Research Article

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology
ISSN 2354-3917

2021
Vol. 9 No. 8: 103

Secured E-Commerce System Using ECC and Multimodal Biometrics

Abdulkarim Musa Onuja[1]*, Ishaq Oyebisi Oyefolahan[2], Olawale Surajudeen Adebayo[3], Abdulkadir Onivehu Isah[3], Olayemi Mikail Olaniyi[4] and Muhammad Bashir Abdullahi[5]

[1] Department of Computer Science, Confluence University of Science and Technology, Osara, Nigeria

[2] Department of Information and Media Technology, Federal University of Technology, Minna Nigeria

[3] Department of Cyber Security Science, Federal University of Technology, Minna Nigeria

[4] Department of Computer Engineering, Federal University of Technology, Minna Nigeria

[5] Department of Computer Science, Federal University of Technology Minna Nigeria

***Corresponding author**
Abdulkarim Musa Onuja Department of Computer Science, Confluence University of Science and Technology, Osara, Nigeria

onujaam@custech.edu.ng

Citation: Onuja AM, Oyefolahan IO, Adebayo OS, Isah AO, Olaniyi M, et al. (2021) Secured E-Commerce System using ECC and Multimodal Biometrics. Am J Compt Sci Inform Technol Vol. 9 No. 8: 103.

Abstract

This paper focuses on the need to win electronic commerce customers trust by developing a secured electronic commerce system using elliptic curve cryptography (ECC) integrated with multimodal biometrics (iris and voice) as a methodology. Unlike the use of Rivest, Shamir and Adleman (RSA) algorithm that is commonly used in many computing devices to enforce the confidentiality of information, this research uses ECC, thereby reducing memory space complexity and computation power. Also, freed-up memory space is used to add other security measures in the form of iris and voice biometric to effect authentication. The mathematical expression of ECC was modified to reflect the encryption and decryption of image (iris) and audio (voice) data types integrated in the modeled secured electronic commerce system. Performance evaluation were carried out after implementation and results show a system that is promising by completing the processing of new user registration and logging in within 90 seconds. Although, the use of only RSA was discovered to occupy less space when the bit strings are less than 30 kilobyte, the methods-the integration of iris and voice biometrics into ECC (Sum iv) as used in this research consumes lesser memory, the moment the key-size is greater than 30 kilobyte, and increase the difficulty in eavesdropping through information traffic analysis and impersonating a customer with second and third line authentication measures.

Keywords: Electronic commerce system; Elliptic curve cryptography; Rivets; Shamir; Adelman; Voice biometrics

Received: August 04, 2021, **Accepted:** August 18, 2021, **Published:** August 25, 2021

Introduction

Security is the fundamental need to secure online information. The high degree of trust required in the authenticity and privacy of such transactions can be difficult to maintain [1].

Cryptography is a process that makes information unintelligible to an unauthorized person, thus providing genuine users with confidentiality. Confidentiality can be described as attempting to keep information from being known by an unauthorized party [2]. More importantly, enhancing the privacy of information against unauthorized access is the major goal of cryptographic mechanism [3]. It is possible to use different cryptographic algorithms. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advance Encryption Standard (AES), rivets, Shamir and Adelman (RSA) and blowfish are the most commonly used algorithms listed in Patil et al. [4]. Other noteworthy algorithms include Nth degree Ring Unit Truncated (NTRU), Diffie-Hellman (DH), Digital Signature Scheme (DSS). RSA is widely used to secure information channels and gateways such as the web traffic, electronic mails, scientific information about innovation and new technologies, electronic commerce and transactions, and information gathering and capturing products and devices such as phones, cameras and satellites. **Figure 1.1** illustrates public-key cryptography.

The algorithm of Rivest, Shamir and Adleman (RSA) is based on the factoring problem of finding two large prime numbers. Over the past few years, the key length for safe RSA use has increased,

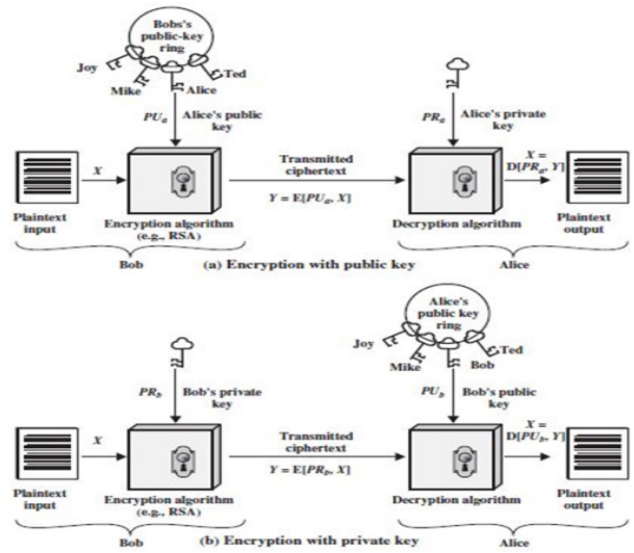

Figure 1.1 Public-key encryption and decryption diagram.

placing a heavier processing load on RSA applications (Stallings, 2014), example; key size is 1024 to 4096 bits. The need to have a large key size has implications in terms of higher overhead cost, especially for electronic commerce sites that process numerous transactions that must be secured. A competing algorithm that challenges RSA is the elliptic curve cryptography (ECC). ECC is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography (Stallings, 2014). Reveals that elliptic curve cryptography (ECC) matches RSA in utilization as both cryptographic algorithms can be used for encryption and decryption, digital signature, and key exchange. Nth degree Truncated Ring Unit (NTRU) decryption and signature take much less time and memory space than ECC, RSA, and most other public key cryptosystems with the same security level [5]. The NTRU is a post quantum cryptography system often considered as the most practical post-quantum public key crypto scheme [6]. And this scheme uses the properties of structured lattices to achieve high efficiency but its security remains heuristic and it was an important open challenge to provide a provably secure scheme with comparable efficiency [7]. However, the implementation of an NTRU encryption scheme is to be effected on quantum computers as a counter measure to the vulnerabilities of RSA and ECC to quantum computing attacks while the focus of this research work is on the security of normal personal computers and computing devices commonly used in electronic commerce transactions. On the other hand, the use of ECC instead of RSA is discovered to be technically feasible and suitable for the desired secured electronic commerce system in this research work **(Table 1).**

The computational effort required in the cryptanalysis of symmetric key algorithms, Diffie-Hellman and digital signature algorithms, Rivest Shamir and Adleman (RSA) and Elliptic Curve Cryptography (ECC) has been compared to discover that elliptic curve cryptography (ECC) use about one-eighth of the key-size used in RSA to offer the same level of security **(Table 2).**

Biometrics are being used to authenticate the identity of users in a biometric system, this is becoming more popular than traditional identification methods that includes password,

Table 1: Applications of public-key cryptosystems.

Algorithms	Encryption and decryption	Digital signature	Key exchange
RSA	Yes	Yes	Yes
ECC	Yes	Yes	Yes
DH	No	No	Yes
DSS	No	Yes	No
NTRU	Yes	Yes	Yes

Table 2: Comparable key sizes in terms of computational effort for cryptanalysis.

RSA (size of n in bits)	ECC (size in bits)
1024	160-223
2048	224-255
3072	256–383
7680	384–511
15360	512+

personal identification number (PIN), and user identification card [9,10]. The authentication process should provide user comfort, simple usage, fast verification and the security properties such as non-forgeability, soundness, completeness, low false acceptance rate and privacy protection. Biometrics, some of which shown in **Figure 1.2**, are unique, unchangeable, universal and measurable.

A biometric system's performance or accuracy is data-dependent, usually influenced by factors of the environment and performance. Environmental factors include temperature, humidity and illumination conditions around the system, while performance factors include capturing good quality images, composition of the target user population, time intervals between enrolment and verification phases, and robustness of recognition algorithms [11]. However, the accuracy of a biometric system is usually measured as a pattern recognition system in terms of sample acquisition and performance errors described **(Table 3).**

Given the challenges inherent in one modal system, it is clear that multi-modal systems offer greater defensive lines against threats with respect to accuracy of recognition as well as poor quality management of biometric samples [12]. This is basically the idea behind the use of iris and voice biometrics in this thesis work.

According to Mali & Bhattacharya, the comparative analysis of biometric traits reveals that iris is high in universality, distinctiveness, and permanence, having a medium value in collectability like fingerprint, low rate of circumvention, which is good for the security of a secured electronic commerce system. In order to fend off the possibility of spoofing attack against iris biometric, ECC is used in the system to encrypt the datasets of customers. Voice biometric is added for its high acceptability, as for the high level possible circumvention, the research gets over the challenge by modeling the system to speech recognition of users and advises the users to keep the uttered statement private as in the use of passwords. It is believed that while it easy for an intruder to mimic a public personality and a widely spoken language, such will be difficult against a private customer speaking in a native dialect that is not popular.

Related work

In general, a secure mobile-commerce credit card mechanism

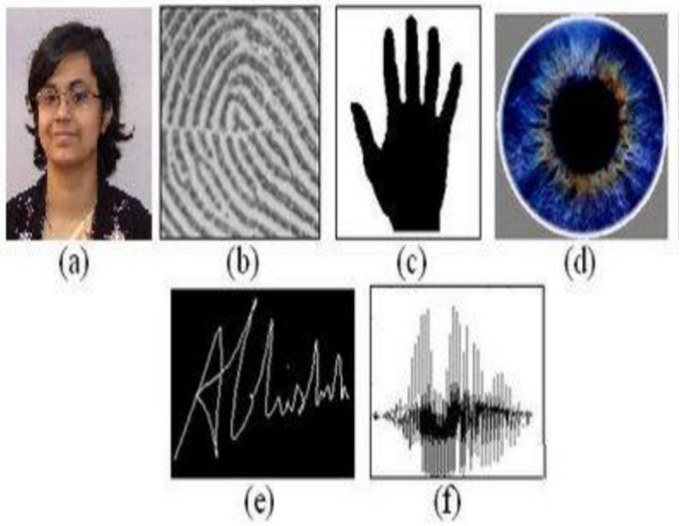

Figure 1.2 Present some examples of biometrics.

