A Qualitative Study on Adoption of Biometrics Technologies: Canadian Banking Industry

Inkingi Fred Gatali
Bishop's University
2600 College Street
Lenoxville, QC, Canada
1-819-822-9600
IGATALI14@UBishops.ca

Kyung Young Lee
Dalhousie University
6299 South St
Halifax, NS, Canada,
1-514-265-0827
Kyungyoung.lee@gmail.com

Sang Un Park
Kyonggi University
154-42 Gwanggyosan-Ro
Yeongtong, Suwon, Korea
82-31-249-9459
supark@kgu.ac.kr

Juyoung Kang
Ajou University
206 Worldcup-ro
Yeongtong, Suwon, Korea
82-31-219-2910
jykang@ajou.ac.kr

ABSTRACT

This study examines the adoption of biometrics technology in the Canadian banking industry. By comparing Canadian banks with the financial institutions in other countries in terms of their adoption to biometrics, it explores current status of adoption to biometrics technology by Canadian banks and the potential future consequences as a result of their delayed adoption. Through literature review, this study first provides various aspects of biometrics technologies; technical specifications, performance metrics, types, current applications, and some issues and concerns with this technology. Second, it discusses current and future potential applications of biometrics in the banking industry. Then, the study provides a context with which to analyze the extent of the popularity and practicality of the technology in Canadian banks. Finally, based on qualitative interviews with biometric researchers and professionals in Canada, this study reports the research findings with regards to the following four topics: 1) Integration and accessibility to biometrics, 2) Public opinion and concern, 3) Transition of technologies, and 4) Current accommodations for biometrics, followed by discussion of the contributions of this study.

CCS Concepts

Security and Privacy → Security services → Authentication → Biometrics

Keywords

Biometrics, FinTech, Canadian Banks, Fingerprint, Iris and Voice Recognition, Security, Privacy, and Authentication

1. INTRODUCTION

Biometrics technologies today have accelerated at an immense pace, from the world of business, to governance, and right at our fingertips. The biometrics industry is experiencing staggering change. What was once seen as a futuristic concept is here and now [11]. The market for biometric technologies globally was $14.9 Billion in 2015 with an expectation of reaching $41.5 billion by 2020, increasing at a compounded annual growth rate of 22.7% in the 5 preceding years, according to a BBC Research report [39]. Today, biometrics technology is used in governmental programs for citizen identification, in the healthcare industry for user authentication, and many others such as the automotive industry which uses voice recognition in its cars [31]. With the fast technological advancements in the automatization and storage of information, biometrics offer new avenues of information storage and classification [8].

Currently biometrics technologies are used for authentication and identification. They are used to access control of computer systems through face recognition software; for surveillance purposes such as the US department of Homeland security system that uses fingerprint recognition for border control, as well as face recognition software that automatically records face signatures in search of specific individuals [7].

In the banking industry, the applications of biometrics technology are now getting significant attention worldwide [2]. Especially with a growing number of FinTech (Finance Technology) services based on mobile apps and mobile payment systems, it is expected that biometrics authentication will become a major authentication technology for banking services within the next five years, replacing traditional ID and PIN based authentication [38]. Actually, some Canadian banks have recently made an effort of adopting biometrics through pilot projects, such as Royal Bank of Canada's voiceprint technologies (See details in section 4).

In the field of Information Systems (IS), the extant literature on biometrics in the banking industry has looked into several topics, such as the intrusiveness of the technology to privacy [9], the necessity of biometrics in the authentication methods for banking services [37], and users' adoption of biometrics [10]. While these research efforts by global researchers provide us with good knowledge on the practicality of biometric technology usage and benefits, little is known about the current and future use of biometric technology in the Canadian Banking industry.

The purpose of the study is, therefore, to identify and analyze biometric systems that could be applied in the Canadian banking industry and explore Canadian banks' motivations for applying these technologies. Thus, this study will address the following

ICEC '16, August 17 - 19, 2016, Suwon, Republic of Korea,

ACM 978-1-4503-4222-3/16/08…$15.00
DOI: http://dx.doi.org/10.1145/2971603.2971623

research questions; 1) What is the future of biometrics in the Canadian banking industry and what is known about or being adopted in practice so far? And 2) What are banks' motivations for applying the technology? Is it a trend or does it open opportunity for the introduction of more financial products?

