Dual Biometrics And Elliptic Curve Cryptography Based E-Commerce Security (C004)

Onuja, Abdulkarim Musa
Department of Computer Science
Federal University of Technology Minna,
Minna, Nigeria
e-mail: onuja14@gmail.com

Oyefolahan, Ishaq Oyebisi
Department of Information and Media Technology
Federal University of Technology Minna,
Minna, Nigeria
e-mail: ishaq.flhn@gmail.com

Abstract—**This paper presents a preliminary result of an ongoing research which integrates elliptic curve cryptography (ECC) with biometrics as a methodology to improve the security of electronic commerce (e-commerce) transactions. While an existing system use the iris of bank clients to generate cryptographic keys for ECC, this paper use the iris and voice biometrics for authentication given that ECC has the capacity to generate encryption and decryption keys. The model is to be implemented on webservers that serves as electronic commerce platforms. The experimentation of the methodology shows a promising model that makes it harder for malicious hackers to compromise transactions on e-commerce platforms. It supports the drive for a cashless economy and payment for goods in instalments.**

Keywords-Biometrics; ECC; E-Commerce Security; RSA

• INTRODUCTION

E-commerce is a powerful tool for business transaction and transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customers as well as for service providers [20]. E-commerce websites are not only tools to support a business transaction, but also companies' channels to interact and communicate with their consumers [10]. In the retail industry, websites for business-to-consumer e-commerce (B2C ecommerce) provide more accessible, easier, faster, and cheaper methods for individual consumers to conduct their retail transactions [9]. As individuals and businesses increase information sharing, a concern regarding the exchange of money securely and conveniently over the internet increases [20]. Consequently, the future of B2C e-commerce may well depend on the selling firm's ability to manage security threats and improve consumer perceptions of Internet security [9].

Cryptography is a process of making information unintelligible to an unauthorized person, hence, providing confidentiality to genuine users of online internet infrastructure. There are various cryptographic algorithms that can be used [17]. The most commonly used algorithms as listed by [17], this include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advance Encryption Standard (AES), Rivest, Shamir and Adelman (RSA) and blowfish. Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA [18].

TABLE I Application of Public-Key Cryptosystems [18]

Algorithms	Table Column Head		
	Encryption/d decryption	*Digital signature*	*Key exchange*
RSA	Yes	Yes	Yes
ECC	Yes	Yes	Yes

It is widely used to secure information channels and gateways such as the web traffic, electronic mails, scientific information about innovation and new technologies, and e-commerce transactions. Table I reveals ECC matches RSA in utilization as both cryptographic algorithms can be used for encryption and decryption, digital signature, and key exchange.

The computational effort required in the cryptanalysis of symmetric key algorithms, that includes RSA and ECC has been compared to discover that ECC use about one-eighth of the key-size used in RSA to offer the same level of security, as shown in table II. The Table presents public-key cryptography [18] such as RSA algorithm and elliptic curve cryptography (ECC), as the key length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA. A competing algorithm that challenges RSA is the ECC. It is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography [18].

COMPARABLE KEY-SIZE IN TERMS OF COMPUTATIONAL EFFORT FOR CRYPTANALYSIS (STALLINGS, 2014; NIST SP-800-57)

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

- RELATED WORK

  - *Literature Review*

Mahto and Yadav [14] worked on the security of One-Time Password by using the irises of bank clients for generating their cryptographic keys, and then the keys are used in ECC to provide data communication security while sending the one-time password (OTP) from OTP Transaction Server to 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 this paper titled dual biometrics and elliptic curve cryptography based electronic commerce security.