Table 3: Comparing accuracy between different biometric techniques.

S. No.	Biometric modality	Accuracy level
1	Fingerprint	99.90%
2	Palmprint	>95%
3	Face	95%
4	Iris	99.90%
5	Retina	99%
6	Voice	>90%
7	Signature	>90%

(m-commerce) must be able to secure relevant transactions and personal information [13]. Secure Sockets Layer (SSL) can provide point to point security of delivery, but it is not able to confirm user's identities [14]. In finding solution to this drawback, the Visa and MasterCard organizations known for embedded security systems, submitted a Secure Electronic Transaction (SET) electronic payment system specification [15].

SET, for example, has its own problem, a consumer must apply for a certificate, and SET takes a long time to calculate asymmetrical encryption and decryption key that are complicated [16]. Then propose a secure mobile commerce scheme (SMCS) as a methodology for users to create safe credit card transactions in electronic commerce. The authors agree that SSL and SET are dependent on public and private key cryptosystems, but were not able to explain the basis on which DCC pre-link wireless systems and users for authentication. More so, RSA algorithm is heavily relied on by the SMCS instead of ECC, which is not seen as an effort to reduce the overhead cost mentioned as a challenge in computing encryption and decryption keys. Also, the researchers did not find biometrics as an easy technique to authenticate users' identity in electronic commerce transaction as widely believed.

Researchers propose an authentication scheme that uses the pre-computing of nonce (one-time) passwords to avoid time-consuming exponential computations to improve the security of telecare medicine environments. The proposed scheme consists of four phases: registration, login, authentication, password change. The security analysis of the proposed system shows improved resistance against password and private key guessing attack, parallel session and reflection attack, server spoofing and insider attack. Authentication scheme proposed to secure, Telecare Medicine Information Systems (TMIS) is vulnerable to reflection attacks and fails to preserve user anonymity [17]. The authors improve on the existing system by proposing a three-factor authentication scheme for the telecare medicine information systems. The telecare server selects a master key, a secure chaotic one-way hash function, and computes the system's public key. Arshad and Nikooghadam further improve on the scheme by proffering solution to its vulnerability to replay attacks and Denial of Service (DOS) attacks [18]. An effective three-factor anonymous authentication and key agreement scheme for TMIS is proposed to overcome these security flaws. Analysis of security and performance shows superiority of the proposed scheme compared to previously proposed schemes related to TMIS security. Lu et al. discovers that an offline password attack is successful in this scheme [19]. Any user of the system can be impersonated, in order to thwart and tighten this vulnerability, the authors proposes a methodology called enhanced biometric and smart card based remote authentication scheme for TMIS. The proposed system analysis shows satisfactory results using the Burrows, Abadi and Needham (BAN) logic. The researchers assert that the intended system is more secured and with less computational cost.

Lu et al. scheme is susceptible to varieties of attacks such as Telecare Medicine Information System (TMIS) server impersonation attack, patient impersonation attack and patient anonymity violation attack. The authors propose a system that removes these vulnerabilities and then use Provera as a popular automation tool to analyses the strength of improvement in the new scheme. The challenge with the research is that studying the progress made from to there was no mention of the specific public key encryption and decryption algorithms used in the work. Although, many authors agree that the use of biometric is a good authentication technique, the authors were not emphatic about the idea of the technique used to improve authentication.

Mahto and Yadav worked on one-time password security by using bank client's irises to generate their cryptographic keys, and then using ECC keys to provision the security of data communication to transmit the server's one-time password (OTP) to the client. ECC could have been allowed to generate its own cryptographic keys as it has the power of securely exchanging keys while the use of irises of the clients could have served as an outright addition of another security measure as proposed in secured electronic commerce system using elliptic curve cryptography integrated with biometrics [20].

Computer network infrastructures provide online platforms to do e-commerce tasks such as ordering of goods and services, online banking, advertisement, and information sharing. For dual purposes, security is required; to protect the privacy of customers and to protect against fraud [21]. Although, multiple end users are communicating with each other, most of them are concerned about secrecy (confidentiality), authentication of data, non-repudiation [22]. They use cryptography with biometric features to mitigate these issues. In its security model, the identity and authenticity of an individual using cryptography and biometrics respectively gives reliable assurance [23]. They

proposed an OTP security enhancement algorithm using ECC with biometric palm-vein. The ECC's main effect in contrast to public key cryptography such as RSA is that it permits better security per bit with a smaller key size [24]. The proposed model is able to handle encryption and decryption technique problems such as key privacy, key storing and management as achieved from the results of implementation. However, the size of palm-vein print to be captured has an effect on the ease of use and deployment.

Yoon & Yoo proposed to use biometrics secured smart card and elliptic curve cryptography to authenticate multiple servers [25]. However, Odelu et al. highlighted that in a situation of losing the smart card, the scheme could not counter against assumption of the offline passwords [26]. In addition, the idea of an improved scheme to plug the security loophole identified in the scheme is subsequently, has shown that is not secured against rogue insider attack and impersonation. Not long ago, He D and Wang D discussed robust multi-server environment biometrically enabled authentication system to address these security issues, claiming their scheme is safe against any known attacks [27]. However, the scheme does not prevent a temporary attack on known session information, and as a result the method could not protect against response attack and impersonation. The authors also show that the scheme is unable to provide strong anonymity for the user.

Therefore researchers are proposing a secure multi-server authentication protocol using a biometric smart card and ECC with more security features. The researchers demonstrate that the scheme provides secure authentication using the Burrows-Abadi-Needham (BAN) logic. In addition, the scheme was simulated with the widely accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to test for formal security verification, revealing that the scheme is secure against passive and active attacks [26]. is that the paper was not specific on the choice of biometric traits that suits the model.

Silva et al. presents an analysis of cryptographic algorithms in hardware systems for performance evaluation. Average processing and memory space needed, execution time and power consumption are parameters considered in the analysis. The authors discuss these parameters in five test scenarios in the performance evaluation. The researchers noted that each case study have a unique goal and implementation. Thereby suggesting which of these algorithms can be used for hardware systems for optimum performance and result in different situations [28].

Researchers compare the performance assessment of RSA and ECC algorithms with respect to the times of key generation, duration of encryption and decryption processes, the cipher text sizes and the time taken to sign digital signatures and verify equal key sizes in terms of safety and security strength [29]. For large key sizes, the plaintext message used in the encryption and decryption time it takes is unmanageable in RSA. In contrast, even if the key sizes are very big in ECC, the encryption and decryption time required is efficiently manageable. The signing of RSA signatures are relatively slower than its verification, while the signing of the ECC signature is usually faster than verifications. These results of implementation appeal to the use elliptic curve cryptography as a substitute for RSA in this thesis.

Overview of Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is used to establish a session key with forward secrecy property due to its ability to provide a low key size with stronger security level [30]. The ECC's security lies in the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), and with the key of less bits, it can achieve the same safety as RSA [31]. ECC presents an attractive alternative cryptosystem as its safety is based on the problem of the elliptic curve discrete logarithm (ECDLP) and operates on an elliptic curve that is over a group of points. It can provide a level of security comparable to conventional cryptosystems using much larger key sizes.

The elliptic curve operation is explained below and it is given by;

$$E_p(a,b): Y^2 = X^3 + ax + b \left(\mathrm{mod}\ P_1\right) \quad (1)$$

Over a finite field Fp of prime order p>3, where a, b ∈ Fp

On the condition that;

$$4a^3 + 27b^2 \neq 0 \left(\mathrm{mod}\ P_1\right) \quad (2)$$

Given a random integer a ∈ Fp^* and a point P ∈ Ep (a,b). The elliptic curve (EC) point multiplication a. P over Ep(a, b) is defined as;

A·P=P+P+...+P (a times).

Constants a, and b, variables x, y can be integers, real, complex, polynomials, and any other elements belonging to the field. Draw the tangent line to the curve at P in order to define the double of P. This line will intersect the curve at a point **(Figure 2.1)**.

Then, R(x3, y3)=2P(x1, y1) is the reflection of this point about the x-axis.

Let E be defined in field K as the given elliptic curve. The following formulae allows the formation of the algebra on the curve y2=x3+ax+b;

- The identity rule: P+0=0+P=P for all P ∈ E (K).
- Negative of a point: If P=(x, y) ∈ E (K), then (x, y)+(x,-y)=0. The point (x,-y) is marked with P and is called the negative of the point, P, as presented in **Figure 2.2**. It must be noted that -P is also a point in E (K). Also, as in normal algebra: 0=0.

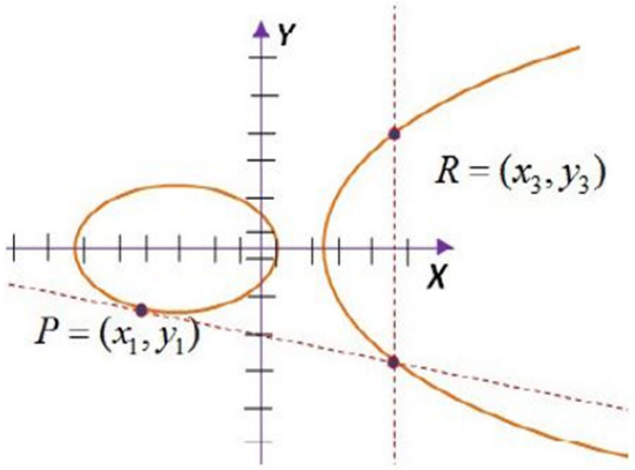

Figure 2.1 Doubling of P.

Addition of points: let P = (x1, y1) ∈ E(K) and Q = (x2, y2) ∈ E(K)

Where P ≠ ± Q

Then P+Q=R(x3, y3) as illustrated.

