Multimodal Biometric Technology System Framework and E-Commerce in Emerging Markets

Chike Obed-Emeribe (PhD)
Head Research,
Association for Promoting Interest in Mathematics and Sciences (APRIMATHS)
Abuja, Nigeria

***Abstract*— It is self-evident that the game changer of our modern world – the "internet" has endowed the twenty first century man with enormous potentials and possibilities. Ranging from enhanced capabilities in business (e-business), governance (e-governance), politics, social interaction and information exchange. The internet has indeed shrinked the global distance that once posed a great barrier and limited man's endeavours in the preceding centuries.**

Amidst the great advantages derivable from the use of internet for various purposes lie inherent security threats. To a large extent, these security hindrances have been addressed in advanced nations of the world, as a result, internet phenomenon has pervaded all aspects of the advanced nation's economy. This is evident in different electronic platforms that are available for the delivery of various products and services. On the contrary, the application of internet in various aspects of commerce has been hampered by the challenges of security limitations due to identity issues in the developing/emerging economies. Due to these security threats, business owners and the general public in less-developed world demonstrate great sense of apathy in the use of available electronic options for the purpose of commerce.

Against the backdrop of the above, and the poor infrastructure basis of the developing nations, this research paper analyses and proposes the implementation of multimodal biometric technology frameworks with novel server architecture to tackle the security threats inherent with e-commerce in the developing world.

Keywords—Biometrics; Multimodal; Frameworks; e-commerce; Emerging Markets.

I. INTRODUCTION

Considering the enormity and sensitivity of transactions expected to be carried out via internet platforms in the wake of the accelerated internet access of the modern age, adequate means of identification and verification (authentication) should be evolved in other to give business owners, consumers and the general public an assurance of safety.

Quite a number of means of ensuring safety of transactions in e-commerce platforms have been developed in the recent past, but the inadequacies of such methods have precipitated into incessant cases of internet fraud and online theft, a situation that calls for urgent action to guarantee internet security particularly in less advanced nations. Quite recently, the issue of cyber crime and cyber security has been in the front burner.

As a solution to this internet security threat, biometric technology was evolved to ensure the security of all e-commerce transactions. The origin of biometrics can be traced back to the primordial Greek society [1] The technology of biometrics entails the use of intrinsic physical, behavioural and psychological features of individuals as a means of identification and verification (ie Authentication) . The most commonly used biometric features for the purpose of identification and identity management include: facial features, hand geometry, vascular pattern, fingerprints, retina, iris, keystroke, handwriting, gait and voice. These features have either being used singly or in combination in different security applications with the attendant advantages of robustness, universality, permanence and accessibility [3].

Due to the peculiar nature of developing world, in terms of infrastructure development and public awareness, a suitable framework for the implementation of biometric technology in e-commerce is highly imperative. This framework when fully implemented will enable business owners to adopt e-commerce as well as encourage consumers to engage in e-commerce transactions.

In this research paper, the potential prototype framework proposed is both suitable and safe to be implemented in any developing economy with such peculiarity. Under this framework, backend server architecture is delivered, in such a way as to give the multimodal mix of the biometric design. One of the bases for this research endeavour is the fact that about 79% of world population lives in the developing countries. This statistics shows that there are huge economic potentials in these countries in terms of e-commerce which is yet to be tapped owning to the barriers of poor infrastructure, legal issues, socio-cultural bottlenecks as well as lack of trust.

Given the fact that e-commerce has been proven to improve market efficiency, operational effectiveness, access to markets and linkages, establishing a highly secure and robust e-commerce system in the emerging market economies is truly a well come development.

II. ANALYSIS AND DESIGN OF MULTIMODAL BIOMETRIC TECHNOLOGY

It has been advocated at different quarters that data and system security is the next frontier of information technology in the coming centuries. As more people access the internet infrastructure, more businesses go online, and most traditional operations become internet based, reliable means of user

identification and verification become of high essence. The only means of attaining this height of online internet security is via biometric technology.

Basically, a complete biometric system majorly is characterized by three elements namely;

- Enrollment sub-system
- Template representation
- Matching process subsystem.

