extra products to take the amalgamation of the clients earlier order products and demonstrate the authentication.

Registration: In the module, clients will be permitted to provide their input details and postcode to store the database, and it verifies whether the stored data to delivers the order utilizing the postcode. The verification provides correct, and the order can be delivered to the client's address. The client needs to fill a registration containing all the essential details that are needed to complete the order dispatch.

2.1.4 View Shopped Products

At any time, the clients will be able to view his/her shopped products that are added to the cart. At the same time it also able to modify and remove and individual and group products from the shopping cart list. It will be an option for the clients to add or remove the quantity of individual products in the shopping cart. The authenticated clients only buy the products and added to shopping cart. But the non-authenticated clients just view the products and its descriptions.

2.1.5 Shopping Cart

In the shopping cart to permits to the clients to include individual products or group of products and it automatically modify the full amounts and others. The clients to remove individual products or group products from the shopping cart and it will modify the total amount and others.

2.1.6 Order process

In the module, clients order is processed. A client requires buying products and it can place the order for the products. The postcode validation can be done to confirm the dispatch at clients place. The dispatching details and the address at which the product should be delivered are provided.

2.1.7 Payment process

In the payment module options for the order is provided and processed. Payment should be through credit card, debit card and net banking. The total amount is the addition of cost of the products and dispatch charges will be deducted from the clients account in case of payment options other than cash on delivery.

2.2. Enhanced High-Speed Key Transmission (EHSKT) Technique

An Enhanced High-Speed Key Transmission (EHSKT) Technique is proposed for secure and efficient payment transactions and avoids fraud activity. The proposed system works based UUID (Universally Unique Identifier) to generate unique id for payment transactions. Proposed system generates Unique id have combination of number, alphabets, & special character to avoid fraud users. In the technique provides facility to user for utilizing multi-banking account transaction at single place. The proposed system is highly dedicated to avoid fraud entry and an-authorized users. The approach enhances the RSA algorithm with the key length 4096 which is more effective for secret key generation and key distribution insecure medium. Here, User's secret key used to reflect the access mechanisms so that the authorized user can able to validate the transaction if and only if the transaction attributes to fulfill the criteria of secret key access. Data are generally assumed to be either vertically or horizontally partitioned. In the case of horizontally partitioned data, different sites collect the same set of information about different entities. Proposed system produced security according to data attributes. The proposed design reduces the encryption, decryption time and key complexity. The Proposed designed have following process:

a) *Setup*: In the algorithm takes input parameter is set of number, alphabets and special character k and revert the public key PK as well as a user secret key USK. PK is utilized for unique transaction id generation.
b) *Secret Key Generation:* In the algorithm will take input K for access structure A and the user secret key USK. Here, in the approach provides secret key SK which enables the user to validate the transactions for respective users. USK utilized for generating the key by an authorized user only.
c) *Transactions Validations:* It receives the input from users with their secret key SK to proceed for payment validation process for key access structure A. The proposed method performs payment transaction validations, if and only if the set of payment attribute confirms the user secret key access structure A.The pseudo code of proposed algorithm is given below in details:

```
The Input: Take input parameters set of number, alphabets and special character k
Output: UUID base Secret key SK
Procedure:
 Start;
            Start the applications;
            Enter the necessary attributes for transactions process;
            Proceed for Enhanced UUID based secret key SK generations;
            Take the parameters K;
            Proceed for computations;
                If computation process completed;
                    Then SK generated from access structure A;
                    Proceed for transaction and payment process is completed;
                    Initialize the transaction validation process;
```

```
        Enter the secret SK for validation;

    **If** SK is validated then

        Transaction is completed, and SK is taken from access structure A;
    **Else**
        Unauthorized users and process is declined;
    **Else**
        Restart the process;
    **End**
```

3. RESULTS AND DISCUSSION

3.1. Programming Setup

To evaluate, the proposed system with existing approaches, the deployment process conducted on a laptop with Intel Core i7 7600 processor, 16GB memory, and Window 7 Ultimate system. Here, this method implemented in JAVA using NetBeans 8.0 with Apache Tomcat 8.0.3 and MYSQL 5.5 Database. The Proposed algorithm is evaluated with transaction processes in the financial domain to check the efficiency of proposed mechanisms. For applying and validating the transactions, the proposed method is used centralized & implementation done in JAVA.