In order to answer these research questions, we interviewed several experts in the field of biometrics in Canada such as research and development officers at Canadian banks, associates of Canadian biometrics companies, as well as Canadian journalists that have written on topics of biometrics. This study will contribute to the banking and IT industry in Canada by providing a more clear understanding of the future of security in the banking industry. Also, it discusses the potential benefits and effects of biometrics development in banks, which can advance the accessibility to information and security in all manners.

The remainder of this paper is structured as follows. The next section explains various technical aspects of biometrics technologies, which defines biometrics and its current uses in several industries, as well as specifically in the banking industry and more distinctly in Canada, followed by a brief literature review on biometrics in the IS discipline. Then, our research methodology is presented with a set of qualitative interview questions with key informants from biometrics industry in Canada. Finally we will present our research findings as well as the discussion of contributions of this study.

2. TECHNICAL ASPECTS OF BIOMETRICS TECHNOLOGIES

2.1 Technological Aspects of Biometrics

Biometrics refers to the technologies that measure and analyze human body characteristics such as DNA and fingerprints for authentication purposes [42]. From palm-vein authentication, to iris recognition systems to voice recognition systems, there's been development of biometrics to get rid of the more time consuming and less trustful securitization methods of password authentication. The use of biometrics in the Canadian Banking industry is still in its infancy in comparison to many nations in Asia, Europe or the US, as only recently banks have started creating and applying systems of authentication that are not 'written-password' protected. The idea of biometrics in the banking industry is a topic of special interest as it has the potential to change the industry as a whole.

2.1.1 Components of biometrics technologies

A typical biometric system is comprised of five integrated components: (1) A sensor is used to collect the data and convert the information to a digital format, (2) Signal processing algorithms perform quality control activities and develop the biometric template, (3) A data storage component which keeps information that new biometric templates will be compared, (4) A matching algorithm that compares the new biometric template to one or more templates kept in data storage, and (5) Finally, a decision process (either automated or human-assisted) which uses the results from the matching component to make a system-level decision." [25]

The first component is the Sensor which uses the data it collects to transform the data it receives into quantifiable information. The converted information requires a reader that can properly assess the information it receives for maximum quality retention [27]. This user interface has to be significantly accurate so as to provide clear minute distinctions of the data it is recording. The quality of the raw data that the sensor receives depends on the characteristics of the sensor that is used [27]. The sensor is imperative to a successful and rapid biometric system.

The second component is the Signal processing algorithm which takes data and conducts control activities on the quality to develop a template that can be integrated. This is the step that is used to confirm proper and sufficient data received. This component goes through quality assessment, segmentation, and enhancement. During quality assessment, the biometric data that is received is analyzed to determine its eligibility for continuous acceptance. If the data obtained is not sufficiently received, the system will either try to re-obtain the biometric raw data by the user or simply elicit an error message, indicating the insufficiency of the data, or it can alternatively provide alternate procedures, which are setup by the administrator of the system. In segmentation, the biometric data is isolated so as to block out any excess noise or factors that might hinder the system's ability to recognize and process the data. In the end is the enhancement algorithm which further enhances the biometric data and soothes out any additional discrepancies which might affect how the data is received. In the end of this component process, there should be a template which offers only the needed information that is essential for recognizing the person through the biometric data. At the time of recognition, the template is retrieved from the database and matched against the biometric data that is sampled from the user of the interface [27; 40].

The third component is the data storage which keeps all the information that had previously been stored and approved as a benchmark for comparison. The samples stored in the database are from the enrolment process. The data usually contains the biometric information along with more personal identity information such as the name, address or PIN and so forth. The database can be either centralized in one location or decentralized in several locations [17].

The fourth component is the matching algorithm which takes the newly added information template and compares it to the templates already stored in the database. The matching algorithm uses match scores as an indicator of the similarities or dissimilarities between the samples stored in the database and those that are newly acquired. A large match score indicates a large similarity between the stored data and the new sample. Each system usually has its own guidelines and restraints that determine at what match score a sample can be considered a sufficient match for the stored data [27].

In identification, the biometric input is compared with all biometric data and information in the database and the system will present the template with which the input has the highest similarities or it will conversely show that the information it has received has not matched with any template within the system.

The fifth component is the decision process which uses the results from the matching component and makes a decision to give access or to deny access.