These three main elements are depicted in the figure below:

Fig.1. The general block diagram representation of a typical Biometric System.

A. THE ENROLLMENT STAGE:

At this stage, data samples are collected from the enrollee. Mostly devices such as scanners and readers are employed for this purpose. This stage is usually crucial as any mistake will lead to identity misrepresentation.

B. THE TEMPLATE REPRESENTATION STAGE:

At this stage of biometric operation, data samples obtained at the enrollment stage are gathered and stored for future referencing. This operation is usually carried out by some specific software tools.

C. MATCHING PROCESS SUBSYSTEM:

Here, input data is compared with the already store data template within the system for the purpose of identification and verification.

III. BIOMETRIC PROCESSES AND CLASSIFICATIONS

As earlier stated, the biometric process entails capturing the unique biological, behavioural or psychological features of a particular individual with a view to identification and verification. This process can be done basically in two modes, viz: unimodal and multimodal forms. Each of these modes of biometric authentication has its computational requirements as well as inherent advantages and demerits. The adoption of any particular mode depends on the expected outcome of that application.

IV. THE UNIMODAL BIOMETRIC SYSTEM

As the name suggests, this is a type of biometric process that uses only single biometric feature such as fingerprint, iris, retina, vascular pattern etc for the purpose of authentication of individuals either in e-commerce platforms, e-governance etc. The unimodal biometric system is the most commonly system used in e-commerce due to its simplicity and affordability.

Although no particular biometric system can be said to be 100% efficient, but the loophole of the unimodal biometric systems currently employed in most e-commerce raises various questions on the degree of the security of certain sensitive transactions being done in e-commerce today. Among these weaknesses are: limited degree of freedom for users, noisy input data during enrollment and use, inter-class variations, distinctiveness, non-universality and spoof-attacks. All these weakness found to exist in the unimodal biometric system gives room for a more robust system devoid of such loopholes to evolve. Hence the multimodal biometric system came into being.

V. THE MULTIMODAL BIOMETRIC SYSTEM

This combines two or more unique biometric features of the individuals for authentication. The combination of these features could be in terms of multiple snapshots of a single fingerprint, faces or palm or any combination of choice. However, "the biometric characteristics of an individual is normally a biological feature which can either be genetically implied possibly environmentally altered or feature acquired or learned over time that can be used to recognize or identify the individual"[4]. How secured a system is, usually is based on the amount of time it will take an impostor to decipher the ciphered biometric digital data streams. Multimodal biometric system, due to its high computational requirements is more robust and less prone to attack by an impostor.

"A recent study undertaken within the context of a fingerprint biometric system indicated that a blend of multiple enrollment templates or multiple fingers of a specific user can improve a fingerprint verification system with greater accuracy" [2]. While great attention has been given to the front end processes of this biometric system mode, the backend biometric server architectural framework has received limited attention especially as it concerns emerging economies.

Thus, the next section of this paper lays down a framework for proper implementation of a multimodal biometric server authentication system based on the combination of fingerprints and palm biometric features.

VI. FRAMEWORK FOR IMPLEMENTATION

Under this framework, the fundamental prototype architecture at the backend consists of the e-commerce database server, a Transaction Process Monitor Server, and a multimodal biometric database server. See fig1.5. Similarly, the frontend stage (client/user system) comprises the hardware input device (e.g. a pad with a scanner for both fingerprint and palm made to be used for enrollment of intended e-commerce customers.

However, here, multimodal server architecture was selected due to the fact that the number of potential e-commerce users is expected to grow with time (this is a feature that is commonly found in emerging markets with high population growth rate). The superiority of the multimodal biometric system considered in this paper is in the fact that the palm geometry is most suitable for verification whereas the fingerprint which reveals a lot about an individual's identity is used for identification [2]. This is most suitable and secured for the developing economy where trust barely exists. This framework is such that the actual authentication takes place in

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

the multimodal biometric server, whereas, the Transaction Monitor Server will be responsible for the encryption.

A typical transaction flow for the proposed framework is as shown below: Also, see Fig2.