3.2. Performance Metrics

In the phase, proposed method explores the performance metrics to improve the security for secure payment in financial transactional process. Table 1 displays following evaluation parameters separately such as average delay, throughput, energy consumptions encryption time & decryption time.

Table 1. Performance Metrics

Metrics	Description	Formula
Average Delay	Time difference between the current data packets received and the previous data packets received	$Average\ Delay = \frac{Pkt\ Recvd\ Time - Pkt\ Sent\ Time}{time}$
Throughput	Average of successful data delivered to the destination	$Throughput = \frac{\sum_{0}^{n} Pkts\ Received\ (n) * Pkt\ Size}{1000}$
Energy Consumption	Difference between the initial energy and the residual energy over the simulation time	Energy T_x = (330*data Size)/2*106 Energy R_x= (230*data Size)/2*106
Encryption Time (ET)	Total time to produce a cipher text from plain text	$EP = \left(I, CT\{\mathrm{EP}_{\mathrm{i}}\}i\varepsilon \mathrm{I}\right)$
Decryption Time (DT)	Total time to produce plain text from encrypted text	$EP(\mathrm{EPi},\ \mathrm{ski}) = EP(g, g)^{\mathrm{pi(0)s}}$

Where,
Pkt – Packet Rx - Residual Energy EP - Encoding Process
Recvd - Received I - Attribute Set sk - Secret Key
Tx - Initial Energy CT - Cipher Text

3.3. Result

Table 2 explains the Average Delay, Throughput, Energy Consumption, Encryption Time, and Decryption Time for several input constraints with previous methodologies. The proposed methodology calculated on various kinds of algorithms like DES, AES, and BF, with closest existing approaches. Based on tabular result observation, it can be said that the proposed method performs well compare than existing techniques. The proposed framework calculated by following existing methodologies namely: Data Encryption Standard (DES) [16], Advanced Encryption Standard (AES) [16] and Blow Fish (BF) [16] methodologies. According to Table 1, it noticed that EHSKT has the best score on each particular factor.

Table 2. Average Delay, Throughput, Energy Consumption, Encryption Time, Decryption Time for E-Commerce

Algorithm	Average Delay (s)	Throughput (Kbps)	Energy Consumption (Joules)	Encryption Time (s)	Decryption Time (s)
DES	48.7766	28.13	83.087	0.434	0.451
AES	49.1367	5.27	72.087	0.214	0.221
BF	48.7349	35.2	85.544	0.262	0.253
EHSKT	13.334	95.16	48.168	0.119	0.136

According to Figure 2 to 5 observations, the proposed technique is estimated based on average delay, throughput, encryption time, energy consumption, and decryption time. Proposed EHSKT is computed with Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blow Fish (BF) methodologies behalf of on average delay, throughput, encryption time, energy consumption, and decryption time. BF is the closest challenger. AES provided the data confidentiality, integrity. AES fails to decrease key complexities, and it easily broke the important key privacy. EHSKT improved the security for secure and efficient payment transactions and avoids fraud activity. Proposed EHSKT reduces 4.73 AD (Average Delay), 23.91 EC (Energy Consumption), 0.95 ET (Encryption Time), and 0.85 DT (Decryption Time) and improves 59.8% (Throughput). Finally, the paper claims the proposed EHSKT methodology performs best on every evaluation matrix & respective input parameters. In conclusion, it claims the proposed EHSKT strategy is best of several overall factors.

