Adoption of Biometric Fingerprint Identification as an Accessible, Secured form of ATM Transaction Authentication

Michael Mireku Kwakye
Faculty of Informatics
Ghana Technology University College
Accra, Ghana

Hanan Yaro Boforo
Genkey Solutions Africa
Accra, Ghana

Eugene Louis Badzongoly
Faculty of Informatics
Ghana Technology, University College
Accra, Ghana

***Abstract*—Security is continuously an important concern for most Information Technology-related industries, especially the banking industry. The banking industry is concerned with protecting and securing the privacy and data of their customers, as well as their transactions. The adoption of biometric technology as a means of identifying and authenticating individuals has been proposed as one of the varied solutions to many of the security challenges faced by the banking industry. In this paper, the authors address the ATM transaction authentication problem of banking transactions using fingerprint identification as one form of biometric authentication. The novel methodology adopted proposes the use of an online off-card fingerprint verification, which involves the matching of live fingerprint (templates) with pre-stored templates read from the ATM smart card. The experimental evaluation of the proposed methodology presents a system that offers a faster and relatively better security of authentication, as compared to previous and existing methodologies. Moreover, the use of BioHASH templates ensures an irreversible cryptographic hash function, facilitates a faster authentication, and enables an efficient framework of detecting potential duplicates of banking account holders.**

Keywords—Information Technology; Automatic Teller Machine; Biometrics; Fingerprint; BioHASH; Token

I. Introduction

The revolution of Information Technology (IT) has generated a lot of development and innovation in the areas of business, academic and industrial research, and healthcare, amongst others. Technology has become the backbone of every organization and an appreciable volume of system, human, and financial resources are utilized in the adoption, development, and incorporation of these technologies into the day-to-day activities of an organization.

The emergence of the internet has paralleled the IT revolution and facilitated IT development into various innovations [1]. The internet has changed the manner in which individuals and organizations interact and communicate with each other [2]. The internet has also changed the way businesses operate, and as a result the introduction of electronic commerce has enabled easy, accessible, and efficient medium for businesses to effectively interact with their customers and partners all over the world [2].

The banking industry has become one strategic industry that utilizes Electronic Commerce (E-Commerce) [3]. The past decade has seen an increase in the adoption of technological innovation in the banking sector. The increase is mainly being driven by the desire of the banks to remain profitable and competitive [4]. Automatic Teller Machines (ATMs), telephone banking, and online banking make up more than 50% of the banking transactions in some developed economies, like the United States of America (USA); and this is growing at a rate of 15% annually [2]. Electronic banking presents the banking industry with an electronic and remote distribution channel, which serves as an electronic market place where consumer with individuals and business can conduct their financial transactions virtually [4].

With the increase in electronic banking, one major concern for this medium of transaction processing is security and privacy [2]. Most internet users get worried about privacy issues, including transparency in the collection, use, and disclosure of their personal information. A relative number of users are also worried about the security of their bank accounts and transaction details [2]. Electronic banking comes with a high level of exposure to common cyber-related risks. Varied risks, such as, information hacking, cyber-sabotage, and cyber-terrorism, amongst others, all together adopt unique ways of attacking a system [5]. Electronic banking requires the implementation of high-quality security features and procedures [2]. One of such security features is the use of biometrics in identifying and authenticating an individual user to a system. Biometric technologies enable the identification and authentication of an individual user based on the physiological and/or behavioural characteristics [5]. Though biometric systems have been successfully adopted and deployed in areas, such as, criminology, health, electioneering procedures, and immigration control, there is little research and implementation pertaining to the banking industry [5].

In this paper, the authors introduce a framework that offers a viable biometric technology implementation in the banking industry. The primary focus is the adoption of fingerprint identification as a biometric measure for an accessible and secured form of ATM and card technologies security in the area of electronic banking.

The motivation of the authors is to employ the concept of BioHASH templates, which ensures an irreversible cryptographic hash function, facilitates a faster authentication, and enables an efficient framework of detecting potential duplicates of banking account holders. The authors' key contribution in this paper is the adoption of an online off-card fingerprint verification, which involves the matching of live fingerprint (templates) with pre-stored templates read from the ATM smart card.

The technical contributions are summarized, as follows;

- The authors design a biometric enrolment system that requires new customers of a financial institution to register their biometric information together with their biographic information during account opening;
- The authors propose the design and implementation of an online off-card verification and biometric authentication system on ATMs that works without a remote connection to an application server for verification and authentication on the ATM system;
- The authors employ the BioHASH template technology for a cryptographic hash function in the identification, verification, and faster matching of biographic data.

The rest of the paper is organized as follows. In Section II, the authors review the fundamental background studies on ATM banking and biometric authentication. In Section III, the authors discuss the proposed biometric (fingerprint) methodology framework. Here, the authors address the overview of the proposed system for the adopted methodology approach. In Section IV, the authors address the proposed system architecture, discuss the modules encompassing the proposed architecture, and outline the overall system operation and flowchart. In Section V, the authors address the propositions of the fingerprint methodology; where the authors outline the merits for the accountholder and transaction processing and authentication procedures. In Section VI, the authors address the implementation, testing, and evaluation of the methodology framework; as an effective approach in providing security in ATM systems. The authors discuss the related work and comparison of other approaches in Section VII. Finally, in Section VIII the authors conclude, discuss open issues and the areas of future work.

II. Background

Information Technology (IT) has brought about improved efficiency and effectiveness in the operations of most organizations. This trend has posited an assertion that currently IT is the backbone of every organization. Electronic Banking (E-Banking) is the provision of banking products and services through electronic delivery channels. Services offered via electronic banking channels include, Automated Teller Machines (ATM), Internet banking, and Mobile banking, amongst others. ATMs have existed in recent past and are found in most parts of the world for different forms of electronic transactions and processing. ATMs have become the most visible pieces of electronic hardware in the banking sector, and they are also the fastest growing element in banking. ATMs became popular more than 20 years and as a result banks and their respective client users have since gained a lot of advantages from the use of ATMs [6].

Biometric authentication using fingerprint identification is seen by many as the solution to most of the theft and fraud cases being reported in the use of ATM systems and ATM cards. Biometrics-based authentication offers several advantages over other authentication methods, as there has been a significant surge in the use of biometrics for user authentication in recent years [7]. Onyesolu and Ezeani (2012) [8] in their study found that, majority of their respondents chose fingerprint identification as the preferred biometric identification solution to ATM card theft and fraud. In the proposed biometric-based ATM authentication system designed and developed by the authors in Oko and Oruh (2012) [7], the result of their methodology and testing evaluated that biometric authentication on ATM systems was practicable and could be implemented in production environments.

Daula and Murthy (2012) [9] developed an embedded fingerprint identification system which is used for ATM authentication. Their system makes use of GSM modem for authenticating users. The system required banking institutions to capture the biometric fingerprints and cellular (mobile) number of customers during account opening. At the ATM system console, the customer of the bank places his/her fingers on the fingerprint scanner attached to the ATM machine. The system on the ATM then compares the fingerprints to the previously captured fingerprints. If the fingerprints are found to be a match, a 4-digit code is generated and sent to the customer mobile phone. These 4 digits are then entered on the ATM. This system does not require the use of an ATM card. The system is secured because it securely verifies and authenticates the identity of a cardholder who tries to do transaction through the ATM.