2.1.2 Technical specifications

An effective biometrics system is supposed to present characteristics that have: universality, uniqueness, permanence, collectability, performance, and acceptability, listed in table 1 [30].

2.1.3 Performance metrics of biometrics

For biometrics technologies to work, they are based on essentials that calculate the error and accuracy rates which determine the authenticity of the information or biometrics that the systems receive. These accuracy and rejection rates are classified into False Rejection rate (FRR), false acceptance rate (FAR), and Equal Error Rate (ERR).

The FRR is seen as the probability the system may not grant access to an authorized person. This would be due to the system failing to correctly identify the received biometrics with a template in the system.

The FAR is the probability that the system grants access to an unauthorized person. This would occur if the system incorrectly matches the given biometrics and the available templates. These are the circumstances at which fraud may occur [50].

The ERR measures the rate or proportion at which the false acceptance rate and the false rejection rate are equal. It calculates the correlation and indicates performance of the biometric systems through cross charting the relationship between the FAR and FRR. The lower the equal error rate value, the higher the accuracy of the biometric system [32].

2.2 Types of Biometrics

Biometrics can be used in several forms such as fingerprint verification, face recognition, hand geometry based verification, keystroke dynamics based authentication, and so on. The most used methods are fingerprint, iris recognition, and voice recognition. These are the most famously used because they offer better consistency in terms of creating a universal way of analyzing and using them for each individual. They are also the most practical when applied to the banking industry. Here is a brief analysis of voice and iris recognition programs and their difference between the well-known biometrics of fingerprint scanning.

2.2.1 Voice Recognition

Voice recognition allows the user to use his/her voice as an input device. It is not relatively new technology however the accuracy and applications of voice recognition have substantially increased over the last decade [16].

In older voice recognition software, the voice of a user used to be used only for commands or to dictate texts over the computer such as opening the browser or opening applications through some sort of one-word command. In new voice recognition software, a user can use their voice at normal speaking levels and the algorithm will recognize speech patterns and perform commands at a continuous and fast rate [16].

Voice recognition software remembers the way a person says each word and recognizes that as the platform at which to comprehend your speaking style for better recognition. This allows for a creation of a database of words without the effort of recording each word in the dictionary, individually [44].

2.2.2 Iris Recognition

It has been found that there are individual differences in the iris of humans. Therefore, it has become a method that is used for personal identification. Iris scan biometrics uses these characteristics of the iris to create individual identity. To scan the iris, a camera is maintained that uses infrared imagery to illuminate the eye and capture very high resolution photographs. The process takes less than two seconds, in which it can provide the details of the iris and store it into a database that can be used in the future for access using the same technology [19]. What makes this technology advanced is that eyeglass wear or lenses do not deter it from capturing a consistent image as the camera adjusts to the changes in pupil size. Irises are good indicators because, unless eye damage occurs, irises remain the same throughout a person's life. The uniqueness of the iris resides from the fact that it can contain over 200 unique identification spots and that no individual's left or right eye is the same, meaning that it creates a platform which makes it hard for false matching or fraud [16]. The False acceptance rate is about 1 in 1.2 million which is statistically better than the fingerprint recognition [26].

Table 1. The characteristics of biometrics system [30]

Characteristic/ Parameter	**Definition**
Universality	Able to be applied to the most or all targeted population
Uniqueness	Ability to recognize differences within the biometric data
Permanence	Data remains the same over a period of time
Collectability	Collection of data into database for future comparison
Performance	Shows accuracy and how well the system can perform
Acceptability	The use of system in capable and accepted industries

2.3 Applications of Biometrics in General

Several applications of biometrics are currently employed to many different industries in other countries in the world. Processes such as fingerprint scanning have been used for several years to create databases of information since the automatization and mass collection of data.

In the 21st century, biometrics are used from the government-sanctioned fingerprint technologies to create a database matching a person to their fingerprint all the way to private buildings that require fingerprint scanning to access their facilities [43]. The application is growing steadily and will keep on growing.

As people accumulate more and more personal data and application power on their portable smart devices, it drives the need for more security and distinguishability, which can result in more personalization. Right now, biometrics technology has been applied to smartphones through the use of fingerprint as security to access applications and personal data stored on the phone, such as the iPhone 6 and Samsung Galaxy 6.