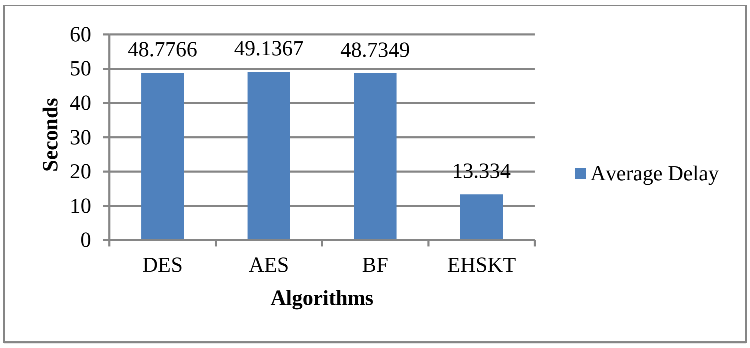

Figure 2. Average Delay of E-commerce

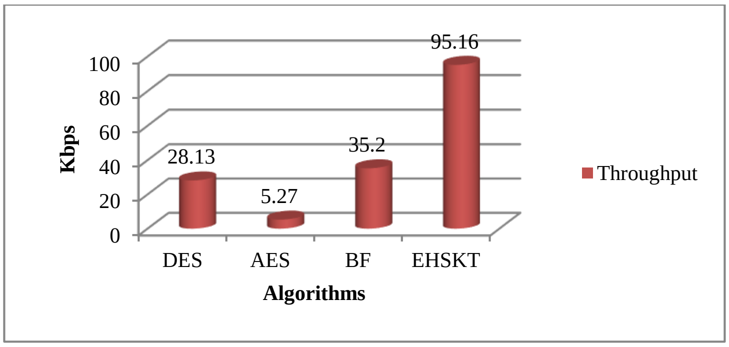

Figure 3. Throughput of E-Commerce

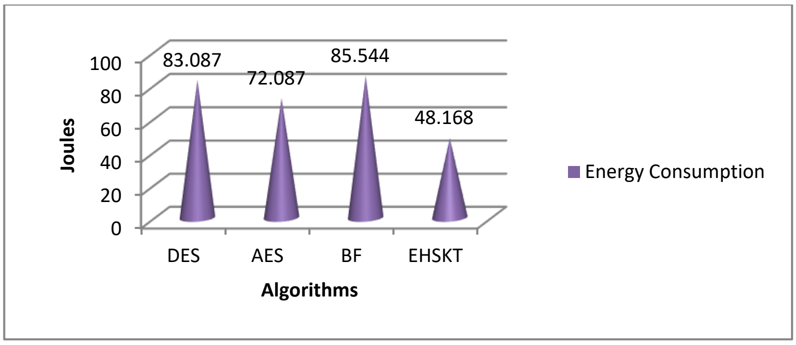

Figure 4. Energy Consumption of E-Commerce

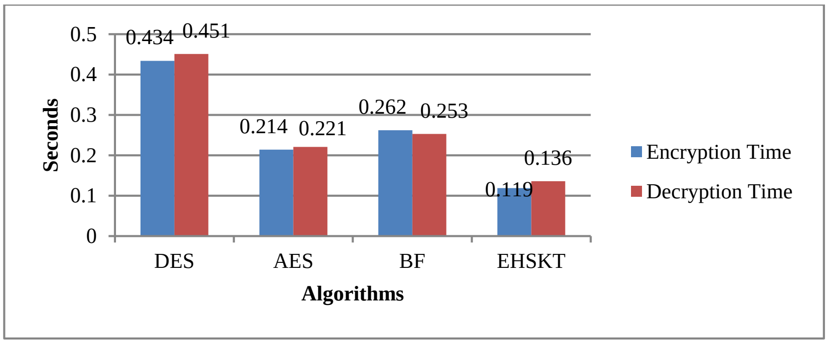

Figure 5. Encryption time and Decryption time of E-commerce

4. CONCLUSION

In In modern business, the main resource is a World Wide Web, and it provides new opportunities for business. E-commerce is an online website where the selling or buying of merchandise ordered electronically. In the paper developed an Enhanced High-Speed Key Transmission (EHSKT) Technique for secure payment transactions and avoids fraud activity. The privacy mechanism maintained traders & customer content profile management. Proposed methodology improved the throughput of secure and efficient payment transactions and avoids fraud activity. Proposed EHSKT reduces 4.73 AD (Average Delay), 23.91 EC (Energy Consumption), 0.95 ET (Encryption Time), and 0.85 DT (Decryption Time) and improves 59.8% (Throughput). Finally, the paper claims the proposed EHSKT methodology performs best on every evaluation matrix & respective input parameters.