Biswa et al. (2012) [10] also conducted a research which was aimed at developing a crypto-bio authentication system in ATM banking systems. Their system relied solely on the usage of retinal image. Hossian et al. (2013) [11] proposed a biometric authentication scheme for ATMs, their system made use of an Advance Encryption Standard (AES) processor instead of the Triple Data Encryption Standard (3DES). The study concluded that, the usage of an AES processor and fingerprint biometric identification made the ATM transaction more secured.

Previous works in the area of biometric fingerprint authentication of ATM cardholder followed a client-server paradigm. The ATM system captures the scanned fingerprints of a cardholder who wants to perform a transaction and transfers it to a biometric verification application on a remote server. The application connects to the biometric repository (biometric database) of the financial institution that owns the ATM system, and verifies the submitted fingerprint templates against the pre-existing templates of the cardholder in the biometric repository. The system developed by Daula and Murthy (2012) [9] follows the same paradigm and improves the procedure in generating a 4-digit Personal Identification Number (PIN) that is sent to the cardholder via a Short Messaging Service (SMS). The 4-digit code is then entered and verified on the ATM.

Venkatraman and Delpachitra (2008) [5] in their study concluded that, though biometric has been successfully deployed in areas, such as, immigration control and criminology, there is little literature on their implementation in the banking sector. Their study identified 4 main categories of issues that are critical to the viable adoption of biometric-based authentication in New Zealand. These factors are listed as; Technological, Management, Legal and ethical, and Monetary.

The biometric identification systems described above have some flaws that can impact on their performance. The solution proposed by Daula and Murthy (2012) [9] relies on the use of a 4-digit PIN that is sent to the account owner via a SMS. This PIN is entered at the ATM terminal in order to complete the authentication process. The major flaw with this system is the delivery of an SMS is not 100% reliable because of the unreliable channels in telecommunication networks. There are instances where the SMS will fail to reach its destination or it could take quite a while in reaching its destination. Additionally, the system only limits the use of the ATM in connection to the ownership of a mobile phone.

Other systems as one described by the authors in Gelb and Decker (2011) [12] requires access to a central biometric database in performing identification or verification. However, this method can result in higher error rates depending on the number of templates being accessed. The system also poses privacy concerns because the biometric of an individual are stored in a central database [13]. Firstly, access to a central database during an authentication process can be quite slow depending of the number of templates stored on the database. Secondly, the use of a central database means that, authentication at the ATMs can only be done for people who have their biometric information stored on the central database that is being access by the ATM. This makes it impossible for a cardholder to perform transactions on ATMs owned by different financial institution even if they are using the same biometric vendors as the parent institution of the cardholder. This is mainly because their ATMs will most likely connect to a different biometric repository.

The proposed solution in this paper described in Sections III, IV, and V addresses the major flaws identified in the previous systems above, and will employ the use of smart card (debit cards) with the biometric information of the cardholder encrypted on the card.

III. Fingerprint Methodology Framework

In this Section, the authors address the problem statement leading to this research and propose a methodology solution that is efficient and secured enough in comparison to earlier and existing approaches.

A. *Problem Definition*

The continuous growth in the various paradigms of financial services, such as, Electronic Commerce, Internet Banking, and ATM banking requires the development and implementation of sound security systems and procedures [2]. ATM transactions require the designing and implementation of authentication mechanisms in a remote environment. The current systems of authenticating ATM transactions involve the use of an ATM card and a Personal Identification Number (PIN).

The major concern with this type of authentication is that, ATM cards can be cloned on one hand, and on the other hand, PINs are often shared with family relatives or close associates. Sharing of PINs happens when a cardholder (account owner) decides to allow a friend, an associate, or a family relative undertake some ATM transaction on his or her behalf.

ATM fraud is a major issue being faced by most financial institutions, research has shown that, there is a continuous rise on the number of ATM fraud being reported yearly [8].

B. *Overview of Proposed Biometric ATM Methodology*

The authors approach for designing an efficient biometric ATM solution for banking transaction is such that, an individual’s biometric details will be captured when opening an account. This biometric information will be sent to a third party biometric vendor (say, Genkey Solutions), and the vendor will process the biometric fingerprint information and generate BioHASH tokens from them. The BioHASH token is written onto the microchip of a smart card or a debit card. The captured biometrics are discarded after BioHASH tokens have been generated from them. At the point of authentication or performing a transaction at the ATM, the pre-stored biometric details on the smartcard and the live fingerprints captured at the ATM are sent to an authentication server in a secured manner. This approach ensures that verification is not done against a set of templates stored in a database. This decreases the possibility of a false reject identification and also gives the user more privacy; having his or her biometric information in his or her own custody [13].

The authors address the methodology using the diagram in *Figure 1* below. This system architecture outlines various components; such as, Registration Client, Biometric Database to store biometric templates, Biographic Database to store the biographic details of the account holder or customer, and the Biometric Vendors De-duplication Server. Communications between these various components is done over a secured network. Each of these components is described in Section IV (Proposed System Architecture).

IV. Proposed System Architecture

The proposed system architecture is modelled into 2 main modules; namely, the Registration Client module and the Biometric Authentication module. The authors discuss each of these modules, as follows:

A. *Registration Client Module*

The Registration System Module is split into 2 subsystems; namely, the Registration Client, and the Biometric Vendor’s de-duplication server. The Registration Client is made up of the following components: the Application Server, the Work Station (for capturing biographic, biometric details of applicants and also for generation and producing ATM cards), and the Storage (for customer biographic information and biometric information). The Biometric Vendor’s de-duplication server is made up of the following components; the REST Application Server, and the Storage (for biometric information).

The authors illustrate the diagrammatic description of this module in *Figure 2*. The diagram depicts the processing that takes place on each of the various components that make up the registration module. The Enrolment Workstation illustrated in the diagram is used for capturing both Biographic and Biometric data from a Customer. The biographic details are validated and stored in the Biographic Database, the Biometric data is sent to the de-duplication server (Biometric Web Server) for de-duplication to take place. The de-duplication server processes the fingerprints and generates BioHASH templates and matches those templates against templates previously stored in the Biometric Database.

B. Biometric Authentication Module

This system is operational on the ATMs when users are about to perform transactions. *Figure 3* below illustrates the system architecture for the biometric authentication module. The biometric authentication module is made up of the following components; the ATM Console, the Smart Card, and the Fingerprint Scanner (attached to the ATM console).

The system architecture (*Figure 3*) depicts the general flow of an online verification process. Every activity related to the verification takes place in the biometric authentication server. The ATM performs the following functions outlined below, before sending biometric information to the biometric authentication server (verification server), for verification and/or authentication. These are;

- Validate ATM card;
- Read the ATM card to retrieve biographic and biometric information (BioHASH templates) of the cardholder;
- Invoke Fingerprint scanner to take fingerprints of cardholder;
- Encrypt scanned fingerprints and information read from ATM card;
- Transmit biometric information to biometric authentication server for verification (authentication);
- Grant or deny access depending on the success or failure result, respectively, from the verification (authentication) process.