In the healthcare industry, patient identity and the protection of patient data are used as it helps counter Medicare fraud and the use of personal information for payments. In Australia's healthcare industry, Salmat's VeSecure Technology uses voice biometrics to create a distinct voice identifier [22]. When customers call the major insurer such as AHM, the distinct voice identifier is used to confirm the identity of the insured person.

Today, biometrics technologies have been applied in many national identification programs. For example with India's project Aadhaar which is already the largest Biometric database in the world. The Indian government started a program in 2010, called Aadhaar, which registers a unique identity based on biometrics [20]. This program, through bills passed in parliament, contains biometric identifiers in the millions, from urban to rural, that has been approved for implementation within the banking sector which can later create access to mobile phone banking services [22]. The goal of the Aadhaar program is the secure categorization of biometrics data through fingerprint, iris scanning, photos and demographic data for each one of the 1.25 billion residents. The program currently has 550 million residents as of 2013 and aims to have everyone catalogued in the coming years [35]. Other national biometrics programs have been implemented even in lesser developed nations such as Rwanda, which stores the fingerprint data of its citizens for easier and faster border crossing and receipt of governmental services [12].

In the mobile industry we have seen that mobile devices such as the new Samsung S5 and S6 series as well as the iPhone 5s and 6 series contain fingerprint scanners as a method of securitization of the mobile devices and the mobile payment solutions. The implementation of these biometric technologies on the devices shows the popularity that biometrics is gaining. Other computing companies such as Microsoft, Sony or HP have also released several devices that have used biometrics such as Microsoft's X-box One which includes use of voice recognition or facial recognition in order to gain access to the console.

In the automotive industry, with the increased availability of fingerprint scanning technologies, the cost of applying them has significantly decreased. Automakers such as Mercedes have implemented finger scanning in the S-Class model as a form of starting the car through fingerprint scanning the owner of the vehicle [21].

As such, biometrics technologies have been applied in computing devices, healthcare, and automotive industries, as well as public sectors (E.g., government security systems.)

2.4 Benefits of Biometrics Data Security

The use of biometrics as replacement technology for current technologies applied to security can have beneficial effects in maintaining security and decreasing operational costs and losses [26]. Also, the more the technology is being used, the cheaper it becomes in the long term to implement it. Biometrics that are much more developed, such as fingerprint scanning have hit global levels [48], and biometrics technologies are being put in financial organizations such as commercial banks and investment banks [34]. The need for passwords and PINS become obsolete as one's own biological makeup acts as passkeys and passwords. This makes our authentication particularly unique and discriminative which makes it almost impossible to duplicate. This creates efficiency as it limits the need for external processes of identification. With development, we can soon apply behavioral biometrics which can for example figure out the way we behave as a signatory for our checks and so forth.

In every type of biometric security verification, the fingerprint is used heavily. It is still playing most important roles in biometric security system. When the user's or approved person's fingerprint is entered into the security system, only he or she is able to access the computer or can proceed to a secure region. Biometric devices verify every time you try to enter. So, they are allowing only authorized people to proceed and hence reducing risk of fraud or breach of privacy.

There is also easier accessibility for customers who may not be as able bodied as the rest [29]. Written password can be replaced by iris recognition or voice recognition.

2.5 Applications of Biometrics in Banking Industry

2.5.1 Access to Personal Accounts

The need to have records and provision of several pathways to which a biometric can be applied is met with biometrics. Looking at biometrics with Western Bank in Puerto Rico, the bank managed to implement a multiple biometric system which caters to employees and customers. It allows employees and customers to gain access through finger-print scans in all branches of the bank throughout the country. In that way, employees use their fingerprint to gain access to their records and customers can gain quick access to their bank accounts [36].

2.5.2 Automate Teller Machines (ATMs)

Customers and banks have a possibility of benefiting through biometrics in ATMs which can allow better security and better efficiency. The use of biometrics in ATMs can be quicker functioning with users through finger-print scanning or even palm-vein recognition. BPS Bank in Poland was the first to initiate a biometric ATM in Europe, in 2010, by using finger-vein analysis. The system uses an infrared scanner to detect idiosyncratic micro-vein patterns below the skin of the tip of your fingers. Similar ATMs have, since, been deployed across the nation [23].

2.5.3 Mobile Talk Transactions

Through the use of voice recognition biometrics, customers would have the option of faster access to their accounts when dealing with bank representatives as authentication would be faster. In 2012, Barclays released a voice biometrics that allowed international customers' identities to be validated as they spoke with a customer representative. This resulted in an average of 20 seconds gain and the omission of the authentication process [4].