Where x3=λ2–x1–x2, y3=λ(x1–x3)–y1

Doubling of a Point: As shown in **Figure 2.3**, let P=(x, y) ∈ E(K), where P ≠ ±P. Then 2P=R(x3,y3),

Where x3=λ2−2x1, y3=λ(x1–x3)–y1 and

$$\lambda = \frac{(3x_1^2 + a)}{(2y_1)}$$

ECC can be used for the encryption of plain human readable messages into a bunch of meaningless text messages called cipher texts and then, the decryption of the cipher texts back into the initial plaintext message. The plaintext messages are first mapped to a point on the curve [32]. ECC key generation algorithm is explained as stated bellow;

Alice and Bob agree on a common curve;

y2(mod p)=x3+ax+b (mod P)

With the generator point as G(xg,yg) (3)

Alice selects an integer na as private key and computes a point,

Pa=naG=(xa,ya) (4)

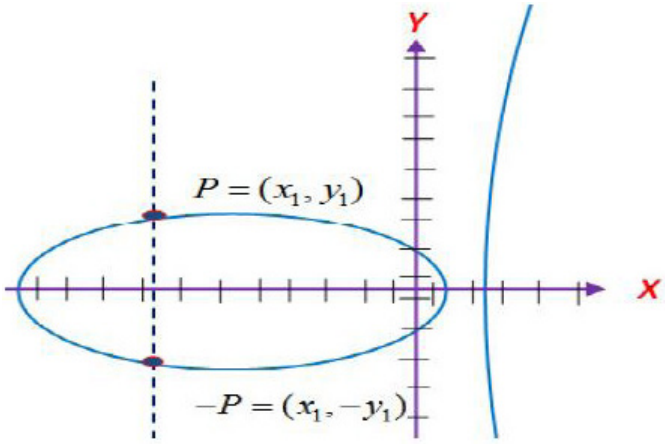

Figure 2.2 Negative of a point.

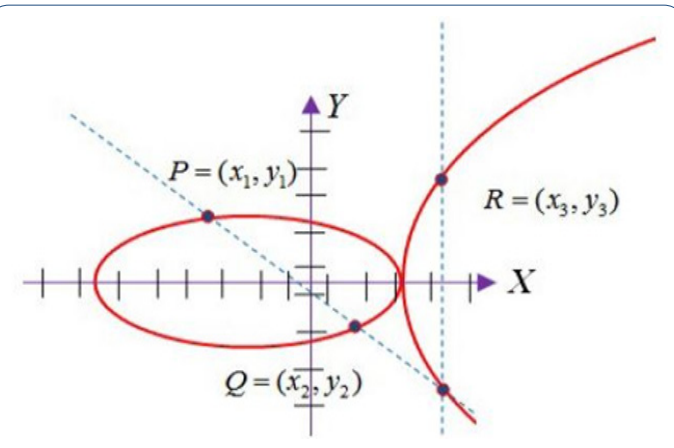

Figure 2.3 Negative of a point.

using the group law.

Alice's public key is reported as Pa=(xa, ya) (5)

Bob also selects an integer n_b as private key and computes a point,

$P_b=n_bG=(x_b,y_b)$ (6)

using the group law.

Bob's public key is reported as $P_b=(x_b,y_b)$ (7)

Supposing that alice is transmitting the message.

$P_m=P(x_m,y_m)$ (8)

to bob. The algorithm to be used in encrypting the message is given below;

Step 1: Alice chooses a random integer k.

Step 2: And using the group law, computes the two points,

c1=kG (9a)

$c2=P_m+kP_b$ (9b)

Step 3: Alice sends the two pair of points,

$Cm=C(c_1, c_2)$ (10)

as ciphertext to Bob.

Bob obtains the ciphertext, $Cm=C(c_1,c_2)$ from Alice on which decryption is computed by using the formula below:

Bob multiplies c_1 by private key n_b and subtracts it from c_2.

That is; $c_2–nbc_1 = (P_m+kP_b)–n(kG)$ (11)

$=(P_m+kn_bG)−nkG$ (12)

$=P(x_m,y_m)$

=Pm (the initial plaintext message).

NIST recommended key length sizes for ECC and RSA are 20 bytes and 128 bytes respectively.

Research Methodology

Research framework

The exchange of high economic value information such as during online transactions on the internet as a communication medium necessitated the need to enforce security against inherent threats to the data in transit from hackers of different malicious motives [33]. The desire to improve on the security of electronic commerce follow a careful research design, this include the comparative study of cryptographic algorithms that results in the understanding that ECC and RSA can both perform secured key exchange, authenticate with digital signature, and enforce confidentiality of information with encryption or decryption. The memory requirements of the two schemes were put into considerations. The integration of iris and voice biometrics into ECC for a secured e-commerce system is discovered to maintain a lesser memory space with smaller key sizes after implementation. Thus, the security of the system is improved with additional security measures **(Figure 3.1)**.

Proposed model for ECC integrated with biometrics: The confidentiality and authenticity of information transmitted online

with the internet as the backbone infrastructure is established by mainly using cryptographic functions. The RSA algorithm is one of the most widely used methodology that applies the use of public key cryptography to offer encryption, decryption, digital signature, and key exchange services to secure data transiting online communication channels. However, it can be inferred from the related research work the implementation of ECC algorithm is more efficient when the same length of key is used for encryption and decryption. Similarly, this means that the key length size of 255 bits for ECC will have the strength of 2048 bits key size of RSA encryption schemes with reference to **Table 1.** Consequently, current research in electronic commerce security is interested in how best ECC can be used to reduce overhead cost with respect to the memory size required for the encryption key in ECC. More so, the algorithm also suits new mobile computing devices such as smart phones that can equally be used to access e-commerce websites for business transactions. This work is focused on taking advantage of the memory space afforded by using ECC, to integrate other security measures in the form of iris and human voice biometrics to improve on the security of electronic commerce as shown in the proposed model**.** The mnemonics used in the proposed model in **Figure 3.2** include customer order information (COI), that list all the items the customer want to purchase with their respective prices added to a digital cart and calculate the total cost to be forwarded to the electronic commerce (E-commerce) website server for processing.

The payment order information (POI) enumerates all information required to effect online payment. Information such as the serial numbers on Automated Teller Machine (ATM) cards, expiration date, personal identification number (PIN), amount to be paid for goods checked onto the digital cart, the name of the customer to whom the goods is to be delivered, the address and phone number are categorized as payment order information (POI).

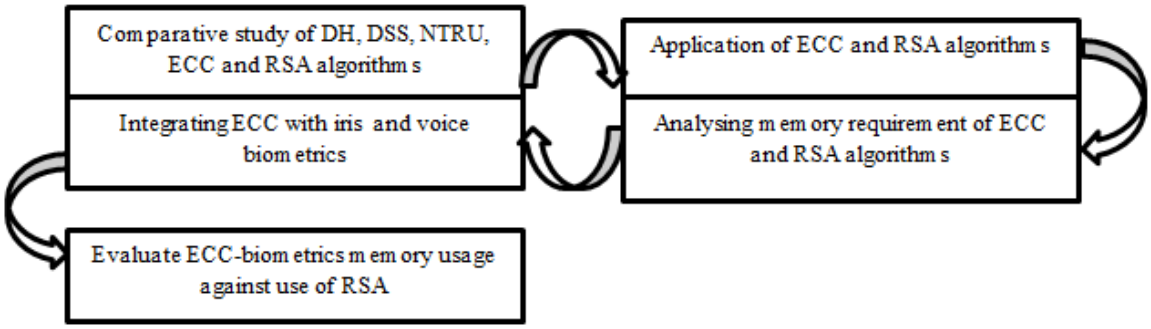

Figure 3.1 Diagram illustrating research framework.

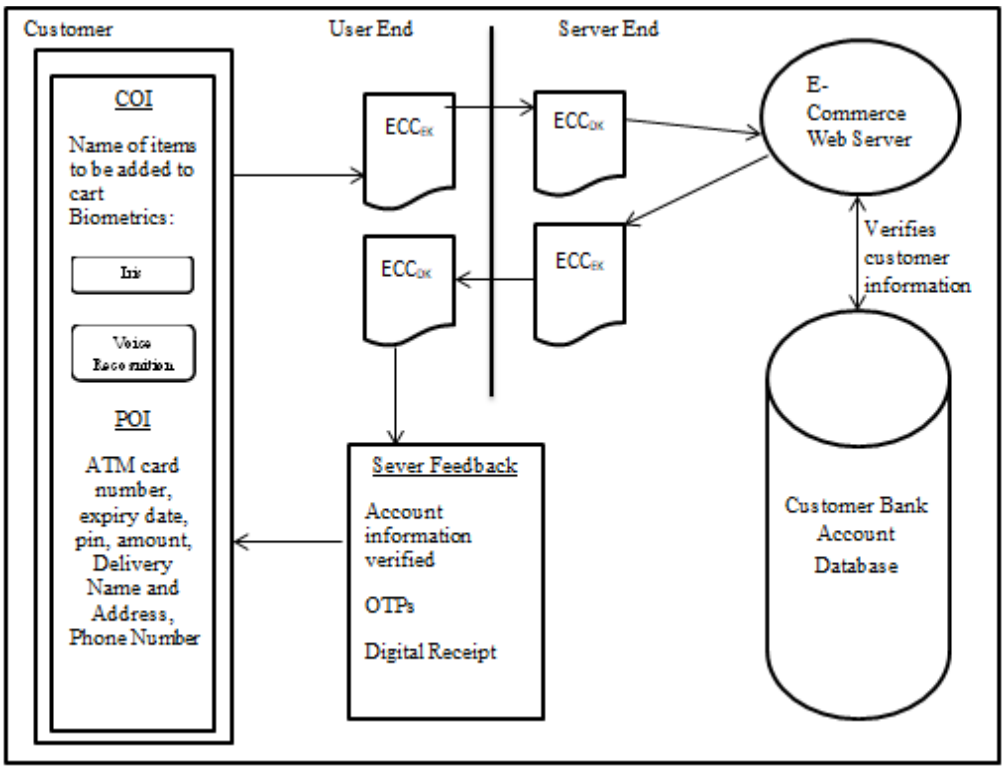

Figure 3.2 Model diagram for ECC integrated with biometrics.

The proposed model also has the automated elliptic curve cryptography encryption key as ECCEK and the decryption key as ECCDK. The electronic commerce website server verifies customer's information by sending verification request to the bank that issues the ATM card used for the transaction and then matches the iris and voice biometric against the one registered and saved with the electronic commerce service provider. The electronic commerce webserver confirms the bank account details of the customer before sending feedback to the customer. The processes involved in the secured electronic commerce system also accommodate the existing security measure known as the one time password (OTP). Then, the online transaction platforms display a digital receipt to be printed for documentation after a successful transaction [34].