Computer networks provide platform to do e-commerce tasks, online banking, and sharing of information [22]. Security is required for dual purposes; to protect customers' privacy, and to protect against fraud [7, 22]. While more than two parties communicate to each other, they worry about confidentiality, data authentication, nonrepudiation [15, 22]. In order to mitigate these issues, [22] apply cryptography with biometric features. The identification and authentication of an individual using cryptography and biometrics, provides high assurance in its security model [21, 22]. Mahto & Yadav [22] proposed an algorithm for enhancing the security of OTP using ECC with palm-vein biometric. The major influence of ECC compared to prevalent and commonly used public key cryptography such as RSA in computing devices, is that it offers higher security per bit with smaller key size [1, 22]. 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 and does not support the portability of computing and capturing devices.

  - *Research Framework*

The research framework include the comparative study of two cryptographic algorithms that results in the understanding that ECC and RSA can both perform encryption and decryption, digital signature, and key exchange. The memory requirements of the two schemes were put into considerations as discussed in the introduction. The integration of iris and voice biometrics with ECC is discovered to maintain a lesser memory space requirement after implementation. The security of the system is improved with these additional security measures. Fig. I illustrate the steps involved in the research framework.

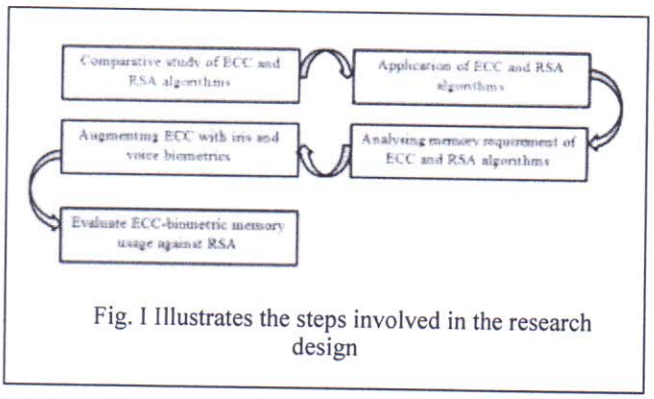

Fig. I Illustrates the steps involved in the research design

  - *Elliptic Curve Cryptography (ECC)*

Elliptic Curve Cryptography (ECC) [12] is used to establish a session-key with forward secrecy property, due to its capacity to provide a high level of security with a smaller key-size. The security of the ECC lies on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), and it can achieve same security as of RSA with the key of fewer bits [23]. The elliptic curve (EC) is given by;

$Ep(a, b) : y2 = x3 + ax + b \pmod p$ ... Equation (1)

Over a finite field Fp of prime order $p > 3$,

Where, $a, b \in Fp$, on the condition that;

$4a^3 + 27b^2 \neq 0 \pmod p$ ... Equation (2)

  - *Iris Biometric*

The iris of the human eye is a circular portion between pupil and sclera [14]. Iris is gaining a lot of attention nowadays due to its distinctiveness, and non-counterfeiting attributes [8, 14], texture pattern [4, 14] and other minute characteristics. Iris compared to other biometrics traits provides reliable and accurate user identification method [4, 14]. Fig. II present the picture of a well labelled human iris biometric

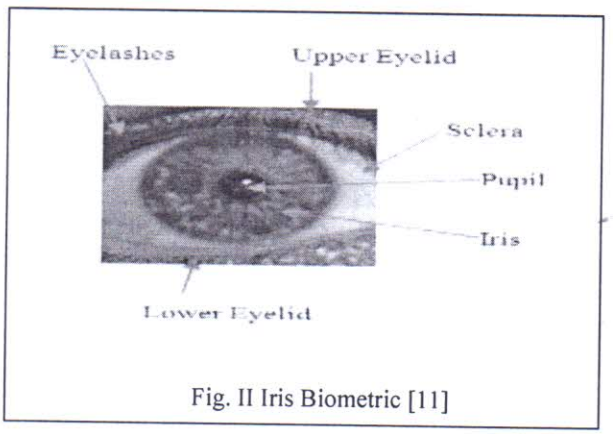

Fig. II Iris Biometric [11]

- *Voice Biometric*

Human beings have been recognized by appearance, gait, and voice for thousands of years [22]. Fingerprint-based and iris-based techniques are more accurate than the voice-based technique [16]. However, in some applications such as tele-banking applications, the voice-based technique can be integrated seamlessly into the existing telephone system [3, 16]. This informed the choice of using voice biometric to complement the use of iris in this research work. Fig.III illustrates voice biometric signal.