2.5.4 Internal Network Access

The internal network access aspects are largely pertaining to employees of the financial institutions and the integrity of the banks. Through creating systems such as BioSignature, it creates an audit trail of all employee transaction activity [33]. The system prevents insider fraud and increases accountability and employee productivity [47].

2.5.5 Smartphone Banking

Today, there is an estimated more than 50% penetration of smartphones globally according to Mobile Marketing Daily. Thus, smartphones are practical avenues for biometric application. Banks in South Africa such as Absa have already implemented smartphone biometric security through Apple's TouchID technology to reduce bank account access through stolen PINs or phones.

3. LITERATURE REVIEW ON THE ADOPTION OF BIOMETRICS IN BANKING INDUSTRY

We have reviewed the literature on the adoption of biometrics at the individual and the industry (national) level. While biometrics technologies have been implemented to various industries such as the aviation industry and immigration departments of governments for their key authentication purposes [1], the implementation of biometrics into end-users' banking services is still in its early stage worldwide. Therefore, although we can find recent news articles and blog posts on biometrics implementation [3; 5], there are not many empirical studies that investigate the adoption of biometrics technologies in banking services.

Among a dozen of articles that we reviewed on biometrics in the banking industry, only a handful of studies have been conducted with empirical data such as surveys or interviews. Those studies identified technological and behavioral factors that influence biometrics adoption. For example, Byun and Byun [10] found that the current and potential users of biometrics (fingerprint) technologies are highly concerned about information privacy risk in using fingerprint ATMs and also found that perceived enjoyment is the most salient factor that influences the adoption of fingerprint ATM. Also, Tassabehji and Kamala [45] found that users' perceived security with biometrics technology and self-efficacy in biometrics use are positively associated with users' intention to use biometrics in banking services. As such, users' security concern and the efficacy with the biometrics technology are found to be key factors for the adoption of biometrics at the individual level.

Also, other conceptual studies almost unanimously argued that non-technological issues are as important as technological factors. For example, Bustard [9] suggests that for successful biometrics implementation in the banking sector, the legislation for biometric system should cover the definition and protection of personal data, the storage of biometrics data, and justification for what is collected. Hassanein [24] argued that educational interventions should increase users' knowledge about biometrics and security. Then the technical knowledge about security and biometrics will help individuals perceive security threat and benefits of biometrics, which will eventually influence intention to use banking services (ATM) equipped with biometrics. Finally, Venkatraman and Delpachitra [49] argued that in order to successfully implement biometrics in the banking industry, the service providers should address not only technological issues but also other issues such as users' privacy fears, human tolerance levels, organizational change and legal issues.

To summarize, the literature on biometrics in banking industry suggests that for successful implementation of biometrics in banking, the banking services providers should address technical issues (i.e., making the technology easier or enjoyable to use) legal issues (e.g., privacy laws and regulations), end-user education (in terms of privacy concern and security threats), and institutional processes [37; 46].

4. CANADIAN BANKING INDUSTRY

Canada has fewer numbers of banks than other countries with similar population size. With the population of 36 million, the big six banks in Canada (Toronto Dominion, Royal Bank of Canada, Bank of Nova Scotia, Bank of Montreal, Canadian Imperial Bank of Commerce, and National Bank of Canada) control over 85% of domestic assets. If compared to US, the “Big 5” banks (JPMorgan Chase, Bank of America, Citigroup, Wells Fargo, and Goldman Sachs) in US control only 44 percent of financial assets in US [41]. The Canadian government and regulators are more involved in almost everything that banks do. Also, Canadian banks are generally conservative in terms of risk-taking in asset management, as well as technological advancement. Due to the small number of major banks and highly involved governmental authority, Canadian banks are highly coordinated among one another, as well as with regulators [41].

When it comes to end user authentication process, in 2015 Canadian Bankers Association released the Payment Security White Paper, which expressed concern about banks losing their control over customer authentication processes in mobile devices which eventually influenced recent regulations on mobile banking. These regulations, although details are not the key scope of this study, actually provided a more level playing field between the banks and new market entries like telecom companies Apple, Google, and Paypal. In sum, the Canadian banking industry is composed of a few key members, coordinated among one another and highly regulated with governmental authority [41].

