A Novel High-Speed Key Transmission Technique to Avoid Fiddling Movements in e-Commerce

A.B. Hajira Be[1]
Ph.D Research Scholar
Department of Computer Science, Mother Teresa Women's
University, Kodaikanal, Tamilnadu, India

Dr. R. Balasubramanian[2]
Professor & Dean
Department of Computer Applications, Karpaga Vinayaga
College of Engineering and Technology,Maduranthagam
Taluk, Tamilnadu, India

Abstract—**To prevent fraud in e-shopping, the High-Speed Key Transmission Technique (HSKT) is primarily focused on safe and effectual transactions of payments and product content. The privacy of users, traders, trader information, product content, and the payment procedure are all protected by this framework. High speed key transmission is also committed to providing an effective, sensible approach to privacy in order to minimize the complexity of applications and the load on consumers. This paper proposes a new key transmission technique that allows users to conduct multi-banking account transactions from a single location. The proposed system is devoted to preventing unwanted people from gaining access. The secret key is used to represent access mechanisms, allowing authorized users to verify the transaction if and only if its characteristics meet secret key access requirements. Finally, the proposed high-speed key transmission technique (HSKT) improves the chances of success and throughput by reducing the time it takes to decrypt and encrypt, the amount of energy it uses, and the average delay.**

Keywords—Secret key; encryption; decryption; transaction; HSKT

I. Introduction

Payment issues plague e-commerce applications including electronic transactions using Visa otherwise debit cards, net banking, PayPal, or other tokens take more inconsistency issues since it is more vulnerable to being targeted. To prevent fraud in E- shopping, the high-speed key transmission method (HSKT) is primarily focused on safe and efficient payment processes and product content [1-5]. The privacy of users, traders, trader information, product content, and the payment procedure are all protected by this framework. HSKT is also committed to providing an effective, sensible approach to privacy in order to minimize the complexity of applications and the load on consumers. This method allows users to conduct multi-banking account transactions from a single location. This system is devoted to preventing unwanted people from gaining access [6-10].

The secret key used to represent access mechanisms, allowing authorized users to verify the transaction characteristics meet secret key access requirements. Finally, HSKT reduces decryption and encryption time, energy consumption, average delay, and increases achievement rate and throughput compared to other sites, which incur greater consequences if information is lost or modified. Although, the Indian government took positive steps encouraging rapid expansion of E-commerce enacting cyber-laws, by lowering framework taxes. People are hesitant to make online purchases due to concerns about security and installation methods [11]. Additionally, there are fraudulent debit cards and credit cards that happens to anybody when shopping online.

E-commerce applications suffer from payment problems; for instance, automated transactions using Debit cards or Visa, PayPal or Net banking, or methods by the way of other tokens partake added consistency issues and are more likely to be targeted than other sites because they suffer more consequences if information is lost or modified. Although, the Indian government has made significant steps to promote the rapid growth of E-commerce by enacting cyber legislation, lowering framework taxes, and so on. People are hesitant to make online purchases due to concerns about security and installation methods.

A. Objectives

The resulting ones are the main objectives of this work:

- To create a High-Speed Key Transmission (HSKT) technique that will allow for safe and quick financial transactions while preventing fraudulent behavior.
- To use a privacy method to keep track of traders and consumer content profiles.
- To provide an E-Commerce information retrieval system that is both effective and secure for both merchants and consumers.

To enhance the suggested method's success rate by reducing encryption and decryption time, average delay, and energy usage when compared to current methods.

II. Literature Review

The term "cryptography" comes from the Greek and means "the process of making data unintelligible." This prevents an unauthorized user from getting their hands on sensitive information. To put it another way, it's a method for concealing data in transit [12]. As soon as the transmitter uses cryptographic methods and a particular key to turn the data into cypher text, it is sent to the recipient. Encryption is the name given to this technique. To decrypt a message, the receiver uses a known key to decipher the ciphertext. Decryption is the term for this step.

There are two types of cyphers known as symmetric (or secret) and asymmetric (or public). In order to accomplish security, each of them makes use of a discrete and distinct set of techniques. Symmetric key cryptography focuses on the structure of simple repeated cryptographic processes, while asymmetric cryptography relies on the complexity of a mathematical problem [13].