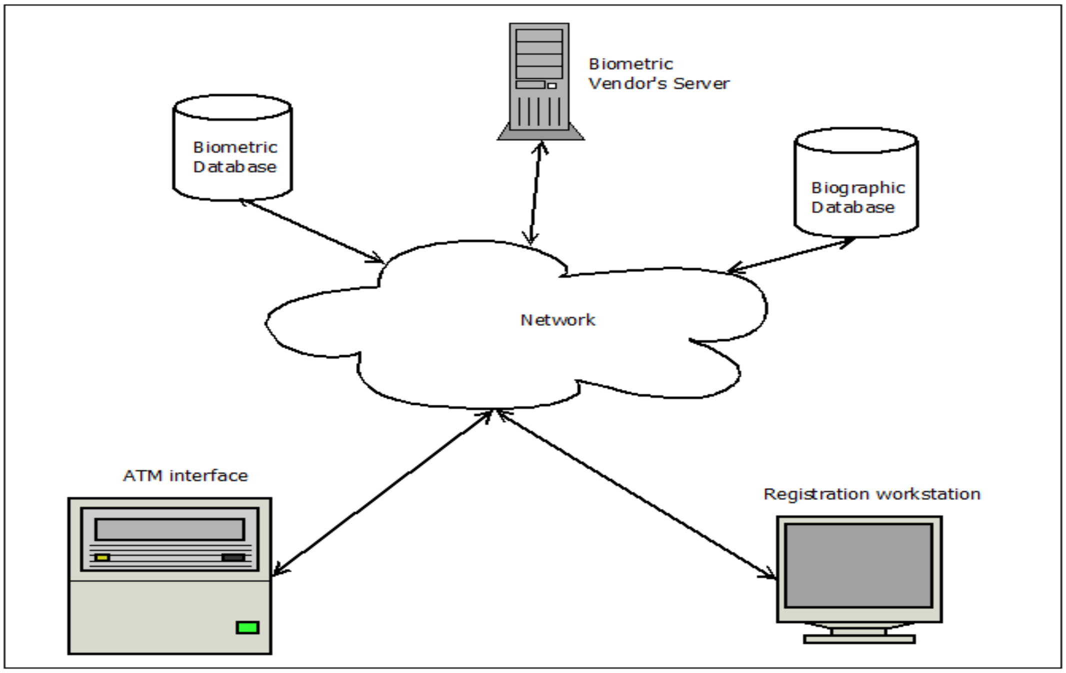

Fig. 1. Overview of Proposed System Design

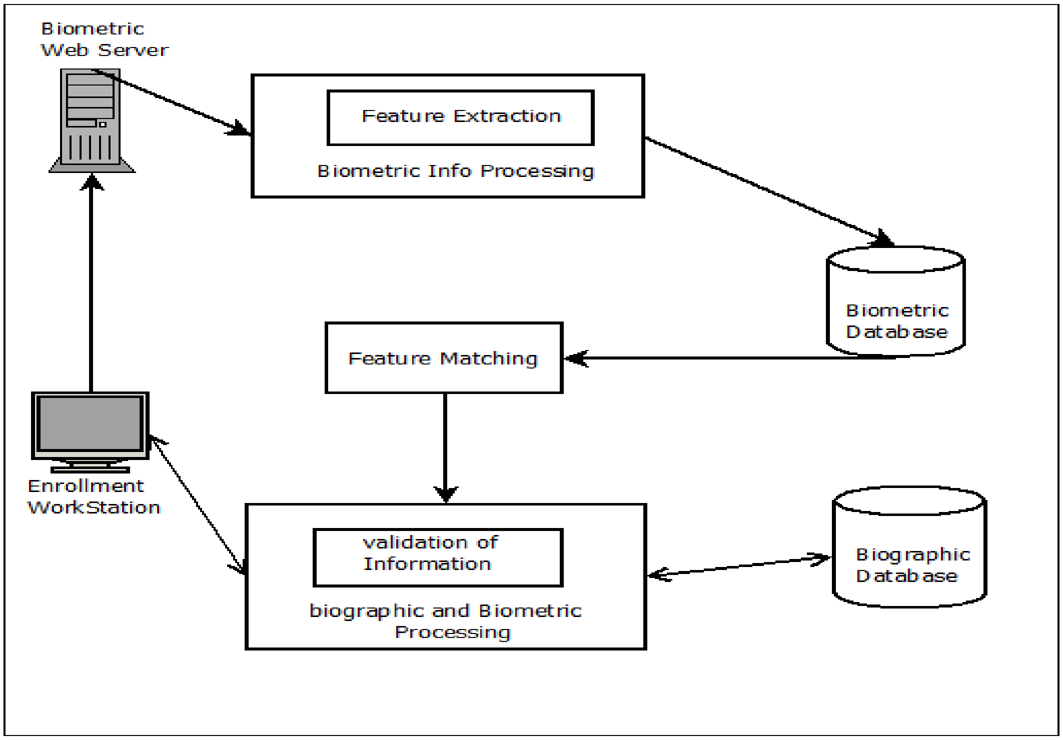

Fig. 2. Overview of the Registration Client Module

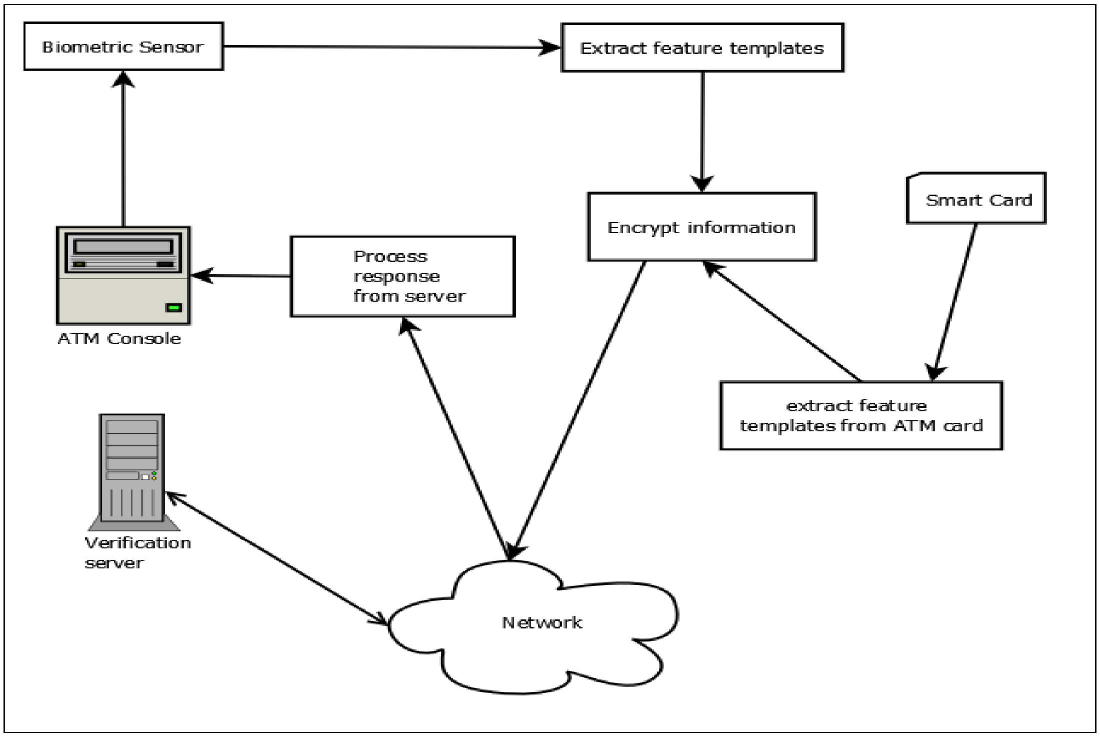
Biometric Sensor
Extract feature templates
Smart Card
Encrypt information
Process response from server
ATM Console
extract feature templates from ATM card
Verification server
Network