- User initiates a transaction from his/her client system using the e-commerce website.
- Transaction process monitor server comes up with both private and public key using the RSA algorithm. While the public key is sent to the client computer, the private key is retained in the transaction process monitor.
- At the front end, the Rijindael crypto method will be used to generate the key for encrypting the fingerprint and palm of the user.
- Further encryption of the user fingerprint and palm is done using RSA algorithm with the public key earlier received from the transaction process monitoring server.
- Fully encrypted data is then transmitted to the e-commerce server, and then to the Transaction Monitoring Server.
- Concurrency control is then ensured by the Transaction process Monitoring Server after which the encrypted data is transferred to the multimodal biometric server which decrypts the data and carries out comparison with the biometric data earlier stored.
- If a match is found, information will be transferred to the Transaction Monitoring Server which in turn sends a signal to the e-commerce server to allow the user's transaction or otherwise.

The cryptographic techniques adopted in this framework as well as the physical layout of the servers involved make it most adaptable and suitable in emerging market environment.

VII. The Architectural Framework

In almost all developing economies, infrastructure is lacking. In this case, adequate network and telecommunication infrastructure upon which e-commerce depends are epileptic to the extent that e-commerce cannot perverse the length and breadth of the country in question. Against this backdrop, a suitable backend and frontend architectural framework is highly required. See Fig1.5.

Basically, in engineering network architecture, the physical layout of network entities vis-a-vis server setup can be either a centralized architecture or decentralized architecture [2]. A typical example of a decentralized architecture is the peer-to-peer- (P2P) networks in which case there is no central controlling system.

Contrarily, the centralized architecture has a central controlling system or server. This is usually a case where application and operating system controlling the main operations or the whole setup is domiciled in the server (i.e. client/server framework). Under this arrangement, the client initiates a request for the required resources from the central server. That is, the client does not have an intelligence of its own. The distributed system based on centralized architectural framework has the advantage of adequate access control, but the issues of concurrency and failure recovery have been a major setback, especially in an environment with poor network infrastructure.

As a matter of fact, due to e-commerce requirement that the business owners determine what transaction is required or otherwise on their platform, the centralized architecture (i.e. client/server model) is still most suitable for e-commerce processes and operations.

In view of this fact, e-commerce operations in a developing economy with poor network infrastructure can best be based on a multi-tier architectural framework so as to tackle the issues of concurrency and failure recovery. By concurrency it implies a situation whereby numerous users are accessing a server at the same time. When this happens, if the network architecture is not based on a robust framework, failure rate will be high leading to poor quality of service (QoS) delivery to the consumers. Thus, in an emerging economy, a multi-tier client/server architectural framework is most suitable so as to take care of the issue of concurrency and failure recovery, especially in view of the huge potentials of the markets in the e-commerce sector occasioned by high population of the emerging market economies.

Under this architectural framework, the Transaction Processing (TP) Server will be configured to restrict processes from running concurrently in order to avoid the contention for resources between the e-commerce database server, and the multimodal biometric server. A typical multi-tier client/server architecture that can operate under this framework is the 3-tier architecture as depicted in fig1.5 below, in this, case the e-commerce server houses the database for the e-commerce business, the middleware which serves as the Transaction Processing Monitoring Server and also the multimodal biometric database server for the template capture from the enrollees.