To save energy, network designers should employ symmetric key cyphers to encrypt data sent by sensor nodes. Due to resource limits, standard cryptographic techniques cannot be used on sensor nodes. For these networks, a key management method provides the best security. Before exchanging information, nodes must safely exchange keys. The key management is a multi-operational approach where the initial key is produced, then disseminated and traded across the nodes, then utilized by the sender and recipient, and finally abandoned and renewed. Thus, key management system essential processes are: creation, distribution, exchange, usage, abolish, and refresh. WSNs are managed in several ways [14].

Conventional public-key cryptosystems have a major drawback in that in order to provide the high degree of security required, the key size must be suitably big [15]. In the third place, we have hybrid key cryptography, which brings together symmetric and public key elements. It combines the best features of the two approaches. Public-key cryptography (PKC) has been demonstrated to be a viable method of encrypting data[16].PKC is gaining traction in WSNs because it is capable of solving two basic and challenging challenges, namely authentication and symmetric key distribution, using DSA and Diffie-Hellman key exchange [17][18]. For sensor nodes with limited resources, ECC is an excellent choice since it has less overhead than RSA, but ECC operations are still hefty [19]. ECC is superior to RSA in terms of security [20].

III. Proposed Methodology

It concentrated on the cryptography algorithms. The reader can get a clear comparison of the key length and the analytical view of the cryptography methods to be utilized in the real-time applications utilizes the model. Where, AES, DES and Blowfish algorithm are discussed details with their key generation, key comparisons, encryption and decryption process. All conventional method is evaluated on regular postponement, energy intakes, throughput, encryption and decryption time. Blowfish algorithm is more secure for increasing the key size. It compared to other symmetric key algorithms and offered less processing time and rounds [21-25].

The secure and efficient payment transaction (SEPT) approach aims to prevent hackers from tracing one's online transaction. Initially, entering account numbers are very simple. Hence, the system gathers account numbers with allotted password details. Next, due to a multi encryption method, consumer will receive interim password for activating the account. Finally, Aadhar number should be entered to validate the consumer profile verifications and activate the account for further transactions [26-30].

A. Implementation Preprocessing Steps for SEPT

Implementation preprocessing steps are as follows Authentication process, Purchase Request, Authorization Demand, Authorization Response, Cardholder Authentication Demand, Cardholder Authentication Response and Ending Payment and Secure and Efficient Payment Transaction (SEPT) Approach.

The system has highly concentrated on the secure and efficient payment transactions to avoid fraudulent action. The study's primary goal is to provide an effective smart method to protect privacy while avoiding the complexity of apps and consumer burden. The study explains about HSKT algorithm with their system workflow, implemented modules, the implementation details, mathematical proof, operational details, and dataflow diagram. It explains the implementation, logical, analytical, and view of HSKT.

The HSKT method is used to get a clear concept of the logical and the analytical view of the proposed HSKT method for implementing in the real-time e-commerce applications. The proposed methodology ensures secrecy and efficiency in payment transactions of product content to avoid fraudulent activity in e-commerce.

B. Implementation Pre-Processing Steps for EHSKT

Implementation preprocessing steps are as follows Admin, Product Upload Module, Product Update and Product History, User Authentication, Product Search, View Shopped Products, Order Process and Payment Process. For safe and quick financial transactions, as well as to prevent fraudulent behavior, a High-Speed Key Transmission (HSKT) Technique is suggested. The suggested method generates a unique id for financial transactions using a UUID (Universally Unique Identifier). To prevent fraud, the proposed system produces a Unique ID (Identifier) that consists of a mix of numbers, alphabets, and special characters. This method allows users to conduct multi-banking account transactions from a single location. The suggested system is devoted to preventing fraud and unauthorized users.

The approach enhances the RSA methodology by using a 4096-bit key length, which makes it more successful for creating and distributing secret keys in hazardous settings. The secret key of authorized user is used to represent access mechanisms in this case, allowing transaction to be verified if and only if transaction features satisfy secret key access criteria. Vertical or horizontal partitioning of data is often anticipated. In case of horizontally partitioned data, several places collect the same set of information about distinct entities. The proposed system created security based on data attributes. The suggested method reduces the time required for encryption, decryption, and key complexity. The suggested design approach is as follows: Setup:

The method accepts a collection of numbers, alphabets, and a special character k as an input parameter and reverses public key PK and user secret key, USK. For the creation of unique transaction IDs, PK is used.