Fig. 3. Overview of an Online Biometric Authentication

C. Proposed System Operation

The proposed system will use smart cards with fingerprint validation instead of the usual PIN. The aim of this systemic approach is to address the defects that have been identified with current implementations of using PINs.

The system works as follows:

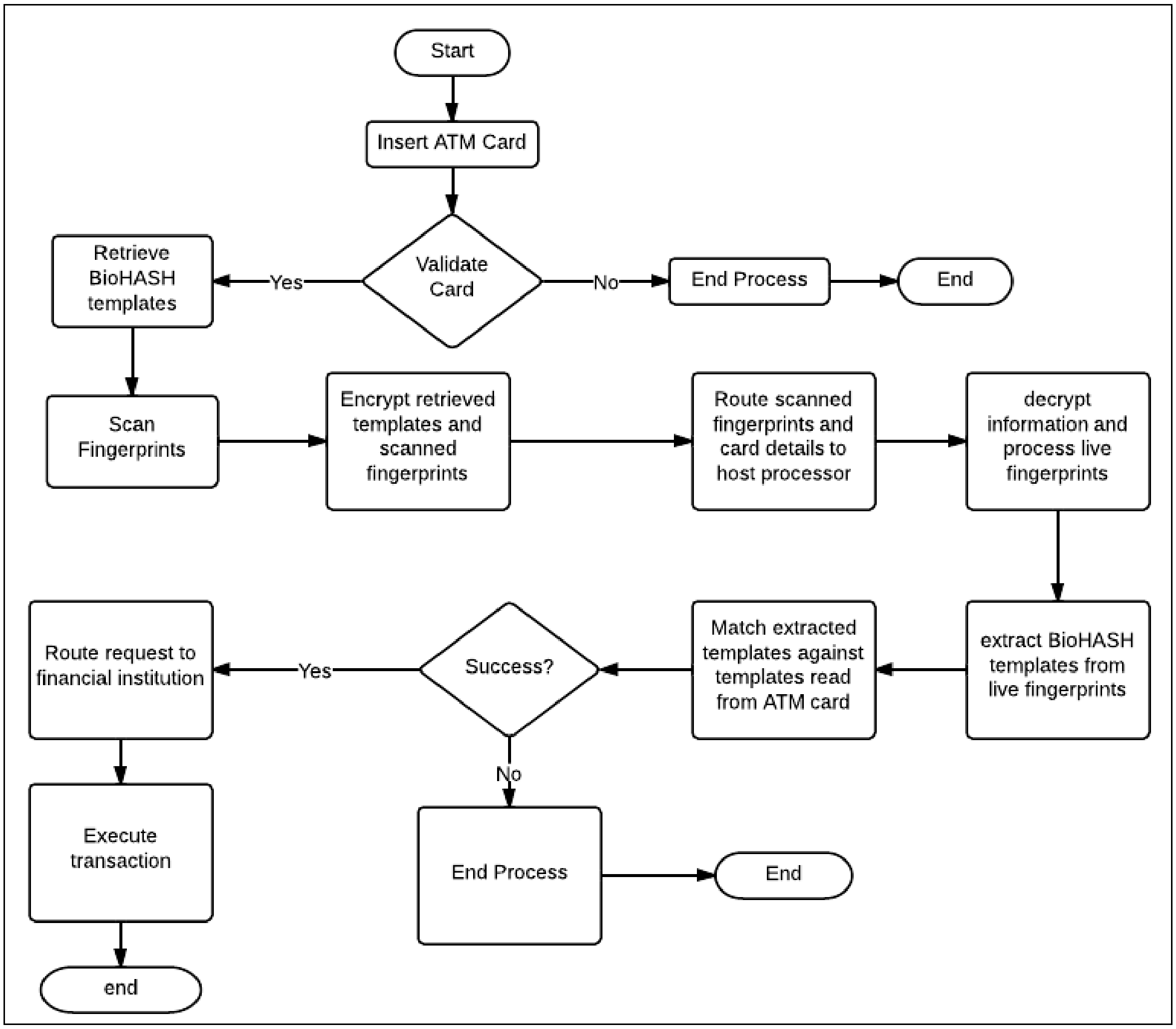
Start
Insert ATM Card
Validate Card
Yes
No
Retrieve BioHASH templates
End Process
End
Scan Fingerprints
Encrypt retrieved templates and scanned fingerprints
Route scanned fingerprints and card details to host processor
decrypt information and process live fingerprints
extract BioHASH templates from live fingerprints
Match extracted templates against templates read from ATM card
Success?
Yes
No
Route request to financial institution
Execute transaction
end
End Process
End

Fig. 4. System Flowchart of Online Off-card ATM Biometric Authentication

```
Algorithm 1:    System Flow of Online Off-card ATM Biometric Authentication
(1)  Insert card into ATM console.
(2)  ATM's processor validates card. Upon successful validation go to Step 4; failure validation go to Step 3.
(3)  ATM's processor ends process and ejects card.
(4)  ATM's processor retrieves information stored on the card.
(5)  Cardholder is prompted to scan his or her fingerprints.
(6)  Scanned fingerprints are encrypted.
(7)  Biometric information are retrieved from card and scanned fingerprints are transmitted to a host processor (verification server).
(8)  Verification server decrypts the information transmitted to it.
(9)  Verification server processes scanned "live" fingerprints and generate BioHASH templates from it.
(10) Server then matches the newly generated BioHASH templates against the BioHASH templates retrieved from the smart card (ATM card).
(11) Upon successful matching go to Step 13, otherwise a match failure means go to Step 12.
(12) Failure processing is reported back to ATM system and process is brought to an end.
(13) Verification server sends match success response to the concerned financial institution.
(14) The cardholder is then allowed to perform his or her financial transaction.
```

A cardholder inserts his or her card into an ATM console, the card is validated, and both biographic and biometric (BioHASH templates) details stored on that card are read. Once the information is read, the cardholder will be required to scan his or her fingerprints. After the scanning of the required fingerpints, the ATM's processor will encrypt the biometric details read from the card and the live fingerprints. This information is then transmitted to host processor (authentication server) via a secured network. At this point, the encrypted information is decrypted. The Verification server then processes the live fingerprints and generates BioHASH templates from them. The extracted templates are then matched against the BioHASH templates retrieved from the smart card.