Mathematical model for ECC integrated with biometrics: The mathematical model representing the integration of ECC with Biometrics is expressed by giving credence to the practical implementation of the secured electronic commerce system that have to encrypt three different data types; texts, iris (images), and voice (audio). Given that parties A (Alice) and B (Bob) have agreed on a common curve of $E_p(a,b): Y^2 = X^3 + ax + b \pmod{P_1}$ as in equation 1, on the condition that $4a^3 + 27b^2 \neq 0 \pmod{P_1}$ as in equation 2, with the key generator point as G (xg,yg) in equation 3. The transmission of plaintext message Pm is given as P_m=(xm, ym) equation 7, as cited in chapter 2.

This research work deems it necessary to split the components of plain message Pm in equation 7 with respect to its data types as:

Pm=(plaintext P_t, plain image P_i, plain voice P_v) in formulating a mathematical model that integrates iris and voice biometrics into the ECC encryption model, to suit the operation of this modeled secured e-commerce system.

Supposing that customer Alice is transmitting customer and payment order information messages

Pm=(plaintext Pt, plain image Pi, plain voice Pv).

=((xt,yt), (xi,yi), (xv,yv)) to Bob. The algorithm to be used in encrypting the message is as modified bellow;

Step 1: Random integer k is chosen by Alice.

Step 2: Computes the two points, using the group law;

c_t1=kG and c_t2=Pt+kP_b

c_i1=kG and c_i2=P_i+kP_b (15)

c_v1 = kG and c_v2=P_v+kP_b

Step 3: The two pair of points is sent by Alice for each of the cipher data types,

C_m=((c_{t1},c_{t2}), (c_i1,$_{ci2}$), (c_v1,c_v2)) (16)

=(c_t, c_i, c_v) as ciphertext to bob.

The ciphertext is obtained by Bob as, Cm=C (c_t, c_i, c_v) from Alice on which decryption is computed by using the formula below:

Bob multiplies (c_{t1},c_{i1},c_{v1}) by private key n_b and subtracts it from (c_t2,c_i2,c_v2) respectively.

That is;

$c_{t2} - n_b c_{t1} = (P_t + k_{Pb}) - n(kG)$

$= (P_t + kn_bG) - nkG$ (11)

$= (x_t, y_t)$

$= P_t$ the initial plaintext data.

$c_i2 - n_b ci1 = (P_i + kP_b) - n(kG)$

$= (P_i + kn_bG) - nkG$

$= (x_i, y_i)$

$= P_i$ the initial plain image data.

$c_v2 - n_b c_v1 = (P_v + kP_b) - n(kG)$

$= (P_v + kn_bG) - nkG$

$= (x_v, y_v)$

=Pv the initial plain voice data=(x_t, y_t, x_i, y_i, x_v, y_v)

=(P_t, P_i, P_v)

=P_m plain message, the human readable customer order and payment order information transmitting between the customers on the electronic commerce platforms as implemented in the model secured electronic commerce system using elliptic curve cryptography (ECC) and multimodal biometrics.

Operation of the proposed model: The system requires the registration of new customers on the electronic commerce platform (web application or website) to facilitate subsequent commercial transactions until the customer's user account is deleted from the database on the request of the customer. The new customer registration details include names, email, phone number, and residential address, birth day, capturing of iris and the recording of voice preferably a native dialect statement [35]. The personal information of a customer already used for registration is matched against information submitted previously, to effect transaction, including automated teller machine (ATM) card details. The customer order information (COI) and payment order information (POI) are secured traditionally by using the RSA algorithm to establish the security goal known as confidentiality of information, but with the lower overhead cost of ECC, ECC is being used in this research work to support its growing prominence. And to solve the authentication problem in ECC that is not practical, this research adds biometrics in the form of iris data capturing and native language voice recognition. The online platform or websites request to capture biometrics and other personal information used for registration to be matched with those in the database. The server then allows for a successful payment if records are verified to be correct [36]. Otherwise, it will not allow payments to be made to avoid security breach due to repudiation. **Figure 3.3** shows the flow chart describing the operation.

Framework for the transaction platform: The customer order information and payment information inputted or outputted on the graphical user interface on the online platform should be encrypted with Elliptic curve cryptography algorithm while transiting communication channel between end user desktop and ecommerce website or application server, with the addition of captured iris and voice biometrics for authentication. The customer order information (COI) includes names of customers,

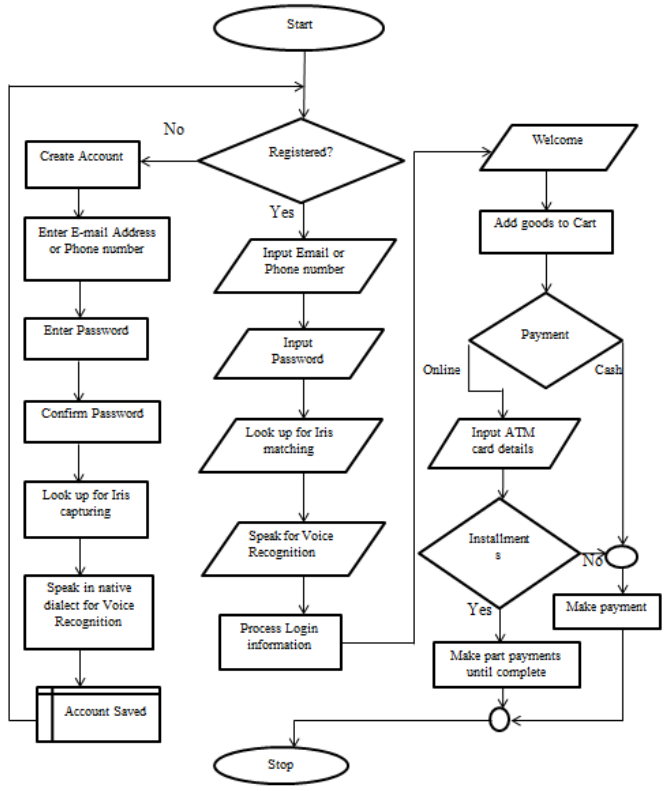

Figure 3.3 Flow chart of the model.

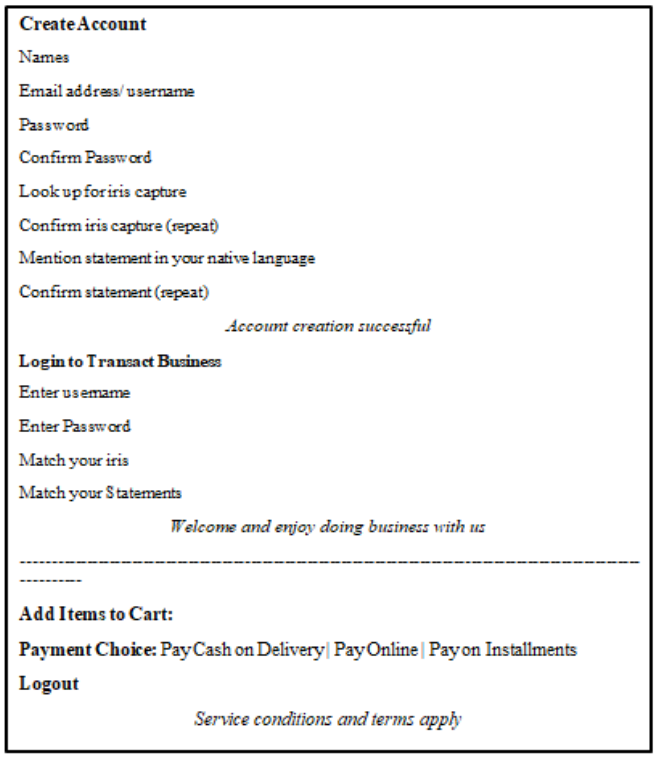

Figure 3.4 System design for graphical user interface for the model.

user names and passwords, iris and voice capture that matches those registered with the online database server, name of items to be added to cart. The payment order information (POI) includes ATM card number, expiry date, pin, amount, phone number, delivery name and address. The online transaction system should support payment on delivery, payment before delivery (48 hours waiting time) and installment payments (3 times in a maximum of 3 months). The list of goods and their respective prices should be classified and grouped in dropdown list [37]. Goods selected are added to the digital cart and the sum of all goods added to cart is computed. Examples are;

a. Computer Accessories; Flash drives (2G, 4G, 8G, 16G, 32G), Hard drives (200G, 300G, 500G), monitors, System Units, Mouse, Power pack, Adaptors, Plugs

b. Computer Laptops: Hewlett Pakard HP (2G RAM, 3G RAM, 4G RAM, 8G RAM,16G RAM, 32G RAM), dell (2G RAM, 3G RAM, 4G RAM, 8G RAM,16G RAM, 32G RAM), Acer (2G RAM, 3G RAM, 4G RAM, 8G RAM, 16G RAM, 32G RAM), Lenovo (2G RAM, 3G RAM, 4G RAM, 8G RAM,16G RAM, 32G RAM).

The features of the system includes the addition of mechanism to capture customer's iris and voice to the security provided the use of passwords for user accounts and pins on ATM cards in the case of making online payments as shown in **Figure 3.4**.

Performance evaluation

Computer laboratory setup: The computer laboratory setup includes a laptop computer of 2.0GHz random access memory running on Window 10, iris biometric datasets, a voice biometric datasets for speech recognition, database management tool, and software development kit (SDK).

System implementation testing: After the implementation and installation of the secure electronic commerce system using ECC and multimodal biometrics (iris and voice), it then establishes communication with the MySQL for managing the database, the system user or customer login and account creation interface in **Figure 4.1** below comes up, to enable the testing of the system.

The next step in the system testing activity is to create a new user or customer account, by inputting the names of the customer, his or her address email and desired password and then repeat the password in the confirm password text-field **(Figure 4.2)**.

The research work had to simulate the capturing of iris biometrics by using datasets. This is because according to www.fulcrumbiometrics.com (Fulcrum Biometrics)-a company that deals in the selling of IriShield-USB MK 2120U single Iris Capture Camera, although, the device is cost effective and can easily be deployed for experimental purposes, it uses 2048-bits RSA key to secure captured data. This is against the opinion of this research that by the time the need arises to increase bit length for high level security, RSA will not be efficient compared to the use of Sum-iv. The system captures iris dataset and voice dataset files as shown in **Figure 4.3**. In line with the use of datasets, the research work uses voice datasets as shown in **Figure 4.4**, although the computer laptop used has microphone to capture voice.