1) Secret key generation: Generating two large random prime numbers h and k and it has approximately equivalent size to item N = hk necessitated 4096 bits length. Computing N=secret key exponent SE, 1<SE<ϕ becomesiSE=1modϕ. The private key is (SE, h, k) and public key is (N, i). Maintain all the values of SE, h, k and ϕ secretly. When using SE, the private key is sometimes expressed as you need as the value of N. We could write the key pair as ((N, I SE) at other instances.

Modulus is a term that refers to the number N. The exponent is also known as the public exponent, encryption exponent, or simply exponent. The secret key exponent (SE) is also known as the decryption exponent.

This method will utilize the access tree structure h and k as well as the user secret key USK as inputs. This method uses a secret key or signature S that allows the user to verify transactions for specific users. Only an authorized user may generate using USK. Transactions Validations:

The user has the ability to make modifications, such as generating a message digest of the material to be shared. Exponent DE between 1 and N-1 is used to represent this message or content digest. Calculates the signature S=DESE mod N using the private key (N, SE) and sends it to the recipient. On the receiver's side, calculate integer x=Si mod N using the sender's public key exponent (N, I Calculates the message or content digest of the data that has been signed independently. It calculates the expected representative integer x′ by encoding the expected message digest if x=x′, the signature is correct.

It takes user input together with their signature S in order to initiate the key access structure's payment validation process. The suggested method validates payment transactions if and only if the set of payment characteristics matches the user signature in the access tree.

2) Encryption: The user may get the receiver's public key and represent the plaintext content as a positive integer PI with 1PIN, compute the ciphertext CT=PIi mod N, and send the ciphertext to the receiver in the following methods.

3) Decryption: Based on the size of SE and N, the receiver uses his/her private key (N, SE) to compute PI=CTSE mod N using his/her private key (N, SE). It retrieves plain text from a message or a PI that represents content.

C. Working with EHSKT Technique System Constraints

H and K are two important prime numbers with bit widths of 4096 that are kept hidden. The size difference between the two sizes must be large enough in the security scenario.

N = H *K, ϕ= (H −1) (K −1), and ϕ is kept secret. Our software utilizes a 4096 bit modulus EHSKT implementation.PI can use only positive integer, but then great general separation with respect to N and ϕshould bw 1. SE * i ≡ 1 mod ϕ where i is an integer.

PK (PI, N) referred as public key PK, whereas SK (SE, N) is the private key. Considering PT equals plaintext, (PTPI) SE ≡ PT mod N ≡ PT mod H, PT mod K.

Process

Encryption: CT =Enc (PI, PT) = PTPI mod N.

Decryption: PT = Dec (SE, CT) = CTSE mod N = CTSE mod H, CTSE mod K.

Operations

Choose two big prime numbers and calculate N and ϕ.To speed up encryption select PI=3. Depended on PI and N then SE can be estimated. "Calculate PTkey mod H, PTkey mod K, where the key can be PI as well as SE.

Forϕ= (H–1) (K–1) is even, PI may be tried from 3. As a result, PI can be raised by 2 once.

The following is an example of a PI computation algorithm:

```
BigIntegerComputePI(BigIntegerϕ)
{
BigInteger PI=3; BigIntegerdivision=0;
While (GCD( ϕ,PI)!=1) // Here Greatest Common Divisor is the function to calculate the greatest common division of two integers, and it can be executed with EuclidAlgorithm.
{ PI=i+2;
}
Returni;
}
GeneratePublicKey (BigInteger PI)
{
BigInteger one = BigInteger.ONE; BigInteger two = one.add(one); BigInteger key = one.add(two); while(PI.GCD(key).compareTo(one) != 0)
{
key = key.add(two);
}
Return key;
}
GeneratePrivateKey (BigInteger N, BigInteger DE)
{
return DESE mod N; // SE is secret key exponent
}
publicBigInteger Encryption(BigInteger□)
{
powerModule(□)
Encryption CT= PTPI mod N
}
publicboolean Decryption(BigInteger CT, BigInteger SK)
{
BigInteger VS = powerModule(SK); if(VS.compareTo(SK) == 0) return true; Decrption PT=CTSE mod N;
return false;
}
publicbooleanVerifySignature(BigInteger CT, BigInteger SK)
{
BigInteger VS = powerModule(SK); if(VS.compareTo(SK) == 0) return true; return false;
}
}
```