Under this industrial circumstance, nevertheless, some Canadian banks have taken a beginner stride in the markets of biometrics through pilot projects. For Example, Royal Bank of Canada (RBC) became the first Canadian company to implement technology to identify clients' ‘voiceprint’ [6]. The program, called RBC Secure Voice, requires that an individual enrolls in the service, to which their voice print is captured through individual characteristics then encrypted and stored on RBC's secure server for future use [6]. TD Waterhouse also unveiled a voice biometric that identifies customers for easier telephone banking [51]. Tangerine (ING Direct Bank Canada), a division of Scotiabank, released biometric specifications for its mobile banking application which includes a fingerprint scanner that supplants old-fashioned passwords [28].

5. RESEARCH METHODOLOGY

The purpose of the study is to gain a deeper understanding into the use of biometrics as a form of security within the Canadian banking industry. Based on extant literature on biometrics, the first author initially generated a draft of interview questions that address the acceptance of biometrics, the transitioning effects as well as a legislation aspect, which would help determine the need for the application of biometrics within the industry. Then, it was revised with an academic expert. The revised questionnaire is composed of 9 questions (presented in the section 6. Results) that can be grouped into 4 categories, namely 1) Integration and accessibility, 2) Public opinion and concern, 3) Transition of technologies, and 4) Current accommodations for biometrics in Canada. Operational definitions of these four categories are presented as follows:

- *Integration and Accessibility*: The ease of which integration of biometrics technology can be achieved into the Canadian banking sector.
- *Public Opinion and Concern*: Public concerns on the hold of large personal biometrics databases by large corporations (corporate trust issues)
- *Timing of Application*: The rapidity of applying the biometrics technology (local and global)
- *Current Accommodation*: The extent to which biometrics technology can be currently accommodated

We conducted interviews with key informants from the banking and biometrics industry in Canada. In order to find interviewees, we contacted about 20 industry experts, including Information Technology managers in banks, CEOs or executives in biometrics service providers, and technology journalists who are specialized in biometrics technologies. As a result, we were able to interview three key informants who provided us with sufficient knowledge on the current situation in terms of the adoption of biometrics in Canadian banking industry. The interviews lasted approximately 20 minutes with each one of the key informants.

6. RESULTS

The questionnaire is comprised of 9 questions. Although their original answers to each interview question are much longer, the responses of each question have been coded, summarized, and then reformulated to represent the opinions of the interviewees in a more clear fashion. The followings are, therefore, summarized answers for each one of questions.

1) What is your general opinion on the future of the security of banks? The Canadian banks are not ready or rather not willing to change their current culture just yet. There is more fraud today and more electronic commerce which creates the same problems of security but at an increasing rate. The industry recognizes the threats but instead there are increased budgets that are allocated to mitigate the losses.

2) Do you think the use of biometrics can be easily integrated into Canada and Canadian banks? Biometrics, especially when used in conjunction with other security applications may be one of the areas to provide some of the best security features for Canadian banks. It can be easily integrated and deployed, but it is a matter of authority in place needing to believe in the technology.

3) Apart from the use of biometrics for security purposes as well as easier accessibility to accounts, do you expect any other practical applications being used in banks via biometrics? The sector is looking at biometrics, not only for account-access and security, but also in processing transaction, and in the mobile space, with the integration of wearables. Fraud overall should always be the main culpability. There's focus on external fraud and credit and debit card losses, but there are also big problems internally. If there were biometric readers on every computer in a financial institution and every POS (points-of-sales) system, no one would be able to use or access accounts of others, which would remove fraud on that level.

4) How would you address the factors of concern of privacy in biometric technology? What is the right way to sway people into accepting biometrics? Legislation is indeed needed, but it is no greater than the need for legislation on handling all types of personal data. There is a double-edged sword, where biometrics data is more difficult to fake, while however adding less infallibility when accessed without authorization. The public should realize, however, that when individuals' biometrics data are stored, it is not an image, but rather a fingerprint template which stores markers and unique characteristics. In that note, the hardware finger reader, for example, is creating a file that is not useful for any other purpose than intended. In the nutshell, individuals' fingerprint or iris images are never stored in the database of banks or any other POS systems, but they are coded (encrypted) data that will be stored in the server that should be compared with the previously stored coded data.