The encryption and decryption of customer order information using ECC is processed in the backend of the secured electronic commerce system. **Figure 4.5** showing the moment biometric data is captured in plain image, and **Figure 4.6** showing the encryption.

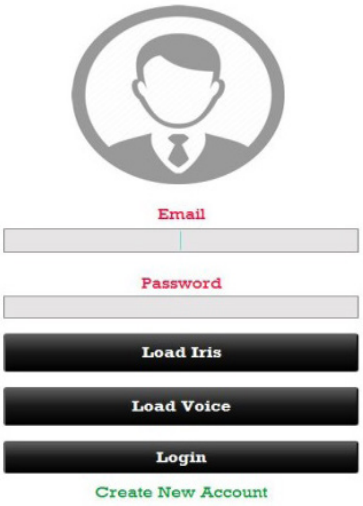

Figure 4.1 System customer login and account creation interface.

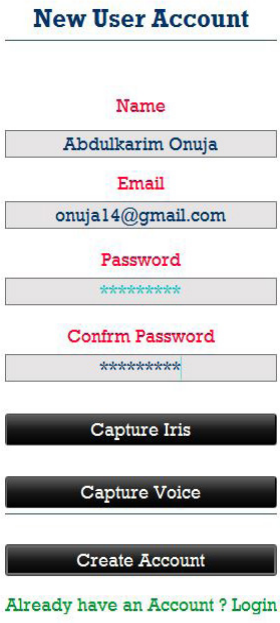

Figure 4.2 New user account creation.

The generation of public and private keys, and encryption is a simultaneous process effected with the creation of account or logging in on the platform, for the purpose of efficiency.

The new customer can then click on the create account button and the system will respond with a statement reading 'account created successfully,' as displayed in **Figure 4.7**.

In order to confirm that the account creation is successful, the researchers check the backend of the system-the database, by opening the MySQL tool and configure the database tool to show databases as shown in **Figure 4.8**.

Then, the tool is queried to use macro hub, and the next line of command is to describe customer that will present all the

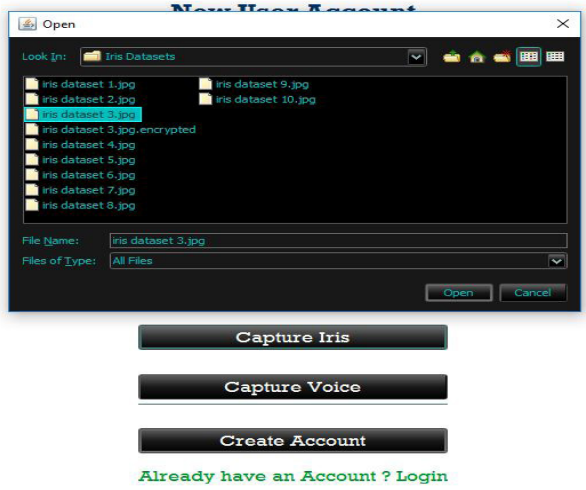

Figure 4.3 Capturing iris dataset for new customers.

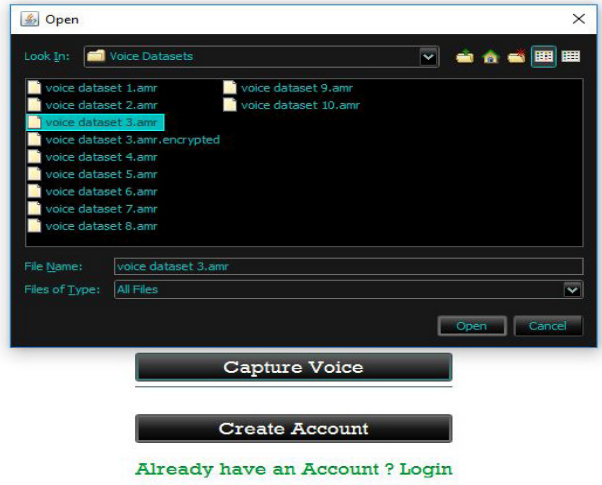

Figure 4.4 Capturing voice dataset for new customer.

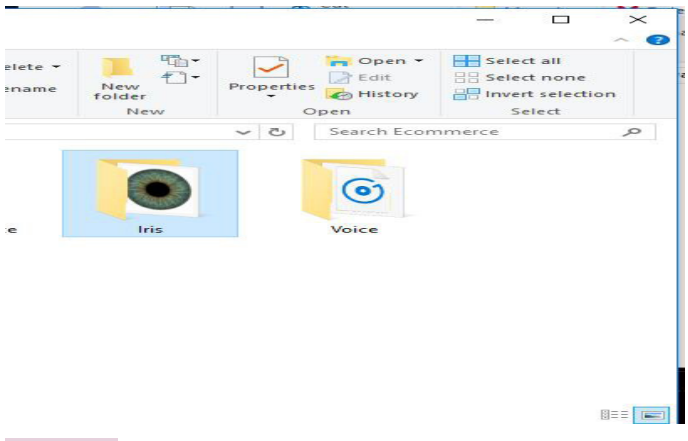

Figure 4.5 Moment iris and voice is capture.

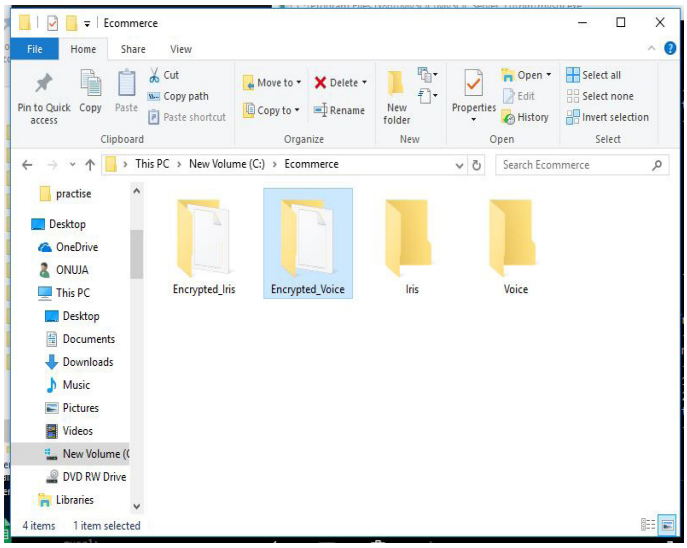

Figure 4.6 Encrypted iris and voice.

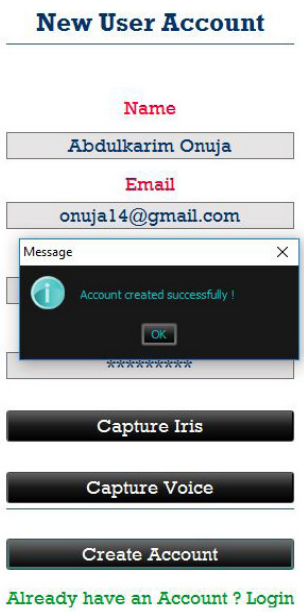

Figure 4.7 Account created successfully.

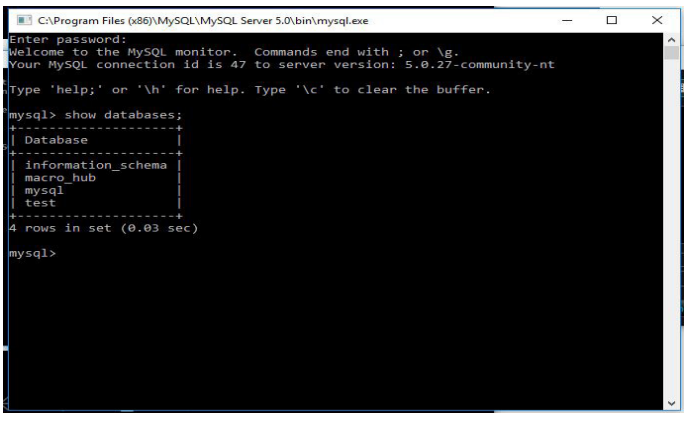

Figure 4.8 Database tool configured.

attributes to the entity customer in the database macro hub. These attributes are name, email, password, iris, encrypted iris, voice, encrypted voice as shown in **Figure 4.9**.

The final querying of the database in the quest to confirm a registered customer is by inputting the query 'select name, email, password, Iris name, voice name from customer.' It will show all successfully registered customers in the database as in **Figure 4.10**.

Subsequently, the customer can do electronic or online transactions by correctly logging in with his or her personal account details, process the matching of his or biometric traits and wait for authentication within seconds of the time, as illustrated in **Figure 4.11**.

The customer progresses to the items in stock on the electronic commerce platform after a successful authentication, to search for goods of interest to add to cart and order. It is the pictorial view of the web platform **Figure 4.12** .

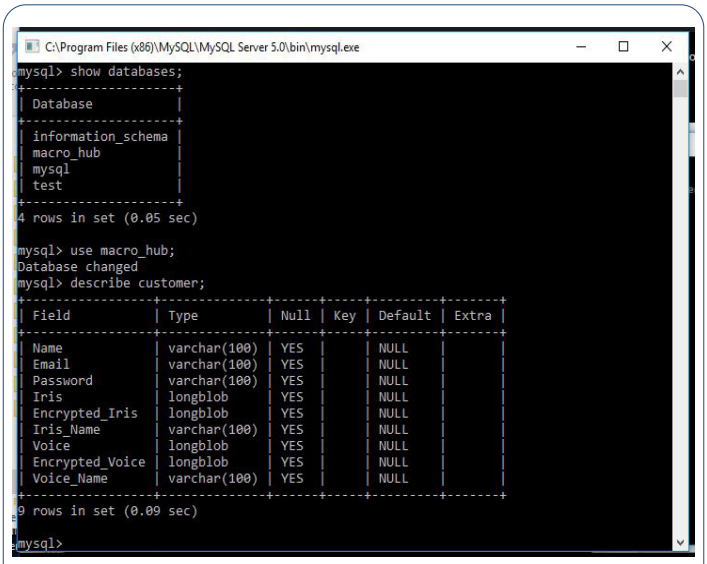

Figure 4.9 Description of customer in database.