IV. Result and Discussion

A. Comparative Analysis of Closest Conventional Approaches

For safe payment in financial transactional processes, DES, AES, and BLOWFISH are used. As shown in Table I, it also supports the suggested technique for reducing delay, encrypting time, energy usage, decryption time, and increasing throughput, and it was discovered that blowfish has the best score for each given constraint for the corresponding parameter.

The suggested method is evaluated based on average delay, throughput, encryption time, energy consumption, and decryption time, as shown in Fig. 1. Based on average delay, throughput, encryption time, energy consumption, and decryption time, Blow Fish (BF) is calculated using Data Encryption Standard (DES) and Advanced Encryption Standard (AES) methods. The nearest competitor is AES. The data confidentiality and integrity were supplied by AES. AES fails to reduce key complexity, and it readily compromises key privacy. Blow Fish (BF) has enhanced security for safe and fast financial transactions while also preventing fraud. Blow Fish (BF) improves 7.02 percent by 0.40 AD (Average Delay), 2.45 EC (Energy Consumption), 0.52 ET (Encryption Time), and 0.68 DT (Decryption Time) (Throughput). Finally, the article argues that the Blow Fish (BF) algorithm is the best.

B. *Comparative Analysis of Closest Conventional Approaches using RSA*

The RSA (1024) and RSA (2048) key length is used for secure and efficient payment transaction process. It also supports proposed methodology for minimizing the average delay, encryption time, decryption time as shown in Table II seen that RSA (2048) shows best score on every specified constraint for the respective parameter.

TABLE I. ENCRYPTION TIME, DECRYPTION TIME FOR E-COMMERCE AVERAGE DELAY, THROUGHPUT, ENERGY CONSUMPTION

Algorithm	**Encryption Time (s)**	**Decryption Time (s)**	**Average Delay (s)**	**Throughput (Kbps)**	**Energy Consumption (Joules)**
AES	0.314	0.321	49.1367	5.27	72.087
DES	0.434	0.451	48.7766	28.13	83.087
BF	0.262	0.253	48.7349	35.2	85.544

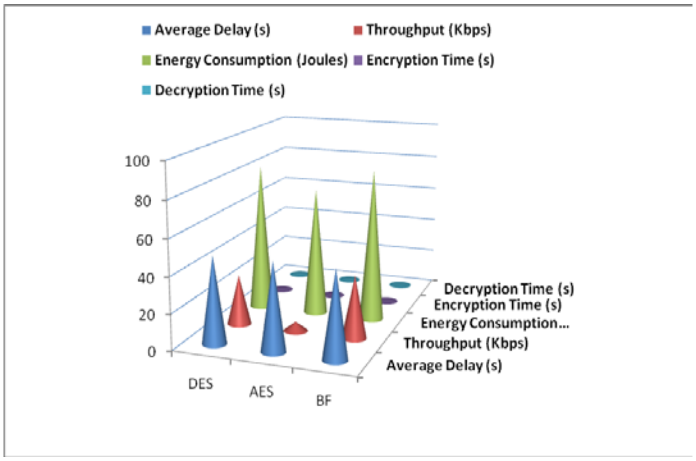

Fig. 1. Encryption Time, Decryption Time for e-Commerce Average Delay, Throughput, EnergyConsumption.

Based on the observation of Fig. 2 is estimated RSA algorithm utilizing key length of 1024 and 2048 bits. The RSA algorithm set the public exponent keys 1 to 3. Since, it offers better performance in key validations. The public exponent is generally utilized in constrained surroundings anywhere various validations have to occur. The results utilizing other exponents, key generations are more proficient, and validations are efficient. Finally, the performance of the RSA algorithm is good for security.