Once matching is successful, the host processor (verification server) routes the client's request to the concerned financial institution or bank. The financial institution then validates that the supposed cardholder is allowed to successfully perform financial transactions.

Figure 4 illustrates the flow of activities of the proposed authentication system. The system seeks to make two changes to the current system of authentication on ATMs. The first change it seeks to make is to replace the use of a PIN with the use of a fingerprint scan. The second change is to drift away from authentication using a database of biometric information to authenticating users using biometric details that have been captured and written to their ATM cards. The functionality of the proposed system is explained by the steps outlined below (*Algorithm 1*):

V. Propositions of Biometric Fingerprint Methodology Framework

The authors' adoption of this proposed solution offers a number of advantages over previous and existing approaches, as well as offering an efficient and security-aware solution for current ATM transaction processing. The authors explain below the propositions of merits for the novel methodology of biometric fingerprint authentication.

1) Flexibility: The proposed system offered a more flexible design where the user does not need to apply a PIN code alongside using the biometric fingerprint. Moreover, all the biometric and biographic information are stored on the smart card. This enables easy transaction on ATM consoles and the cardholder does not need to remember PINs and passwords. This functionality is a major advantage over previous approaches where a card holder combines a PIN code alongside his biometric fingerprint for transaction authentication.

2) Scalability: Scalability is a major concern when developing web applications. In this regard, the proposed system offered architectural design and interfaces where multiple authentications and transactions are performed concurrently with less data flow traffic. Here, the user access at any point in time could range even to a 1000 persons. Additionally, the platform supports the design of related scalable applications. In comparison to other approaches, these systems rather use desktop applications which limit concurrency usage of the application and/or builds up communication traffic during transaction authentication and processing.

3) Fast User Authentication: The proposed system design enables an authentication process that is more efficient and fast enough, in comparison to existing system approaches. This functionality is achieved because of the transfer of smaller file sizes of BioHASH templates over communication networks. Additionally, the matching procedures of the "live" and pre-stored BioHASH templates are easily adjudicated because biometric database needs to validate if tokens from both templates are the same. There is no need to do a match among a lot of pre-stored biometric data, with a resultant effect of high false reject errors. Comparing the use of BioHASH templates to other approaches, this functionality is a major merit. Firstly, the procedures do not require the transfer of the entire biometric data, but rather the template tokens; which are much smaller in file sizes. Secondly, there is no need to match pre-stored biometric templates.

4) Privacy Preservation: The privacy of account holders and their transactions are ensured in this proposed system. This is achieved because of the feature of both the encrypted biometric and biographic information of account holders are stored on the smart card; leaving only encrypted token BioHASH templates on the vendor's biometric database. This feature is quite beneficial because no biometric and biographic data is stored anywhere, whether on the vendor's database.

5) Efficient Security: The system that was designed offered a better and a more efficient system of authentication than the existing systems. The use of BioHASH templates ensures an irreversible cryptographic hash function, and also ensures that the original biometric are discarded as soon as the BioHASH value is derived. This means that the scanned biometrics are never stored or used in the matching process. Since matching is not done against templates stored in a database but rather against the BioHASH templates read from the ATM card, the rate of occurrence for both false acceptance and false rejections are drastically reduced. This makes the system more efficient and more secured. Furthermore, this system prevents the cloning of ATM cards which are prevalent with other approaches.

VI. Implementation and Evaluation

In this section, the authors discuss the implementation, testing, and evaluation work based on the proposed system methodology. The authors present the implementation framework and the procedures, and they discuss and analyze the evaluation results.

A. Implementation

The authors describe the implementation framework of various techniques and processes needed in delivering a secured system of ATM transaction processing. This sub-section focuses on the experimental setup and database design, the development environment deployed, the implementation testing applied, as well as the varied evaluations assessments to ascertain the efficiency of the proposed ATM transaction authentication methodology addressed in Sections III.B, IV.A, IV.B, and IV.C.

1) Experimental Setup and Database Design: The authors implemented the design using various sub-modules as part of system development; namely, Registration Client, De-duplication Server, and Set of Databases (Biographic and Biometric). The Registration Client is made of the following components;

- User Interface;
- Various Entities (Classes);
- Adjudication Client;

- Card Generation Client.

The Registration Client is supported by the Biographic database. There is the biometric de-duplication server and the biometric database used in storing generated BioHASH templates. The database was implemented using 2 different databases; as follows; Biographic, Biometric. The Biographic database is used solely by the registration module to store the biographic and account details of a particular account cardholder. The Biometric database is used by the third party biometric provider to store the biometric data for the customers of the bank.

2) Programming and Code Generation: The Registration Client's interface was developed as User Interface Form. Entities, such as, Staff, Customers, Branches, Account, AccountTypes had individual user interface forms that were designed to either create or edit them. Moreover, classes were developed to handle the business logic of each of the entities listed above. The classes created were used for basic operations like retrieval of Customer, Branch and Account information. The classes developed also handled the insertion of new records into the respective database tables; as well as deleting and updating of information concerning the various entities. A data access class was also created to handle connections to the database. In summary, 9,978 lines of code were written for the entity classes in support of the business logic of the system. In coding the User Interfaces, 8,526 lines of code were written. The de-duplication request and response classes were made up of 10,132 lines of code.

3) Integrated Development Environment (IDE): Microsoft Visual Studio was used to develop stand-alone, web applications, web sites and web services. The programming languages used was C#, which is well-integrated with the .NET platform.

4) Futronic Fingerprint Scanner and SDK: Futronic's FS80 USB 2.0 fingerprint scanner was chosen because of the extensive support it has for a number of platforms, such as, Windows and Linux. The device was also chosen because it has Software Development Kit (SDK) support for both Java and .NET platforms. Futronic fingerprint scanners are very durable and they also use advanced CMOS sensor technology which helps in delivering very high quality fingerprint images. Additionally, they are very fast in capturing fingerprint images.

5) Card Printer: Zebra ZXP series 1 card printer was used as the ideal printer for the proposed system. The card printer provides high quality card printing.

6) Smart Card Reader/Writer: The proposed system is fitted with a smart card reader and writer, for the dual usage of the card envisioned (to be used by both ATMs and POS devices). A supposed reader/writer should read both contactless smart cards, and virtually any other type of smart card. For this purpose, the OMNIKEY 5321 Smart Card Reader/Writer was chosen. This reader/writer offers a dual interface that allows for the use of both contactless and contact smart cards.

B. System Testing

The authors performed a number of tests to ascertain the effectiveness and efficiency of the system that was developed. The authors explain below these set of tests for the modules adopted in the system methodology.