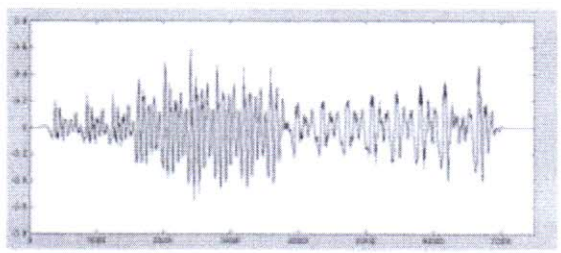

Fig. III Illustrates voice signal (https://archive.cnx.org)

- METHODOLOGY

- *Proposed Model for ECC Augmented with Biometrics*

It can be inferred from [24] that the use of ECC is more efficient since it is established that a key length size of 255 bits of ECC will have the strength of 2048 bits key-size of RSA algorithm with reference to table I. Consequently, current research in e-commerce security is interested in the use of ECC as it reduces overhead cost with respect to the memory size required for the encryption key in ECC [24]. More so, the algorithm also suits new mobile computing devices such as smart phones that can equally be used to access e-commerce websites. This work is focussed on taking advantage of the memory space afforded by using ECC to integrate another security measure in the form of iris and human voice biometrics to improve on the security of e-commerce as shown in the proposed model in fig. IV. The mnemonics used in the proposed model 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 e-commerce website server for processing. The payment order information (POI) enumerates all information required to effect online payment. Information such as Automated Teller Machine (ATM) card number, expiry date, personal identification number (PIN), amount to be paid, name of the customer, address and phone number are categorized as payment order information (POI). The proposed model also has the automated ECC encryption key as ECC_{EK} and the decryption key as ECC_{DK}. The e-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 it against the one on the bank account before sending feedback to the customer with the usual one time password (OTP) and then display a digital receipt to be printed for documentation after a successful transaction.

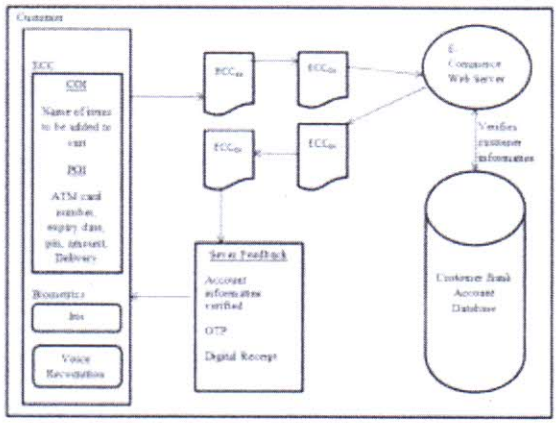

Fig. IV Model diagram for ECC Augmented with Biometrics

- *Operation of the Proposed Model*

The system requires the registration of new customers on the e-commerce platform 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, address, phone number, e-mail address, date of birth, capturing of iris and the recording of voice preferably a native dialect statement. The personal information of a customer already used for registration is matched against information submitted 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 in the mechanism of security collectively called Pretty Good Privacy (PGP) but with lower overhead cost of ECC, ECC is gaining prominence instead. 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. Otherwise, it will not allow payments to be made to avoid security breach due to repudiation. Fig. V shows the flow chart describing the operation.