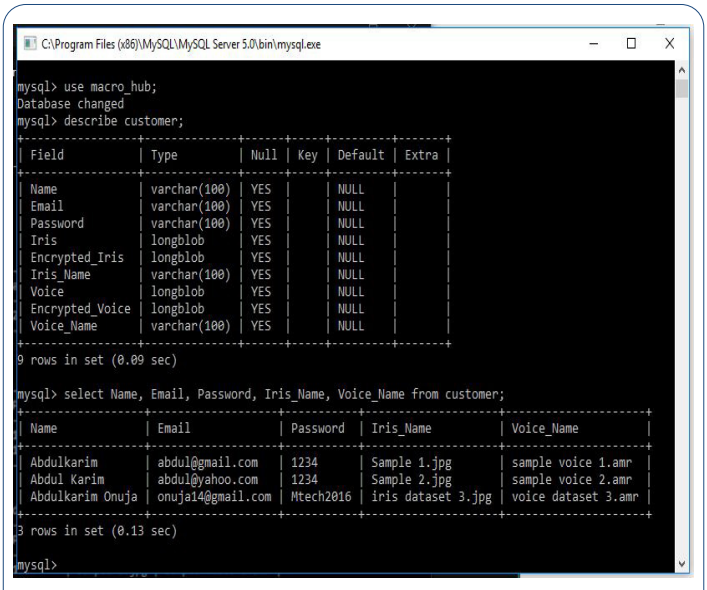

Figure 4.10 Registered customers in the database.

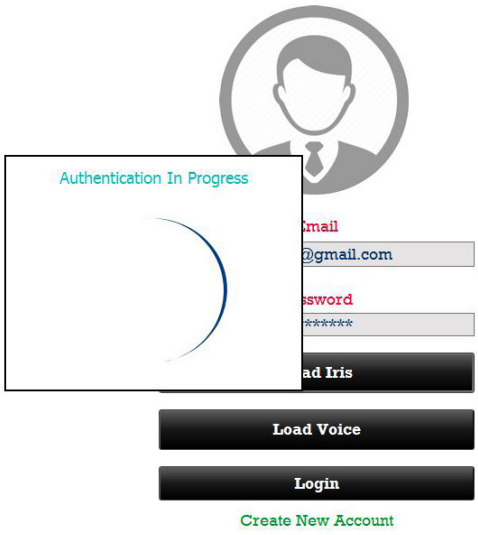

Figure 4.11 Authenticating customer.

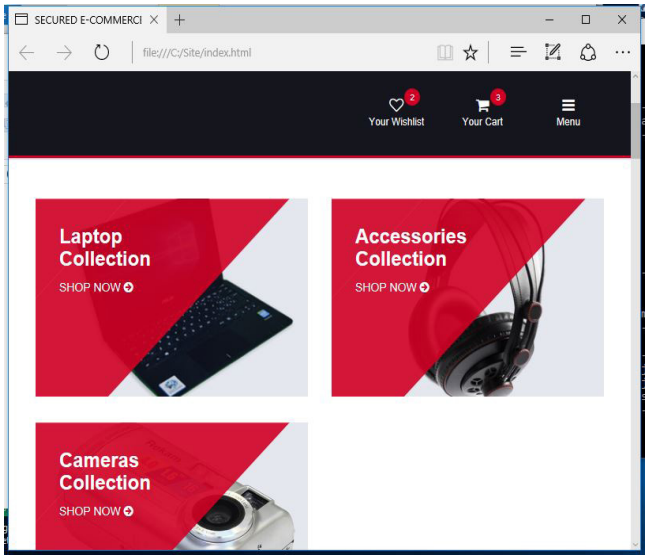

Figure 4.12 Electronic commerce website.

In the event of a customer wrongly typing his or her registered email address or password, the has an effective way of pointing out the mistake as invalid email or password in **Figure 4.13**.

In a situation whereby a captured iris image is matched against the one for a registered customer and the margin of difference is higher than the accepted threshold, the system will respond with an invalid iris message in **Figure 4.14**.

Similar warning can also be displayed by the secured electronic commerce system whenever the margin of difference between a captured voice data and the one on the database is high than the normal range accepted as seen in **Figure 4.15**.

Performance evaluation: The performance evaluation of this secured electronic commerce system using Elliptic Curve Cryptography (ECC) and multimodal biometrics with respect to time of execution and memory space needed to store information

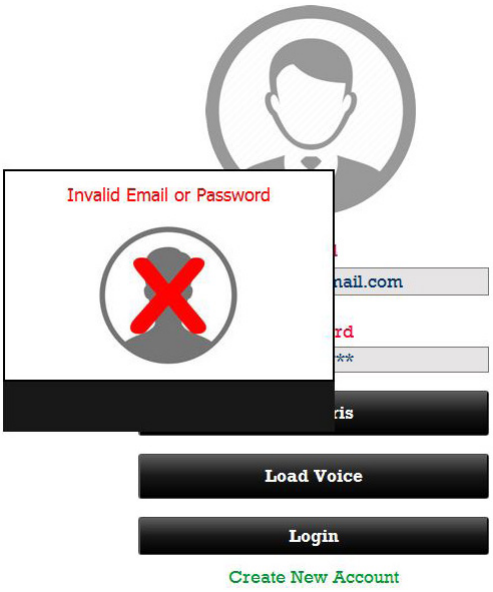

Figure 4.13 Invalid email or password.

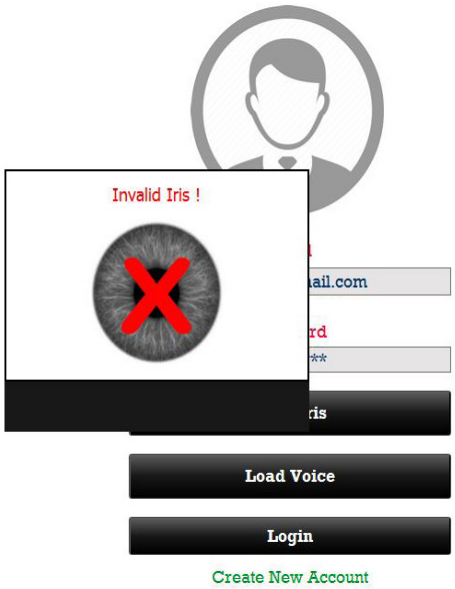

Figure 4.14 Invalid iris.

is in line with the discussion of parameters in literature review [38]. This is to achieve some of the security goals listed; that is, confidentiality and authenticity, thereby agreeing with the established reputable research findings of efficiency in the use of ECC as a means of enforcing the confidentiality (preventing attacks against the secrecy) of information by encrypting and decrypting the customer order information (COI) and payment order information (POI). The performance of the system also benefits from the digital signature capability of the Elliptic Curve Cryptography (ECC) for authentication as cited in **Table 1**. The integration of biometrics in the form of iris and voice, introduce a second and third line of defence against an attack on authentication. The memory size of the ten biometric datasets

for iris and voice used for each customer that enrolled on the electronic commerce platform are tabulated in below **Table 4.**

The key size or bit length of encryption and decryption keys are in bits, example; 4-bits, 8-bits, 16-bits, 1,024-bits, 2,048-bits, 4096-bits, 8,192-bits and 16,384. But for the convenience of this research work, these bits are converted to kilobytes to be able to add it to the sizes of iris and voice datasets. NIST recommended key-sizes for ECC and RSA is in the ratio 1 to 6.4 respectively as cited in the literature review. So, it can be deduced 20byte key

Figure 4.15 Invalid voice.

size of ECC provides the same security strength as 128 bytes of RSA key size.

In the evaluation of memory requirement, the researchers registered 5 customers and then add the size of each customer's iris and voice to the value of key sizes for ECC against the equivalent key sizes of RSA. The key sizes for the encryption and decryption algorithms were varied for test 1 to test 6 for customers A, B, C, D, and E, for comparison of memory size requirement in the model secured e-commerce system, and the graphical representation in **Figures 4.16-4.20**. In the experimental test for the performance evaluation of the secured e-commerce system, SE (iv) denotes the sum of key size for the integration of ECC, iris image and voice data in the tables, while RSA denotes the key size of Rivest Shamir and Adleman algorithm. SE (iv) is plotted against the key size of RSA in the graphical representation of the performance evaluation.

The analysis in the test for customer a starts with key size 7.68kb for RSA and 1.2kb for ECC whose succeeding values are computed by doubling the preceding values, 7.05kb for iris data and 6.80kb

Table 4: Iris and voice biometric datasets.

Customer	Iris dataset in Kb	Voice dataset in Kb
A	7.05	6.8
B	5.27	6.34
C	5.19	7.49
D	8.92	7.14
E	7.11	5.14

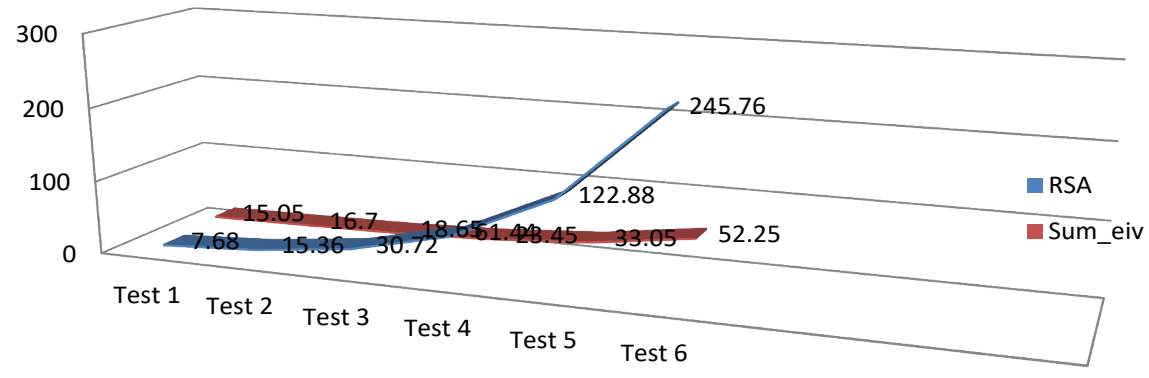

Figure 4.16 Graphical chart of memory requirement for customer A.