1) Unit and System Testing: This form of testing was done in 3 stages; the first stage of testing focused on each of the entities. In this regard, unit test were written to validate the data that were captured for entities, such as, Staff and Customers. The second stage focused on testing the Registration Client independently; the test involved the entire information flow of creating and editing the details of the various entities. The reason for this is to ensure that there is a seamless information flow from one point in the Registration Client to another. The last stage of testing focused on the interaction between the REST server and the registration module. This test also included the card generation and printing.

2) User Interface Testing: The testing procedure on the User Interface for the Registration Client was done in 2 ways. These tests involved the design of the User Interfaces. The first process involved the Cognitive Walkthrough approach. Users were given a series of tasks to perform on the Registration Client, and the feedbacks collated were used to further refine the design of the User Interface. The second process adopted identified inconsistencies in the design of the User Interface. This test focused on the appearance of the Interface and not its functionality. This test focused on the font sizes used, colour, terminologies and layout.

3) Registration Client Testing: The Registration Client was also tested using the Cognitive Walkthrough approach. These tests involved the enrolment procedures that have to be followed in registering a Customer. Users were given the task to enrol a Customer, the feedback received from them during each stage of the enrolment were later used to refine the design and functionality of the Registration Client.

C. Evaluation

The authors assessed the functionalities of the proposed system based on various metrics and discussed the merits over previous system approaches. Moreover, the authors quantitatively analyzed the set of procedures (and sub-procedures) involved in the overall system framework and methodology.

The authors present below in TABLE I. the average response time for the set of procedures in the overall system framework and methodology. Here, the authors analyze the procedures of acquisition of fingerprint using the scanner, completion of the enrolment process for registration, and the online off-card verification during a cardholder transaction authentication. The collation of response times were based on 10 successive attempts of careful system testing for each of the sub-procedures per each procedure.

VII. Comparison to Other Approaches

There have been a few literature and studies in the area of biometric fingerprint authentication on ATM systems. Though the studies explain varied methodologies and techniques and present significant contributions, some pertinent problems are not addressed in-depthly or still unresolved. In this section, the authors discuss these approaches and comparatively explain how the proposed methodology performs better.

A. Biometric ATM Authentication against Central Database (Tokenless Authentication)

This form of biometric authentication does not require the use of an ATM card (Token). This system is currently being implemented in rural areas in India [12]. The system requires access to a central biometric database in performing as part of identification or verification. Access to a central database during an authentication process can be quite slow depending of the number of templates stored on the database.

TABLE I. Quantitative Summary of Average Response Time for System Procedures

Procedure	**Average Response Time (s)**	**Sub-procedure**	**Average Response Time (s)**	**Comment**
Acquisition of Fingerprint using Scanner	32.40	Not Applicable	Not Applicable	The adopted fingerprint scanner (Futronic FS80 USB 2.0) can only scan a single finger at a point in time. An ideal scanner, a Slap Fingerprint Scanner, will scan 4 fingers at the same time and that will appreciably reduce the response time.
Completion of Enrolment Process	380.00	Capture Biographic Information	150.000	The Enrolment process involves the capturing of both biometric (Fingerprints and Photograph) and biographic data. The time taken to complete this process is influence by the typing speed, the ease of taking the applicant's photograph, the fingerprint acquisition process, the network latency, and database performance.
		Capture Biometric Information (Photograph)	78.000	
		Capture Biometric Information (Fingerprints)	120.000	
		Biometric De-duplication Process	132.000	
Online Off-card Verification	5.55	Capture "Live" Fingerprint	3.200	This procedure generally affected by network latency from the ATM console to the vendor's (biometric) database. Furthermore, the matching process is impacted upon by the efficiency and speed in information processing on the vendor's database.
		Read Biometric Information from Smart card	0.800	
		Extract Template from "Live" Fingerprints	0.500	
		Matching of Templates	0.045	
		Recording of Response and Request	1.000	

A database read could become the bottle neck in the system and this might lead to a large number of people abandoning the use of biometric ATMs.

Moreover, the use of a central database means that authentication at the ATMs can only be done for people who have their biometric information stored on the central database that is being access by the ATM. This makes it impracticable for a cardholder to perform transactions on ATMs owned by different financial institution even if they are using the same biometric vendors as the parent institution of the cardholder. This is mainly because their ATMs will most likely connect to a different biometric repository. The benefit of this system is that it reduces the cost of having to issue ATM cards and other related costs. *Figure 5* illustrates a general architecture of the system. The major drawback of this system of authentication is that, matching the biometric details an account holder against a large database of biometric details can lead to high false reject errors [13].

B. Biometric ATM Authentication Using GSM Modem

Daula and Murthy (2012) [9] in their work identified some flaws with the traditional ATM systems authentication. They introduce a solution that was aimed at addressing the flaws in the traditional system. *Figure 6* illustrates an overview of the system flow of their solution. The system flowchart only depicts how a User interacts with their solution and ignores the interactions of a system administrator. The system requires the cellular (mobile) number and fingerprint of an account holder. The account holder scans his or her fingerprint at the ATM. These fingerprints are authenticated and an Short Messaging Service (SMS) with a password is sent to the mobile phone of the account holder. The account holder is then required to enter the password sent, via SMS, to him or her to complete the authentication process.

The system explained above has major technical flaws, as discussed below:

- The system relies on the safe and timely delivery of an SMS that contains a password to be used for the final step of validation at the ATM. The major issue with this is that, SMS deliveries are not always reliable. It also means accountholders who do not have their mobile phone with them cannot perform financial transaction via the ATM.