The cryptography method is used for the protection of information. These methods are utilized for decryption and encryption process over information. The Secure and Efficient Transaction System through RSA algorithm set the public exponent keys and it offers better performance in key validations. The public exponent is generally utilized in constrained surroundings, anywhere various validations have to incur security.

It concentrates on the secure and efficient payment transaction system and subsequently formulates new criterion functions for secure payment framework. It also prohibits hackers from tracing one's online transaction. The proposed system works based on Aadhar for secure payment transaction systems. Here, Aadhar act as a unique identification number (UID). The design narrated above in this chapter, is utilized to get a clear idea of the logical and analytical view of the proposed Encryption and Decryption process of Secure and Efficient Transaction System through Aadhar approach for real-time applications. The study explains the secure payment system through Aadhar ID for internet or web-based business using secure and efficient payment transaction with RSA algorithm process flow, mathematical steps. The system workflow diagrams and security of payment system details are displayed. It explains the implementation, logical, analytical, and mathematical view of secure and efficient payment transaction algorithm. Here RSA algorithm uses 2048 key size. It enhances protection for secure payment process.

TABLE II. DECRYPTION TIME, AVERAGE DELAY AND ENCRYPTION TIME

Algorithm	**AverageDelay (s)**	**EncryptionTime (s)**	**Decryption Time (s)**
RSA(1024)	2.5	4.52	3.12
RSA(2048)	2.9	5.13	4.13

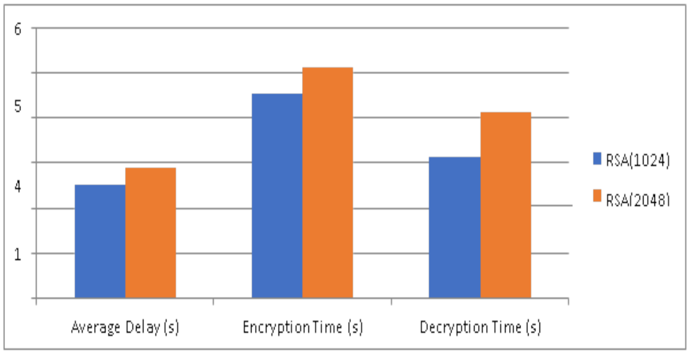

Fig. 2. Decryption Time, Average Delay and Encryption Time.

C. Simulation Result

The proposed technology represents a mathematical model to estimate the performance of Customer Success Rate, Mean of Transaction Time (MTT), and Reliability (R) to find the effectiveness of Secure and Efficient Payment Transaction with Aadhaar technology. The proposed technology expresses the payment process in secure and efficient way in e- commerce applications.

1) Customer success rate (CSR): The customer success rate refers to the person's discernment that utilizing a specific framework to deal with. It considered one of the most influential features behalf of new technology adoption like as the customer success rate. It has an effect on the attitude, self-viability, and instrumentality with utility. The impact of the perceived customer success rate has been exhibited in various database forums with various setting. The customer success rate is depending upon the attitude and aim whose details are explained in equation (1).

$$\mathrm{CSR} = \frac{T_{F_R}+T_{J_u}}{T_F+T_{I_1}+FT_F+FT_{I_I}.} \tag{1}$$

Where, TF Transaction Fail, TT is Transaction True, FTF is False Transaction fail and FTT is False Transaction True. This derivation notifies that CSR mostly based on some features condition.

2) Mean of transaction time (MTT): The mean of transaction time is estimated by separating the total value of all exchanges by the number of exchanges or sales. This can be estimated on a day-day, month to month or yearly premise. The mean of transaction time is exhibited in equation (2).

$$MTT = \frac{\text{Total Transaction Value}}{\text{Number of Salele.}} \tag{2}$$

3) Reliability (R): A client's total number of partnerships with an organization and its products. Client experience management is a fundamental component of client relationship management. The client's overall impression of the organization and contributions is reflected in the overall experience. In equation, the suggested approach provides a mathematical model for Reliability (R) (3).

$$\text{Reliability} = \text{Performances of Process} - \text{Exceptation of Products} \tag{3}$$

Table III represents the Customer Success Rate, Mean of Transaction Time (MTT) and Reliability (R) with payment data for secure and efficient payment transactions. The proposed technology displays their average values for respective parameters with the respective data. The SEPT with Aadhaar technology is evaluated with the existing technology; namely, POS (Point of Sale), Mobile-based technology, Micro-ATM, Kiosk. According to Table III, it noticed that SEPT approach is best method compare than other existing method that have the best result on every specific aspect for the respective parameter.