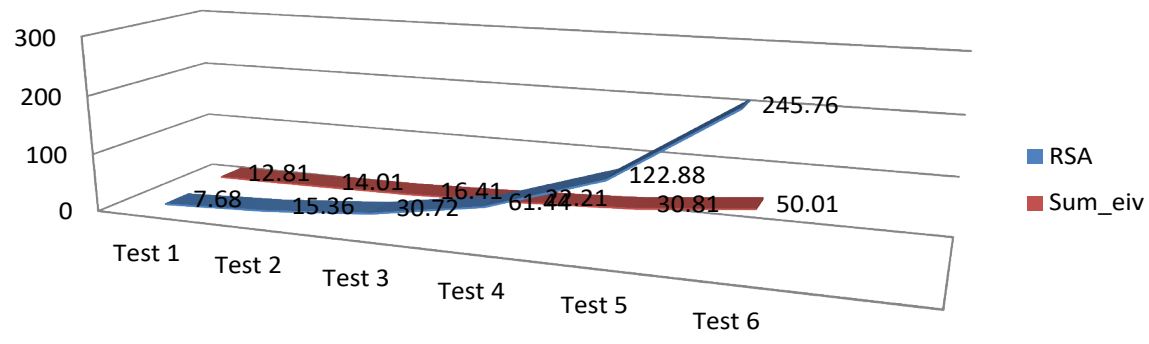

Figure 4.17 Graphical chart of memory requirement for customer B.

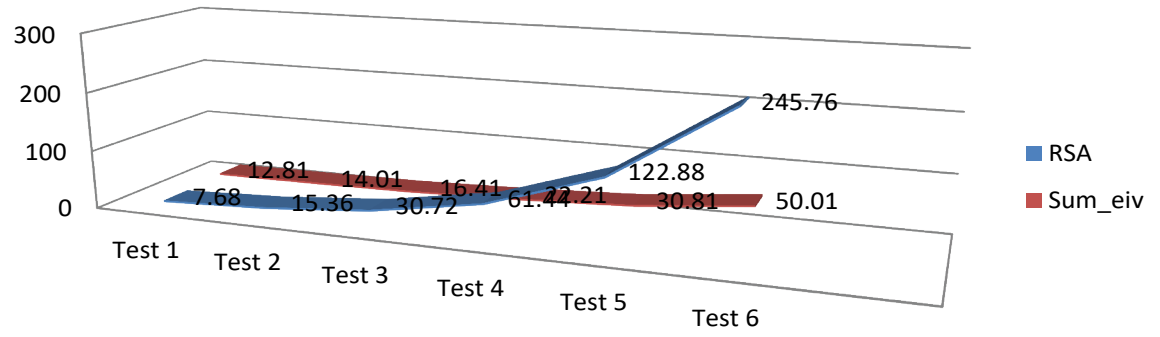

Figure 4.17 Graphical chart of memory requirement for customer B.

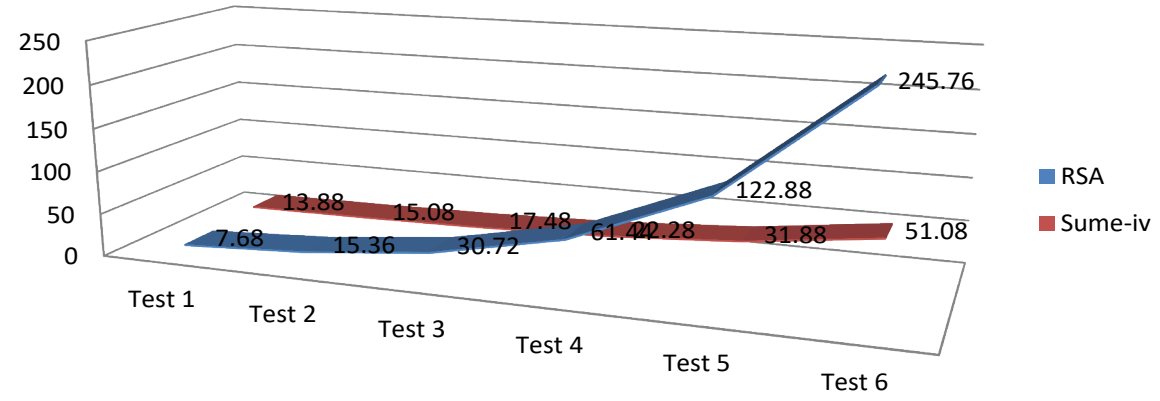

Figure 4.18 Graphical chart of memory requirement for customer C.

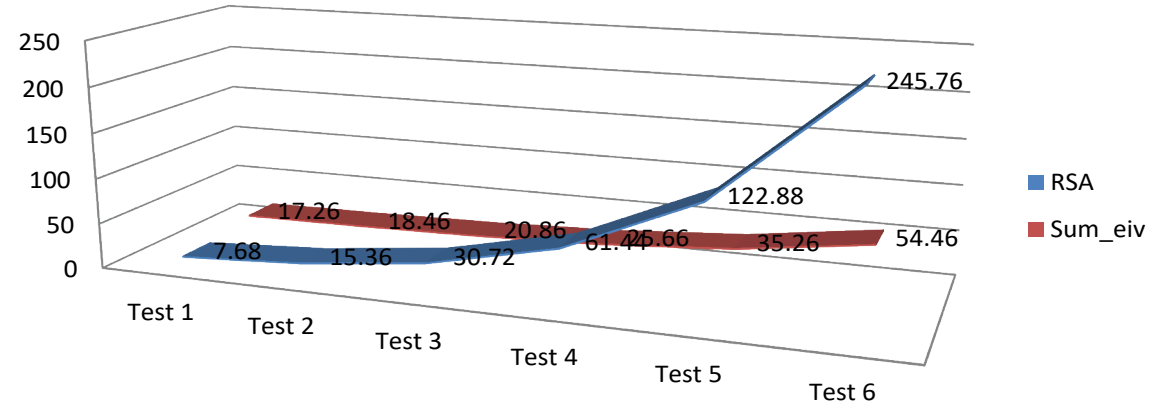

Figure 4.19 Graphical chart of memory requirement for customer D.

for voice data as shown in **Table 5**. The graph in **Figure 4.16** is the plotting of Sum iv (output) against the size of RSA (input).

The analysis in the test for customer B starts with key size 7.68kb for RSA and 1.2kb for ECC whose succeeding values are computed by doubling the preceding values, 5.27kb for iris data and 6.34kb for voice data as shown in **Table 6.** The graph in **Figure 4.17** is the plotting of Sum iv (output) against the size of RSA (input).

The analysis in the test for customer C starts with key size 7.68kb for RSA and 1.2kb for ECC whose succeeding values are computed by doubling the preceding values, 5.19kb for iris data and 7.49kb for voice data as shown in **Table 7**. The graph in **Figure 4.18** is the

Table 5: Analysis of the secured e-commerce system and RSA for customer A.

Test	Input				Output
	RSA key size in kb	ECC key size in kb	Customer A Iris (kb)	Customer A Voice (kb)	$Sum_{e\text{-}iv}$
Test 1	7.68	1.2	7.05	6.8	15.05
Test 2	15.36	2.4	7.05	6.8	16.7
Test 3	30.72	4.8	7.05	6.8	18.65
Test 4	61.44	9.6	7.05	6.8	23.45
Test 5	122.88	19.2	7.05	6.8	33.05
Test 6	245.76	38.4	7.05	6.8	52.25

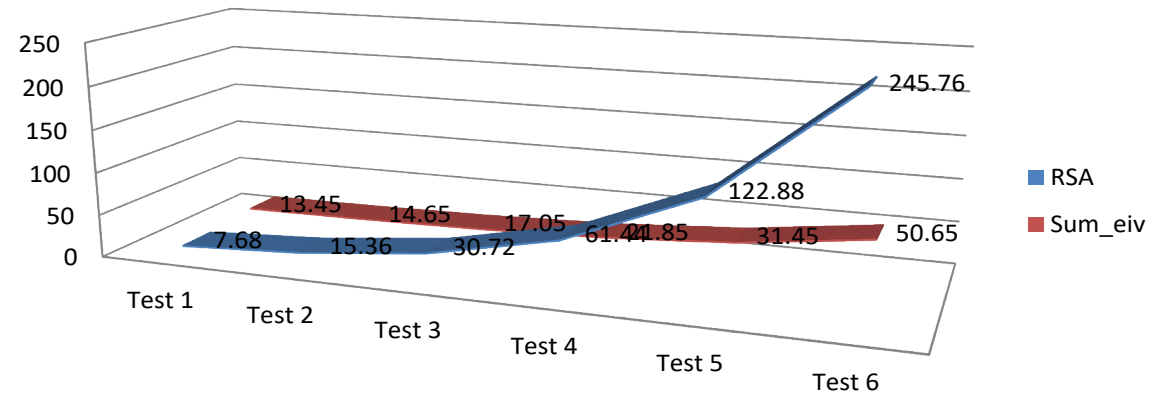

Figure 4.20 Graphical chart of memory requirement for customer E.

Table 6: Analysis of the secured e-commerce system and RSA for customer B.

Test	Input				Output
	RSA key size in kb	ECC key size in kb	Customer B Iris (kb)	Customer B Voice (kb)	$Sum_{e\text{-}iv}$
Test 1	7.68	1.2	5.27	6.34	12.81
Test 2	15.36	2.4	5.27	6.34	14.01
Test 3	30.72	4.8	5.27	6.34	16.41
Test 4	61.44	9.6	5.27	6.34	22.21
Test 5	122.88	19.2	5.27	6.34	30.81
Test 6	245.76	38.4	5.27	6.34	50.01

Table 7: Analysis of the secured e-commerce system and RSA for customer C.