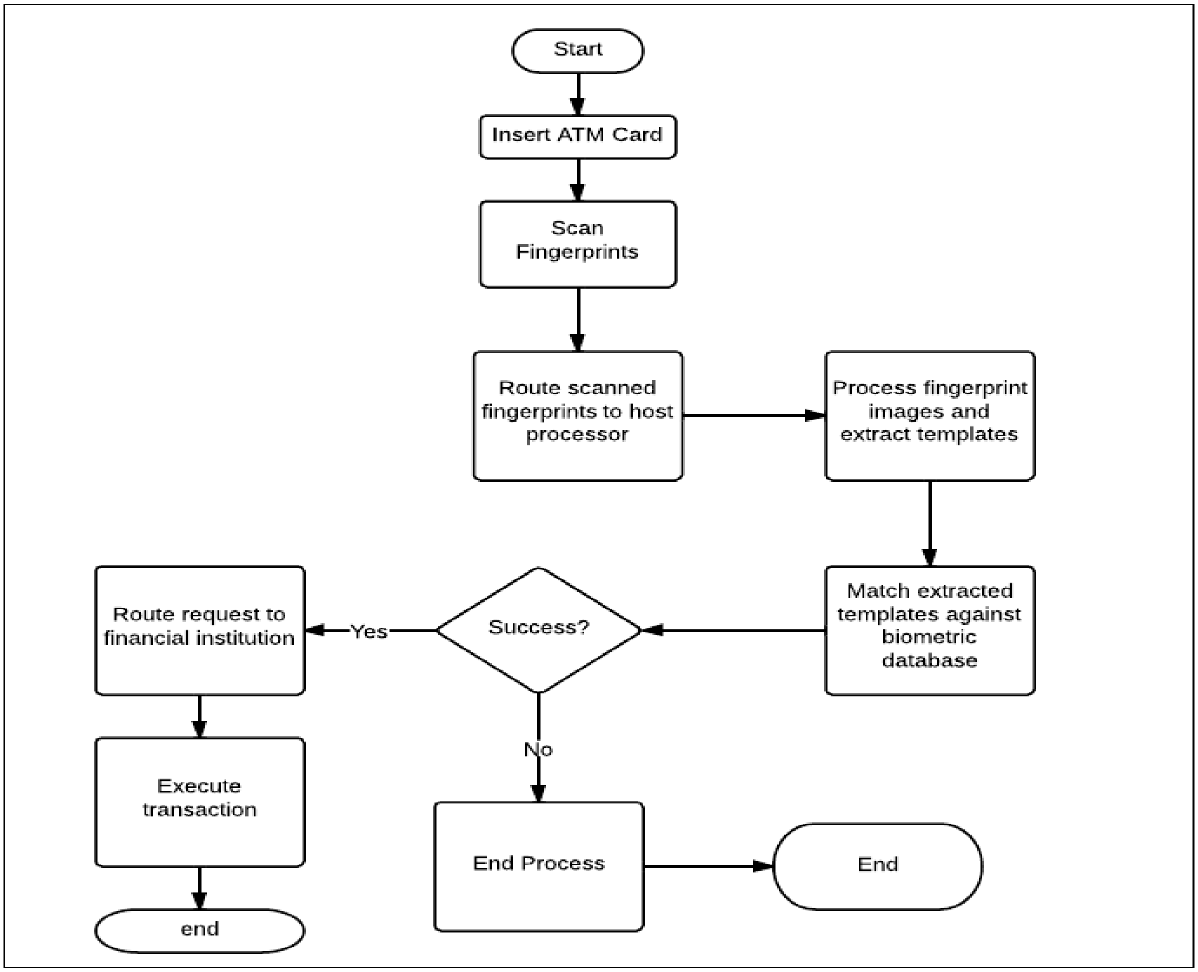
Start
Insert ATM Card
Scan Fingerprints
Route scanned fingerprints to host processor
Process fingerprint images and extract templates
Match extracted templates against biometric database
Success?
Yes
No
Route request to financial institution
Execute transaction
end
End Process
End

Fig. 5. Flowchart of Proposed System of Tokenless Biometric Authentication, Gelb and Decker (2011)

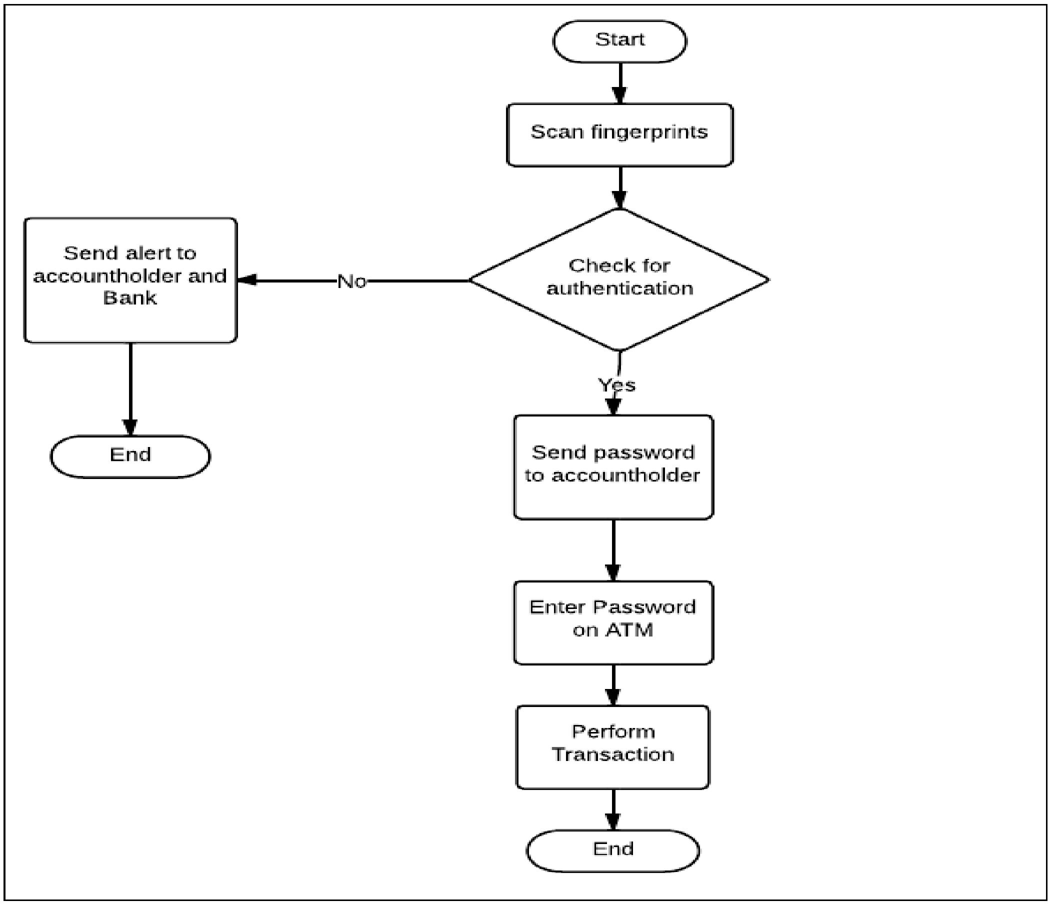

Fig. 6. Flowchart of Proposed System by Daula and Murthy (2012)

TABLE II. QUALITATIVE ANALYSIS OF PROPOSED METHODOLOGY AND OTHER APPROACHES

Methodology Approach / Analysis Criteria	**(1) Tokenless Biometric Authentication, Gelb and Decker (2011)**	**(2) Biometric Authentication using GSM, Daula and Murthy (2012)**	**(3) Proposed System**
Ease of Use	Requires just the use of fingerprints and is therefore very easily to use and reduces the burden of having to remember PINs.	Generally very easy to use and more common in system implementations. The major drawback with this system is the fact that PINs can be easily forgotten or misplaced.	Proposed system requires the use of an ATM card and the cardholder fingerprints. This system is also very easy to use. The system does not require a cardholder to remember PINs since his biometric information is used in the authentication process.
Security	Though more secured than the traditional system (2), the procedure can result in false acceptance error in cases where the number of records stored in the database is very high. This is because the identification of a user is done against a database of huge number of biometric records.	Presents a number of security concerns; ATM cards can easily be stolen and PINs are easily guessed. Additionally, some cardholders have a habit of sharing their PIN with family relatives and close friends; this reduces the security of the system.	The proposed system provides the security that comes with a biometric technology and also eliminates the likelihood of false acceptance. Hence, it only matches the cardholder's biometric information against the information stored on the ATM smart card.
Privacy	This system offers very little privacy in	This system offers more privacy to	The proposed system offers more