Based on Table III, the proposed technique SEPT with Aadhaar ID computes Customer Success Rate, Mean of Transaction Time and Reliability for identifying the effectiveness of the technology. Fig. 3 shows the payment processing of CSR,R and MTT values. The proposed method is evaluated with POS payment technology, Mobile payment technology, Micro-ATM payment technology and Kiosk payment technology existing method on behalf of Customer Success Rate, Mean of Transaction Time, and Reliability. The POS technology depended on resolutions with or without Smart Card for payment process. A customer to offer their payment data in the transaction for a product or service utilizes it. However, there are many forms of POS frameworks utilized in numerous company types and it have privacy problems. The proposed method is providing efficient schemes for secure payment transaction process. Micro ATMs permit clients to perform fundamental economic exchanges utilizing only their unique number and fingerprint as unique evidence (according to a Bank Identification Number for inter-bank exchanges). However, it has manual access to all submitted document works. Kiosk payment technology is banking resolutions utilizing little bandwidth Internet for connectivity. However, it fails to maintain customer success rate and transaction time of payment process. The mobile payment technology is the nearest competitor on overall parameters. Mobile-based technology for transaction achievement will be able to meet their requirements and expectation much better than other delivery resolutions or platforms. However, it fails to maintain security and transaction time for all most cases. Proposed technique reduces 0.6 MTT (Mean of Transaction Time) and improves 0.9% (Reliability) and 0.9% of CSR (Customer Success Rate). Finally, the study concluded that the suggested SEPT technique outperforms all other evaluation matrices and input characteristics. As a result, the SEPT is the best technique in terms of overall characteristics.

TABLE III. AVERAGE CUSTOMER SUCCESS RATE (CSR), RELIABILITY (R) AND MEAN OF TRANSACTION TIME (MTT) FOR 50 USER PAYMENT PROCESSING WITH VARIOUS SIZE OF TRANSACTION RECORD SIZE

Technology	**CSR**	**MTT**	**Reliability**
POS	4.05	2.6	3.6
Mobile	1.8	1.5	2.24
Micro-ATM	3.4	2.4	3.2
Kiosk	2.9	2.1	2.51
SEPT	4.95	0.9	4.5

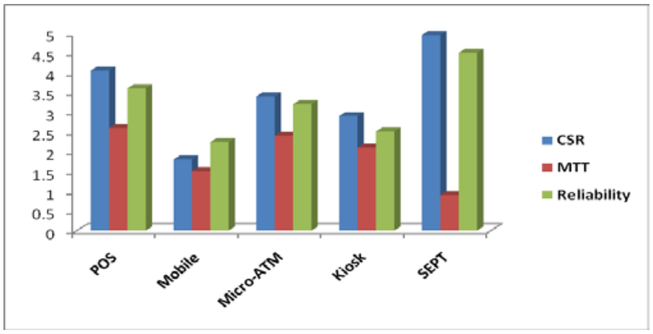

Fig. 3. Customer Success Rate (CSR), Reliability (R) and Mean of Transaction Time (MTT) for Payment Processing.

D. HSKT Technique

To prevent fraud, the HSKT investigates performance indicators to enhance security for safe and fast financial transaction processes in e-commerce applications. It provides evaluation metrics such as average delay, throughput, energy usage, encryption time, and decryption time.

1) Average delay: The timing difference between current data packets received as well as preceding data packets transmitted is evaluated using the HSKT method in the stages. In equation, the suggested approach is defined as a mathematical model for the average delay in equation (4). The average delay (AD) is calculated as follows:

$$\text{Average Delay} = \frac{\text{Pkt Received Time-Pkt Sent Time}}{\text{time}} \quad (4)$$

Where Pkt is Packet and Received time is received time.

2) Throughput: The throughput is an average of successful finance transactions and client record maintenances. The proposed method is described as a mathematical model for throughput in equation (5). Throughput is evaluated as:

$$\text{Throughput} = \frac{\sum_0^n \text{ Packets Received } (n)_* \text{ Packet Size}}{1000} \quad (5)$$

Where n is number of packets.