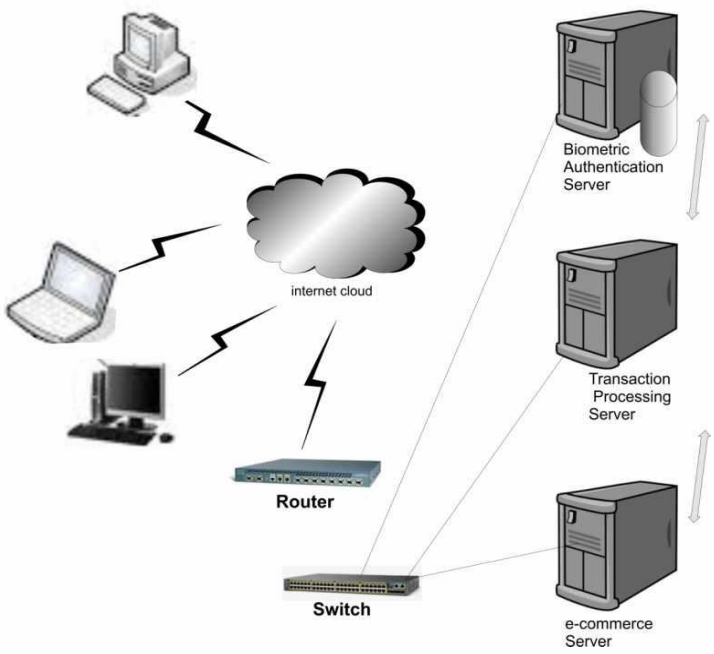

Fig1.5 : Backend Multimodal Biometric Server Architectural Layout

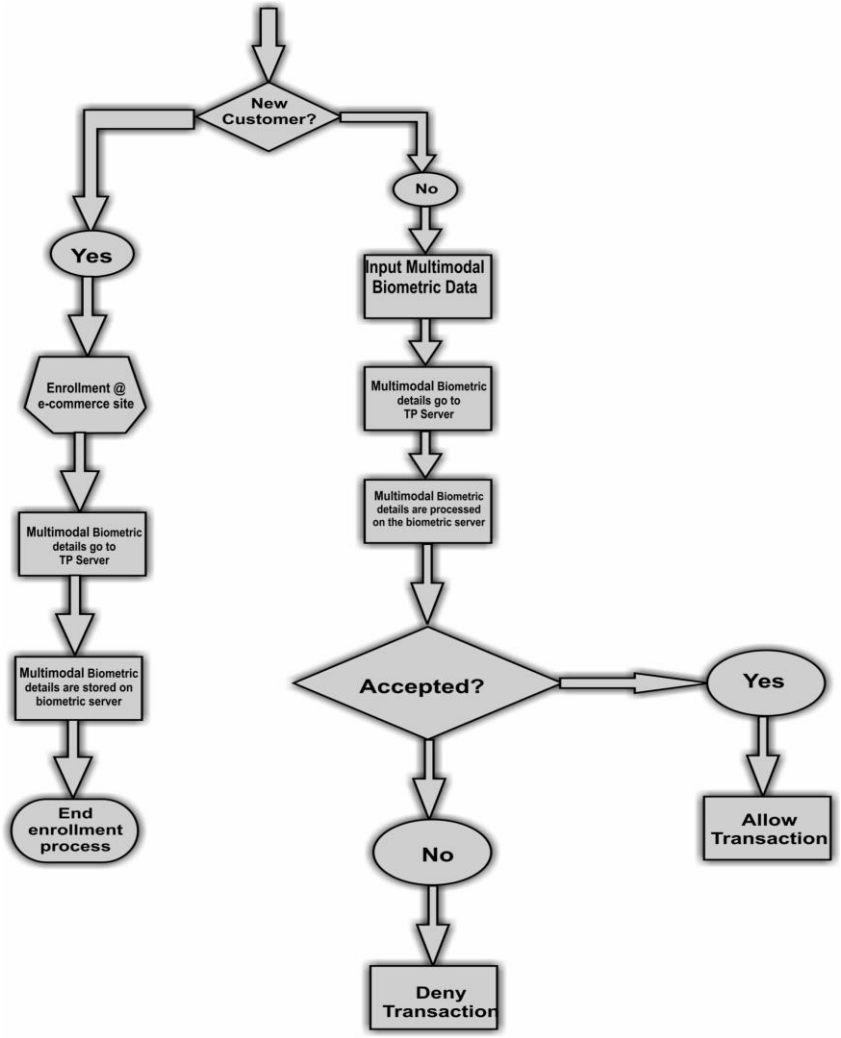

Fig 2: Process Flow of the Multimodal Biometric Architectural System Framework

VIII. CONCLUSION

The paper delved into the analysis of multimodal biometric technology framework and its application to e-commerce. This application was directed to emerging market economies where telecommunication and other network infrastructure are grossly inadequate, yet due to its growing population holds enormous potentials for e-commerce business. The framework for the implementation of the identified multimodal biometric system for the developing economies where trust and identity theft is still a challenge was laid. Information gathered from secondary sources revealed that one of the main reasons business owners, consumers, and general public show high apathy in e-commerce participation is apart from poor infrastructure, lack of security of their transactions.