	terms of biometric information. The biometric information of the cardholder is stored in a database which is accessed during the point of verification.	the cardholder in terms of biometric information; this is because the system does not make use of biometrics.	privacy in terms of biometric information since the individual carries his biometric information on his ATM smart card.
Authentication Time	The tokenless system has a slow response time. This is because reading biometric information from a database and matching against each of the records being read can take some considerable amount of time.	The Traditional authentication system has a fast authentication time due to the nature of the information being transmitted to the host processor and the nature of the authentication being carried out.	The proposed system has a faster response time than the tokenless system. The system does not require access to a database and only matches the presented biometric information against the biometric information read from the ATM smart card. Furthermore, the response time compares just as equal as or better than the traditional system.
Cost	The tokenless system has a very high setup and implementation cost. There is no additional cost afterwards.	The traditional system has a low setup cost, but this cost could increase considerable when you take into account the cost of replacing missing or stolen card and the cost of generating new cards for users who have forgotten their PINs. This system could end up being a very costly approach.	Propose system has a high initial setup cost, if the cost of card maintenance is taken into consideration. This approach is more costly than the tokenless system but less costly than the traditional system; but the merits gained far outweighs cost considerations.

- Matching the biometric details an account holder against a large database of biometric details can lead to false reject errors [13].
- The system is quite slow when dealing with high capacity requirements [14].

C. Methodology Comparisons & Evaluation

The authors evaluated the proposed system in comparison to other approaches. The following criteria were used to analyze the performance of the proposed system; Ease of Use, Security, Privacy, Speed, and Cost. The authors present a tabular analysis of the methodology approaches in TABLE II. This analysis summarizes the discussions regarding methodology approaches presented in the literature, and outlines the merits of the proposed methodology over the other approaches.

VIII. Conclusion

This paper presents a design framework for the secure authentication of biometric fingerprint on ATM systems. The authors addressed the methodology that employs the use of BioHASH templates ensures an irreversible cryptographic hash function, facilitates a faster authentication, and enables an efficient framework of detecting potential duplicates of banking account holders.

The proposed framework architecture is modelled such that biometric fingerprint information of an account cardholder is captured and BioHASH tokens are generated, as a result. These tokens are then written onto the microchip of a smart (debit) card, with the biometric information discarded afterwards. At the point of ATM transaction authentication, the pre-stored BioHASH tokens on the smart card are matched against the “live” fingerprint tokens to determine legitimacy and subsequent accessibility for the supposed account holder.

The authors compared the framework methodology against other approaches and outlined the merits and suitability of their approach for delivering a robust, fast, and efficient authentication procedure on ATM systems. The following were the merits that the framework architecture discussed in this paper offers over the current systems of ATM transaction authentications; flexibility, scalability, fast user authentication, privacy preservation, and efficient security.

The analyses of the evaluation showed that the average response times of each of the procedures (and their sub-procedures) were appreciably small. These procedures were acquisition of fingerprint using scanner, completion of enrolment process, and online off-card verification. The authors’ assessment indicated some areas in the design and implementation that needed improvements. For example, the adoption of a slap fingerprint scanner to increase efficiency and reduce the response time during the capturing of biometric fingerprints.

The authors’ approach, thus, provides practitioners and researchers in the industry of biometric technology with methodology, procedures, and exact measures as to how successful an authentication process on an ATM system is achieved.

One critical area of future research is the implementation and testing of all the major components of this prototype design with a financial institution on a commercial scale. This will expose the design to all the practical technicalities in line with commercial use. The authors also envisage the drift of development from a standalone application system to a web application system using the Model View Controller (MVC) approach.

References

[1] R. Silberglitt, P. S. Antón, D. R. Howell, and A. Wong, "The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications," Technical Report, [Online]. Available: http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR303.pdf, 2006, Retrieved: 29-10-2015.

[2] D. Hutchinson and M. Warren, "Security for Internet Banking: A Framework. Logistics Information Management," vol. 16, issue 1, pp. 64-73, 2003, ISSN: 0957-6053. DOI: http://dx.doi.org/10.1108/09576050310453750

[3] P. Magutu, M. Mwangi, R. Nyaoga, G. Ondimu, M. Kagu, K. Mutai, H. Kilonzo and P. Nthenya, "E-Commerce Products and Services in the Banking Industry: The Adoption and Usage in Commercial Banks in Kenya," Journal of Electronic Banking Systems, vol. 2011, article ID: 678961, 19 pages, 2011, DOI: 10.5171/2011.678961.

[4] L. Bradley and K. Stewart, "A Delphi Study of Internet banking," Marketing Intelligence & Planning, vol. 21, no. 5, pp. 272-281, 2003.

DOI: http://dx.doi.org/10.1108/02634500310490229

[5] S. Venkatraman and I. Delpachitra, "Biometrics in Banking Security: A Case Study," Information Management & Computer Security, vol. 16, no. 4, pp. 415-430, 2008. DOI: http://dx.doi.org/10.1108/09685220810908813

[6] B. Scholnick, N. Massoud, A. Saunders, S. Carbo-Valverde and F. Rodriguez-Fernandez, "The Economics of Credit Cards, Debit Cards and ATMs: A Survey and Some New Evidence," Journal of Banking & Finance, vol. 32, no. 8, pp. 1468-1483, 2008.

[7] S. Oko and J. Oruh, "Enhanced ATM Security System using Biometrics," International Journal of Computer Science (IJCSI) Issues, vol. 9, issue 5, no. 3, September 2012. ISSN (Online): 1694-0814.

[8] M. O. Onyesolu and I. M. Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 3, no. 4, pp. 68-72, 2012.

[9] S. Daula and D. Murthy, "An Embedded ATM Security Design using ARM Processor with Fingerprint Recognition and GSM," International Journal of Advanced and Innovative Research (IJAIR), vol. 1, issue 2, July 2012. ISSN: 2278-7844.

[10] S. Biswas, A. B. Roy, K. Ghosh, and N. Dey, "A Biometric Authentication Based Secured ATM Banking System," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 2, issue 4, April 2012. ISSN: 2277 128X.

[11] F. S. Hossain, A. Nawaz, and K. Md. Grihan, "Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor," International Journal of Information and Computer Science (IJICS), vol. 2, issue 4, May 2013. ISSN Online: 2161-5381.

[12] A. Gelb and C. Decker, Cash at Your Fingertips: Biometric Technology for Transfers in Developing and Resource-Rich Countries, Center for Global Development, Working Paper 253, 2011.

[13] G. A. von Graevenitz, "Biometric Authentication in Relation to Payment Systems and ATMs," Datenschutz und Datensicherheit - DuD, vol. 31, issue 9, pp. 681-683, September 2007. Online ISSN: 1862-2607. DOI: 10.1007/s11623-007-0223-9.

[14] A. Jaiswal and M. Bartere, "Enhancing ATM Security Using Fingerprint and GSM Technology," International Journal of Computing Science and Mobile Computing (IJCSM), vol. 3, issue 4, April 2014.