3) Energy consumption: Over the simulation period, the energy usage is really the difference between the new and residual energy. The energy consumption graph depicts the total amount of energy used in theTx and Rx modes throughout the whole operation. Tx mode is used when one process transmits data to another process. Tx Energy of a process state is the amount of energy needed to transmit a data packet. Tx energy is calculated depending on the size of the data packet (in bits). When a process state receives the packet from some other process state, it is in Rx mode. RX energy is the amount of energy required to receive a data packet. In equation (6), the suggested approach is defined as a mathematical model (7). The following is an estimate of the Energy Consumption (EC):

Energy Tx = (330*data Size)/2*106 (6)

EnergyRx=(230*data Size)/2*106 (7)

Where Tx is initial energy and Rx is residual energy.

4) Encryption time (ET): The encryption time finds to changes over the plaintext into the ciphertext. The encryption time depended on the message chunk size and the key size and illustrated in milliseconds. It has direct impact on the execution of the HSKT technique. The HSKT technique has the less encryption time, to create the encryption technique responsive and quick. The proposed methodology is defined as a mathematical model in equation (8). The Encryption Time (ET) is estimated as:

$$EP = (I, CT\{EP_i\}_{i \in \mathrm{I}}) \quad (8)$$

Where EP is an encoding process, and I is an attribute set. CT is ciphertext.

5) Decryption time (DT): The decryption time is a total time required to recuperate the plaintext from the ciphertext. For this purpose of HSKT technique is quick and responsive, it is attractive that the time taking for decoding is similar to the encryption time, and it is measured in milliseconds. A mathematical model in equations is used to describe the suggested approach (9). The following is an estimate of the Decryption Time (DT):

$$EP(EPi, ski) = EP(g, g)^{pi(0)s} \quad (9)$$

EP is an encoding process, and sk is a secret key.

With traditional methods, Table IV shows the Average Delay, Throughput, Energy Consumption, Encryption Time, and Decryption Time for various input restrictions. The suggested technique compared current methods to different types of algorithms such as DES, AES, and BF. On the basis of Table IV, it can be concluded that the suggested approach outperforms current methods. The method calculates Average Delay, Throughput, Energy Consumption, Encryption Time, and Decryption Time, as well as displaying average values for each parameter with specific data.

As shown in Fig. 4, the HSKT is computed using the average delay, throughput, encryption time, energy consumption, and decryption time. The suggested HSKT is computed using Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Blow Fish (BF) techniques based on average delay, throughput, encryption time, energy consumption, and decryption time. The method that comes closest is BF. AES ensured the secrecy and integrity of the data. AES, on the other hand, fails to decrease key complexity and often compromises the secrecy of critical keys. The framework provides details about the programming environment, execution steps for the experimental process, tabular result, and comparative analysis of the proposed HSKT technique. It discovers the complete overview of how the proposed systems works, what is the necessary software required to implement this methodology. How these approaches are best when compared to other methods. The average delay, throughput, encryption time, energy consumption, and decryption time of the HSKT method are all assessed. The findings of the HSKT approach are compared to the nearest traditional methods in tabular and graphical form. HSKT enhances privacy for safe and fast financial transactions while also preventing E-commerce fraud. The HSKT improves by 59.8% and lowers 4.73 AD (Average Delay), 23.91 EC (Energy Consumption), 0.95 ET (Encryption Time), and 0.85 DT (Decryption Time) (Throughput). Finally, the study argues that the suggested HSKT technique outperforms all other evaluation matrices and input parameters.

TABLE IV. AVERAGE DELAY, THROUGHPUT, ENERGY CONSUMPTION, ENCRYPTION TIME AND DECRYPTION TIME FOR 50 USERS WITH VARIOUS DATA SIZES

Algorithm	Average Delay (s)	Throughput(Kbps)	Energy Consumption (Joules)	EncryptionTime (s)	DecryptionTime (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