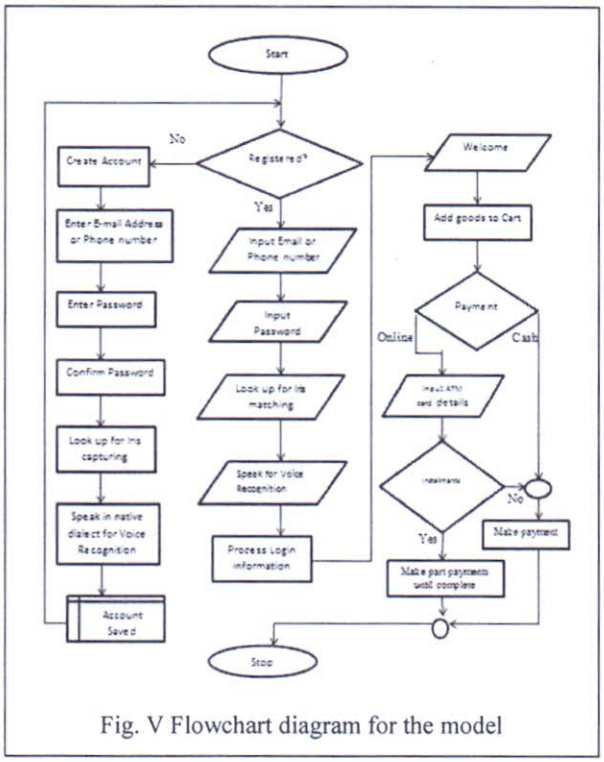

Fig. V Flowchart diagram for the model

• RESULTS

The preliminary findings of the integrated ECC-Biometric model is tabulated in Table 3, where n is key in kilobytes (kb) and $Sum_{e\text{-}iv}$ is the sum of ECC, iris data, and voice data in kilobytes (kb). NIST recommended key-sizes for ECC and RSA are minimum of 20 bytes and 128 bytes respectively [2].

ANALYSIS OF THE SIZE OF ECC-BIOMETRIC MODEL AND RSA

	ECC-Biometrics Model			
RSA (size of n kb)	ECC (size of n kb)	Iris (kb)	Voice (kb)	$Sum_{e\text{-}iv}$
8.192	1.200	6.224	9.211	16.635
16.384	2.400	6.804	7.352	16.556
32.768	4.800	7.344	6.812	18.956
65.536	9.600	8.343	7.568	25.511
131.072	19.2	5.802	6.800	31.802
262.144	38.4	6.612	6.733	51.745

The collections of dataset used for the testing of implementation focused on the use of image capturing device to capture the eyes and voices of volunteers. Image and audio processing were used to process the data to reduce noise. The sum of the key-size of ECC, Iris and Voice biometrics in the model were found to be higher when the key-size of RSA and ECC is less than 32 and 4.8 kb respectively. The key size of RSA is found to be much higher than the model when the key size is greater than 32 kb for RSA and 4.8 kb for ECC. The memory requirement for the model becomes less significant as we continue to double the key size of ECC from 19.2 kb upward while biometrics dataset maintains a normal distribution. The paper is an expression of an idea that is hoped to be updated with results from standard iris and voice capturing and matching tools in the near future. It is to be deployed practically on e-commerce webservers.

• CONCLUSION

The paper models a system that improves e-commerce security using dual biometric traits and ECC. The data used in the preliminary work can replaced with values from standard iris and voice capturing and matching tools in the near future. It is to be deployed practically on e-commerce platforms such as web applications and websites. .

REFERENCES

Figure 46. E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, ''Recommendation for key management part 1: General (revision 3),'' NIST special publication, 800(57), 1-147. 2012.

Figure 47. S. A. Chaudhry, K. Mahmood, H. Naqvi, and M. K. Khan, ''An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography,'' Journal of Medical Systems, DOI 10.1007/s10916-015-0335-y, 2015.

Figure 48. A. K. Das, ''Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards,'' IET Information Security, vol. 5, no. 3, pp. 145–151, 2011.

Figure 49. J. Daugman, and C. Downing, ''Epigenetic randomness, complexity and singularity of human iris patterns,'' Proceedings of the Royal Society of London B: Biological Sciences, 268 (1477), 2001, pp. 1737-1740.

Figure 50. J. Daugman, ''New methods in iris recognition, systems, man, and cyber- netics, Part B: Cybernetics,'' IEEE Transactions, 37 (5), 2007, 1167-1175.