Test	Input				Output
	RSA key size in kb	ECC key size in kb	Customer B Iris (kb)	Customer B Voice (kb)	$Sum_{e\text{-}iv}$
Test 1	7.68	1.2	5.19	7.49	13.88
Test 2	15.36	2.4	5.19	7.49	15.08
Test 3	30.72	4.8	5.19	7.49	17.48
Test 4	61.44	9.6	5.19	7.49	22.28
Test 5	122.88	19.2	5.19	7.49	31.88
Test 6	245.76	38.4	5.19	7.49	51.08

Table 8: Analysis of the secured e-commerce system and RSA for customer D.

Test	Input				Output
	RSA key size in kb	ECC key size in kb	Customer B Iris (kb)	Customer B Voice (kb)	$Sum_{e\text{-}iv}$
Test 1	7.68	1.2	8.92	7.14	17.26
Test 2	15.36	2.4	8.92	7.14	18.46
Test 3	30.72	4.8	8.92	7.14	20.86
Test 4	61.44	9.6	8.92	7.14	25.66
Test 5	122.88	19.2	8.92	7.14	35.26
Test 6	245.76	38.4	8.92	7.14	54.46

plotting of Sum iv (output) against the size of RSA (input).

The analysis in the test for customer D starts with key size 7.68kb for RSA and 1.2kb for ECC whose succeeding values are computed by doubling the preceding values, 8.92kb for iris data and 7.14kb for voice data as shown in **Table 8.** The graph in **Figure 4.19** is the

Table 9: Analysis of the secured e-commerce system and RSA for customer E.

Test	Input				Output
	RSA key size in kb	ECC key size in kb	Customer B Iris (kb)	Customer B Voice (kb)	$Sum_{e\text{-}iv}$
Test 1	7.68	1.2	7.11	5.14	13.45
Test 2	15.36	2.4	7.11	5.14	14.65
Test 3	30.72	4.8	7.11	5.14	17.05
Test 4	61.44	9.6	7.11	5.14	21.85
Test 5	122.88	19.2	7.11	5.14	31.45
Test 6	245.76	38.4	7.11	5.14	50.65

plotting of sum iv (output) against the size of RSA (input).

The analysis in the test for customer E starts with key size 7.68kb for RSA and 1.2kb for ECC whose succeeding values are computed by doubling the preceding values, 7.11kb for iris data and 5.14kb for voice data as shown in **Table 9**. The graph in **Figure 4.20** is the plotting of Sum iv (output) against the size of RSA (input).

Recommendation: In the quest to miniaturize computing devices and optimize computation powers, the efficiency of ECC usage, is highly recommended while computing device manufacturing companies are advised to partner with computer science and network security researchers to enhance further studies in the deployment of ECC and biometrics for emerging devices.

The need for individuals to own many passwords are increasing with the creation of user accounts for lots of online activities to which buying and selling belong. The use of biometric traits as demonstrated in this research work can save the stress of having to remember different passwords for different platforms. Biometric capturing devices for iris and voice should be made affordable and available, especially for research purpose.

In addition, most scientific research materials and tools are very expensive and are not for individual acquisition, it is recommended that provisions be made for research students to be able to access such, through the university subscriptions as a corporate entity and the procurement of tools such as iris capturing devices in the computer laboratory.

Conclusion

The system is able to register new customers within 90 seconds

and login an existing customer in the database within 60 seconds, for all the accounts created successfully. Although, the speed of internet connectivity and the processing speed of a customer's computer and that of the electronic commerce website server are factors to be considered in the ease and time with which the system is able to accomplish a transaction, the system has an efficient performance in the test laboratory as earlier stated.

The thesis is able to model a secured electronic commerce system using elliptic curve cryptography and multimodal biometrics that uses the iris and voice traits of online transaction customers to improve on the confidentiality and authenticity of customer order information that includes passwords, iris data, voice data, and payment order information in the form of automated teller machine pin numbers, one time passwords, and amount of money to be paid or debited. This is achieved with overall memory requirement of a secured system for electronic commerce reduced with the key-size of the encryption and that of decryption in kilobytes is increased beyond 30 kb.

Contribution to Knowledge

The thesis was able to formulate by modification, the ECC mathematical expression to describe the practical need to encrypt and decrypt other data types such as images and iris aside texts. The implementation of the methodology reveals the importance of specifying data types in computer programming unlike the theoretical expression of mathematical models. The performance evaluation discovers that when the system uses the sum total of 19 kb and beyond to enforce the security of confidentiality and authenticity, it is more memory efficient than systems that implements RSA with key sizes of 30 kb or higher. The development of a model that free up memory space in computing devices to add more security measures thereby increasing trust in electronic commerce security is a contribution to knowledge, for an economy that is tended towards cashless transactions to curtail money laundering.

References

1 Haseeb K, Arshad M, Ali S, Yasin S (2011) Secure E-commerce protocol. Int J Comput Sci Sec 5: 742-751.

2 James TL, Khansa L, Cook DF, Bruyaka O, Keeling KB (2013) Using network-based text analysis to analyze trends in Microsoft's security innovations. Comp Sec 36 :49-67.

3 Geetha P, Jayanthi VS, Jayanthi AN (2018) Optimal visual cryptographic scheme with multiple share creation for multimedia applications. Comput Secur 78: 301-320.

4 Patil P, Narayankar P, Narayan DG, Meena SM (2016) A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Comp Sci 78: 617-624.

5 Wang A, Wang C, Zheng X, Tian W, Xu R et al (2017) Random key rotation: side-channel countermeasure of NTRU cryptosystem for resource-limited devices. Comp Elec Eng 63:220-31.

6 Perlner RA, Cooper DA (2009) Quantum Resistant Public Key Cryptography: a survey. In proceedings of the 8th Symposium on Identity and Trust on the Internet 59: 85-93.

7 Karbasi, AH, Atani, RE. (2015) ILTRU: An NTRU-like public key cryptosystem over ideal lattices. IACR Crypt Arc 9: 546-549.

8 Ahmad K, Alam MS (2016) E-commerce security through elliptic curve cryptography. Procedia Comput Sci 78: 867-873.

9 Murillo-Escobar MA, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez RM (2015) A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Exp Syst App 42 : 8198-211.

10 Jain AK, Uludag U (2003) Hiding biometric dataIEEE Trans Pattern Anal Mach Intell 25: 1494-1498.

11 Unar JA, Seng WC, Abbasi A (2014) A review of biometric technology along with trends and prospects. Pattern Recognit 47: 2673-2688.

12 Gudavalli M, Raju SV, Babu AV, Kumar DS (2012) Multimodal Biometrics--Sources, Architecture and Fusion Techniques: An Overview. J Int Sym Biometri Sec Tech 26: 27-34.

13 Leu FY, Huang YL, Wang SM (2015) A Secure M-commerce system based on credit card transaction. Electron Commer Res Appl 14: 351-360.

14 Oppliger R, Hauser R, Basin D (2008) SSL/TLS session-aware user authentication revisited. Comp & Sec 27: 64-70.

15 Lu S, Smolka SA (1999) Model checking the secure electronic transaction (SET) protocol. InMASCOTS'99. Proceedings of the Seventh International Symposium on Modeling, Analysis Simul Comp Telecom Syst 9: 358-364.

16 Bella G, Massacci F, Paulson LC (2003) Verifying the SET registration protocols:IEEE Journal on Selected Areas in Communications IEEE J Sel Areas Commun 14: 77-87.

17 Tan Z (2014) A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. J Med Syst 38: 1-9.

18 Arshad H, Nikooghadam M (2014) Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. J Med Syst 38: 1-2.

19 Lu Y, Li L, Peng H, Xie D, Yang Y (2015) Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 39: 1-3.

20 Mahto D, Yadav DK (2015) Enhancing security of one-time password using elliptic curve cryptography with finger-print biometric. In 2015 2nd Intern Conf Comp Sustainable Global Deve (INDIACom) 47: 1737-1742.

21 Ganesan R (2009) A secured hybrid architecture model for internet banking (e-banking). J Internet Ban Comm 1: 14: 1-6.

22 Mohammadi S, Abedi S (2008) ECC-based biometric signature: A new approach in electronic banking security. Intern Symp Electronic Com Sec 56: 763-766.

23 Zhang P, Hu J, Li C, Bennamoun M, Bhagavatula V (2011) A pitfall in fingerprint bio-cryptographic key generation. Comp Sec 30: 311 -319.

24 Barker E, Barker W, Burr W, Polk W, Smid M (2007) Recommendation for key management part 1: General (revision 3). NIST special publication 800: 1-42.

25 Yoon EJ, Yoo KY (2013) Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. J Supercomput 63: 235-255.

26 Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans Inf Forensics Secur 10: 1953-1966.

27 He D, Wang D (2014) Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst J 9: 816-823.

28 Silva NB, Pigatto DF, Martins PS, Branco KR (2016) Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer. J Netw Comput Appl 60: 130-143.

29 Singh SR, Khan AK, Singh SR (2016) Performance evaluation of RSA and elliptic curve cryptography. In 2016 2nd International conference on contemporary computing and informatics (IC3I) 14: 302-306.

30 Koblitz N (1987) Elliptic curve cryptosystems. Math Comp 48 : 203-209.

31 Hankerson D, Menezes AJ, Vanstone S (2006) Guide to elliptic curve cryptography. Springer Sci & Bus Med.

32 Wu ZY, Lee YC, Lai F, Lee HC, Chung Y (2012) A secure authentication scheme for telecare medicine information systems. J Med Syst 36: 1529-1535.

33 Wen F, Guo D (2014) An improved anonymous authentication scheme for telecare medical information systems. J Med Syst 38: 1-1.

34 Geetha P, Jayanthi VS, Jayanthi AN (2018) Optimal visual cryptographic scheme with multiple share creation for multimedia applications. Comput Secur 78: 301-320.

35 Islam SH, Biswas GP (2013) Design of improved password authentication and update scheme based on elliptic curve cryptography. Math Comput Model 57: 2703-2717.

36 Jain AK, Kumar A (2010) Biometrics of next generation: An overview. Second Generation Biometrics. 12: 2-3.

37 Kumari S, Li X, Wu F, Das AK, Choo KK, Shen J (2017) Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Gener Comput Syst 68: 320-330.

38 Yasin S, Haseeb K, Qureshi RJ (2012) Cryptography based e-commerce security: a review. Int J Comp Sci Issu 9: 132-136.