In future work may be done for large size of video files and different size of keys to investigate best methodology to produce best performance results.

REFERENCES

[1] Rajan, M. T., Vincent, A. J., Prakash, G., Prakash, N., & JU, R. M., “Computerized RTBS System”, *International Journal of Emerging Engineering Research and Technology*, vol. 2, no. 2, pp. 25-29, 2014.

[2] Dass, R., “Unique Identity Project in India: A Divine Dream or a Miscalculated Heroism?”, *Indian Institute of Management*, 2011.

[3] Yadav, V., “Unique identification project for 1.2 billion people in India: can it fill institutional voids and enable 'inclusive' innovation?”, *Contemporary Readings in Law and Social Justice*, vol. 6, no. 1, pp. 38, 2014.

[4] Chander, S., & Kush, A., “Unique Identification Number and E-Governance Security”, *International Journal of Computing and Business Research*, vol. 1, no. 1, 2010.

[5] Jadav, M. B., Desai, M. A., Patel, M. F., & Patel, M. R., “Cloud Computing E-Voting: A Technical Review”, *Int. J. Res. Emerg. Sci. Technol*, vol. 2, pp. 8-13, 2015.

[6] Bahuguna, A., “FIRe: Firefox for Computer Security Incident Reporting and Coordination”, *IITM Journal of Management and IT*, vol. 6, no. 1, pp. 3-11, 2015.

[7] Varshney, D., & Goyal, D., “UID based Mobile Money Implementation in Rural Areas of India”, *International Journal of Research in Engineering & Advanced Technology*, vol. 1, no. 6, 2014.

[8] Chatterjee, P., & Nath, A., “Smart Computing Applications in Railway Systems-A case study in Indian Railways Passenger Reservation System”, *International Journal*, vol. 3, no. 4, 2014.

[9] Anand Shende, Omkar Gurav, Swapnil Shirode, Piyush Govekar, and S.N.Zaware, “Secure Unique Identification using Encrypted Storage in NoSQL Database”, *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 4, 2016.

[10] Henderson-Sellers, B., Firesmith, D. G., Bock, C., & Odell, J., “ESIGN”, *Journal of Object-oriented Programming*, vol. 11, 1998.

[11] Akhilesh, K. B., & Srinivasan, R., “Driving the economy through innovation and entrepreneurship: Emerging agenda for technology management”, 2013.

[12] C. Mukhopadhyay, A. Gurtoo, P. Ramachandran, P. P. Iyer, M. Mathirajan, & M. H. B. Subrahmanya (Eds.). *Springer India. AUTHENTICATION*, UIDAI, 2011.

[13] Choi, Younsung. "Cryptanalysis on Privacy-aware two-factor Authentication Protocol for Wireless Sensor Networks." *Indonesian Journal of Electrical Engineering and Computer Science,* Vol. 8, no. 2, pp. 296-301, 2017.

[14] Singh, Pooja, and R. K. Chauhan. "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN." *International Journal of Electrical and Computer Engineering,* Vol. 7, no. 4, pp. 2232, 2017.

[15] Gayathri, P., Syed Umar, G. Sridevi, N. Bashwanth, and Royyuru Srikanth. "Hybrid Cryptography for Random-key Generation based on ECC Algorithm." *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 7, no. 3, pp. 1293-1298, 2017.

[16] Sahu, S. K., & Kushwaha, A., “Performance Analysis of Symmetric Encryption Algorithms for Mobile Ad hoc Network”, *International Journal of Emerging Technology and Advanced Engineering,* vol. 4, no. 6, pp 619-624, 2014.