Figure 51. X. Fang, S. Chan, J. Brzezinski, and S. Xu, ''Moderating effects of task type on wireless technology acceptance,'' Journal of Management Information Systems, 22, 2006, 123–157.

Figure 52. R. Ganesan, and K. Vivekanandan, ''A secured hybrid architecture model for internet banking (e-banking),'' Journal of Internet Banking and Commerce, 14(1):1–17, 2009.

Figure 53. F. Hao, R. Anderson, and J. Daugman,'' Combining crypto with biometrics effectively,'' IEEE Transactions on Computers. 55 (9), 2006, 1081-1088 doi:10.1109/TC.2006.138.

Figure 54. E. Hartono, C. W. Holsapple, K. Y. Kim, K. S. Na, and J. T. Simpson, ''Measuring perceived security in B2C electronic commerce website usage: A respecification and validation Decision Support Systems 62 11–21 http://dx.doi.org/10.1016/j.dss.2014.02.006, 2014.

Figure 55. https://archive.cnx.org/contents/fcbd1f34-bb85-442c-b25d-bd5204aea692@1/speak-and-sing-time-scaling-with-wsola

Figure 56. S. P. Jogi, and B. B. Sharma, ''Methodology of iris image analysis for clinical diagnosis,'' IEEE International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), (pp. 235-240). doi:10.1109/MedCom.2014.7006010, 2014.

Figure 57. S. Kumari, X. Li, F. Wu, A. K. Das, K. K. R. Choo, and Shen, J. ''Design of a provably secure biometrics-based multi-cloud-server authentication scheme,'' Future Generation Computer Systems, 68, 320-330, 2017

Figure 58. D. Mahto, and D. K. Yadav, ''Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce,'' Applications International Conference on Computer, Communication, Control and informatics. www.springer.com 2017

Figure 59. D. Mahto, and D. K. Yadav, ''One-time password communication security improvement using elliptic curve cryptography with iris biometric,'' International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18, 2017, pp. 7105-7114 Research India Publications http://www.ripublication.com

Figure 60. S. Mohammadi, and S. Abedi, ''ECC-based biometric signature: A new approach in electronic banking security,'' International Symposium on Electronic Commerce and Security pages 763–766, August, 2008.

Figure 61. V. Odelu, A. K. Das, and A. Goswami, ''A secure biometrics-based multi-server authentication protocol using smart cards,'' IEEE Transactions On Information Forensics And Security DOI 10.1109/TIFS.2015.2439964, 2015

Figure 62. P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, ''A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,'' Procedia Computer Science, 78, 617-624, 2016.

Figure 63. W. Stallings, ''Cryptography and network security principles and practice,'' Sixth Edition, 2014.

Figure 64. Y. W. Sullivan, D. J. Kim, ''Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments,'' International Journal of Information Management 39, 199–219 https://doi.org/10.1016/j.ijinfomgt.2017.12.008, 2017.

Figure 65. S. Yasin, K. Haseeb, and R. J. Qureshi, ''Cryptography based e-commerce security: a review,'' International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012, ISSN (Online): 1694-0814.

Figure 66. P. Zhang, J. Hu, C. Li, M. Bennamoun, and V. Bhagavatula, ''A pitfall in fingerprint bio-cryptographic key generation,'' Computers & Security, 30(5), 311-319, 2011.

Figure 67. D. Mahto, and D. K. Yadav, ''Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce applications,'' International Conference on Computer, Communication, Control and informatics, 2015. www.springer.com

Figure 68. S. H. Islam, and G. P. Biswas, ''Design of improved password authentication and update scheme based on elliptic curve cryptography,'' Mathematical and Computer Modelling, 57(1112), 2703-2717, 2013.

Figure 69. K. Ahmad, and M. S. Alam, ''E-commerce security through elliptic curve cryptography,'' *Procedia Computer Science*, *78*, 867-873, 2016