Hence, in view of this fact, implementation of multimodal biometric system using the laid down framework in e-commerce for emerging market economies will boost public confidence as well as ensure increased participation in e-commerce business transactions.

For the purposes of future research in this area, it is hereby suggested that more work is required in area of data encryption techniques to enhance the security of biometric database. With a more robust data encryption method, more time will be required by any impostor to carry out identity theft there increasing the security of the entire biometric system.

REFERENCES

[1] Mguire, M. (2009), "The birth of biometric security", Anthropology Today, 25,2,pp.9-14, EBSCOhost, [Online]. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds

[2] Kunle Adetunmbi, (2013), "Biometrics in e-commerce", MSc thesis submitted to the University of Liverpool.

[3] Dantcheva, A. Velardo, C.D'Angelo, A.Dugelay (2011), "Bag of soft biometrics for person identification", Multimedia tools & applications, EBSCOhost, [Online]. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds

[4] Schatten, M.Baca, M & Cubrilo M. (2010), "Towards a general definition of biometric systems", International Journal of Computer Science issues (IJCSI), 7,4, pp. 1-7, Computers & Applied Sciences complete, EBSCOhost, [Online]. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds

[5] Al-Dala'in, T. Summons, P. & Suhai, (2009), "A prototype design for enhancing Customer trust in online payments", A journal of computer Science, [Online}. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds

[6] Anderson, R. (2008), "Security Engineering: A guide to building dependable distributed systems". 2nd edition, Indianapolis, Wiley Publishing Inc.

[7] Ariyaeeinia, A. (2003), "Biometrics on the internet", IEE proceedings, vision, image & signal processing [Online]. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds

[8] Asha, S. & Chellappan, C. (2012), "Biometrics: an overview of the technology, issues and applications", International Journal of computer applications [Online]. Available at: http://research.ijcaonline.org/volume39/number.

[9] Basha, A. Palanisamy, V. & Purusothaman, T. (2011), "Efficient Multimodal Biometrics Authentication using Fast Fingerprint verification and enhanced Iris features", Journal of Computer Science, Computers and applied science complete, EBSCOhost, [Online]. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds.

[10] Boukhari, A. Chitroub, S. & Bouraoui, I. (2011), "Biometric signature of private key by reliable Iris recognition based on flexible-ICA Algorithm", International Journal of communications network & system sciences, computers and applied science complete, EBSCOhost [Online]. Available at: http://ehis.ebscohost.com.ezproxy.liv.ac.uk/eds

[11] Corbitt B., Thanasankit, T. & Yi, H., (2003), "Trust and e-commerce: A study of consumer perceptions", Electronic commerce Research & Applications, Business source premier, EBSCOhost, [Online]. Available at: http://www.sciencedirect.com.ezproxy.liv.ac.uk/eds

[12] Dihir, V. Singh, A. Kumar, R & G Singh, (2010), ' Biometric Recognition: A modern era security', International Journal of Engineering & Technology, vol2, no.8, [Online]. Available at: http://www.ijest.info/docs/IJEST

[13] Driscoll, E.C & Fowler, R.C, (1989), 'A comparison of centralized versus distributed architectures in Biometric access control systems', security technology, 1989. Proceedings, 1989 International Camahan Conference, [Online]. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp

[14] Elbirt, A.J (2005), "Who are you? How to protect against identity theft", Technology & Society Magazine, IEEE, Vol.24, no 2, pp. 5-8, summer 2005, [Online]. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp

[15] Jones, P. Williams, P. Hillier, Comfort .D, (2007), "Biometrics in retailing", International Journal of Retail & Distribution Management, Vol.35 Iss 3, pp.217-222, [Online]. Available at: http://linkspringer.com.ezproxy.liv.ac.uk/content/pdf