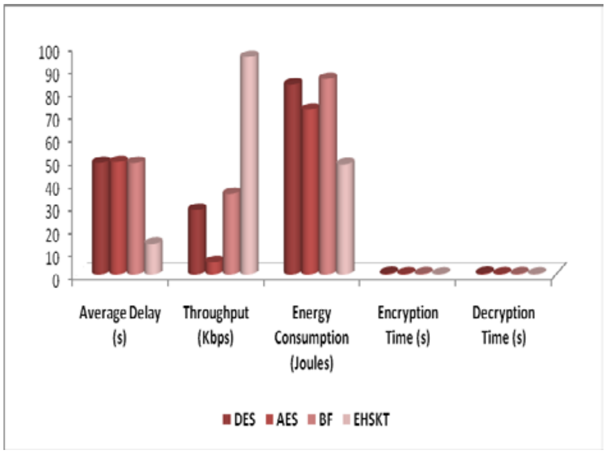

Fig. 4. Average e-Commerce Delay, Throughput, Energy Consumption, Encryption Time and Decryption Time.

V. CONCLUSION

The World Wide Web is the most important resource in contemporary business, since it opens up new business possibilities. E-commerce refers to an online store where goods is sold or purchased electronically. The High-Speed Key Transmission (HSKT) Technique was created to provide secure financial transactions, protect product content privacy, and prevent fraud. The privacy system keeps track of and controls the content profiles of merchants and clients. To prevent fraudulent behavior, the proposed approach increases throughput of safe besides effectual payment transactions, as well as the privacy of product content. The proposed method shows better results in performance parameters. In future, the method needs to focus more on transmission delay.

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] AnandShende, OmkarGurav, SwapnilShirode, PiyushGovekar, 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] 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.

[12] G. R. Patel and K. Panchal, “Hybrid Encryption Algorithm”, International Journal of Engineering Development and Research (IJEDR), vol. 2, iss. 2, pp. 2064-2070, 2014.

[13] Xueying Zhang,et al.,“Energy efficiency of encryption schemes applied to wireless sensor networks”, Security and Communication Networks, John Wiley & Sons, Ltd., 2011.

[14] R.Sharmila and V.Vijayalakshmi, “Hybrid Key Management Scheme for Wireless Sensor Networks”, International Journal of Security and Its Applications, Vol.9, No.11, pp.125-132, 2015.

[15] S. Gajbiye, et al., “A Survey Report on Elliptic Curve Cryptography”, International Journal of Electrical and Computer Engineering, vol.1, no.2, pp.195-201, 2011.

[16] D. Malan, et al., “A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography”, in Proc. 1st IEEE Int. Conf. Sensor Ad Hoc Communication Network, pp. 71-80, 2004.

[17] Y. Liu,et al., “PKC based broadcast authentication using signature amortization for WSNs”, IEEE Trans. Wireless Communications, vol. 11, no. 6, pp. 2106-2115, 2012.

[18] P. Porambage, et al.,“Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed applications” International Journal of Distributed Sensor Network, vol. 2014.

[19] D. Kim and S. An, “PKC-based DoS Attacks-Resistant Scheme in Wireless Sensor Networks”, IEEE Sensors Journal, 2016.

[20] M. Panda, “Security in Wireless Sensor Networks using Cryptographic Techniques”, American Journal of Engineering Research (AJER), vol.03, iss.01, pp-50-56, 2014.

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

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

[23] 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.

[24] 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.

[25] 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.

[26] Xiao, Y. Compensation Method of Electronic Commerce Data Transmission Delay Based on Fuzzy Encryption Algorithm. *Mobile Netw Appl* (2022).

[27] Hassan, M.A.; Shukur, Z.; Hasan, M.K. An Efficient Secure Electronic Payment System for E-Commerce. *Computers* 2020, *9*, 66.

[28] Alam, S.S.; Ali, M.H.; Omar, N.A.; Hussain, W.M.H.W. Customer satisfaction in online shopping in growing markets: An empirical study. Int. J. Asian Bus. Inf. Manag. 2020, 11, 78–91.

[29] Noor Ardiansah, M.; Chariri, A.; Rahardja, S.; Udin, U. The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. Manag. Sci. Lett. 2020, 10, 1473–1480.

[30] Satar, N.S.M.; Dastane, O.; Ma'arif, M.Y. Customer value proposition for E-Commerce: A case study approach. Int. J. Adv. Comput. Sci. Appl. 2019, 10, 454–458.