5) How can banks address the issue of companies holding their biological makeup and the public fear of its misuse? Any procedure that involves the collection of biometrics data should be made well aware by customers and users. The implementation of standardized legislation should help alleviate the concerns and fear. If there are guidelines that have been implemented by our government, a logo or some sort of graphics indicating the compliance of the guidelines by the institution (bank) would create more trust between the customers and the bank.

6) Is there sufficient attention being put into the application of these new technologies in the Banking industry? At this point in time, there is a lack of development and attention to this field, as compared to many other nations. Even internally, there are Canadian telecommunication industries that are investing more into biometrics and increasing their involvement far more than the banking industries, where the stakes may be higher.

7) Some biometrics technologies in banking have been implemented in countries such as Japan for a few years, why do you think it's taking long for Canadian banks? Is it a matter of regulation or a matter of consumer acceptance? Consumer acceptance is not a problem as it has been expressed that there is preference for biometric security in the place of passwords and PINS, by many customers, as far as those informants are concerned. For banks, it seems that they think it is easier for them to charge whatever costs involved with security breach to their clients than to explore and implement a smart system that prevents the cases of security breach. As such, their (banks') willingness for change is very low as they regard the losses that could be avoided or severely reduced by biometrics as part of their operational costs, which could be transferred to their clients.

8) Apart from rights to privacy, is there a need for new legislation to accommodate the new realm of biometrics data collection within the customer's' daily life? There is need for new legislation that is more focused on biometrics and the implication on the financial industry. However, legislators in Canada first need to have a thorough understanding of the applications of the technology.

9) Biometrics involves the use of personal data such as fingerprints, which cannot be changed if compromised, what kind of contingency plans or to what extent should these companies be accountable? The biometric data is the collection of personal information and therefore is protected under the laws and regulation of privacy and personal identity. In order to lessen the risks, banks should have plans that would be specific to individual adoption. Risks can be reduced when they are part of a larger system in which accountability is spread to everyone if there are security breaches, which in itself creates the process of tighter protection.

7. DISCUSSIONS

The purpose of this study is to inform readers about current technological aspects of biometrics technologies and also to provide important implications on the direction of biometrics within the banking industry in Canada. We believe that the employment of this qualitative data collection through interview was best to draw more information from an industry that is lacking transparency on any technological advancement. Based on four categories of our interview questionnaire and answers to each questions, we discuss our views on the biometrics in Canadian banking industry, as follows.

7.1 Integration into Canadian Banks

Overall, the professionals within the industry have a more pessimistic stance in relation to the future of biometrics in Canada. In itself, the inept and incomplete response by banks and bank representatives on the topics shows findings that correlate to lag of the technology within the Canadian banking context. The very protected and regulated financial industry of Canada is moving at a slow pace [41]. An issue that was brought up was the idea of banks charging fraud net losses from their companies as part of the operational costs. According to Canadian Banker's Association, in 2014 alone, there was a total loss of approximately $549M lost in credit card fraud in Canada and over 16M in the Interac association [14]. In 2015, there's been an increase of annualized net loss rate of 3.13% in the past 3 years for Canadian financial institutions that issue Visa and MasterCard due to credit card delinquencies [15]. As consumers are protected under the zero liabilities fraud policy of financial institutions, the banks bear the burden, however this burden is mitigated by increasing customer fees. In 2014, banks reimbursed customers for more than half a billion dollars in losses as the result of credit and debit card fraud. Based on our interview with key informants, we believe that biometrics will offer an alternative that can immensely decrease the cost involved with credit and debit card fraud cases as part of a more securitized and transparent system, which will eventually reduce the consumer fees that is now implicitly transferred from the firms to the clients.

7.2 Perceived Public Opinions and Concerns

The findings of the study point out and suggest that there is a hyperbolized perception that consumers have on the vulnerability of biometrics. As a measure, we need to note if there should be a trade-off between convenience and privacy. However, that is not the case. According to a recent study in the UK by Experian, about 64% of people trust and are comfortable using biometric technology to access their bank accounts and perform online banking [18]. There is an increased trust of biometrics as integration of biometrics is increasing relatively fast, especially in the mobile payment technologies, such as Samsung Pay and Apple Pay. Nevertheless, another factor expressed by the questionnaire concerning consumers' fear about releasing their biometric information is the need for transparency within those banking institutions. Biometrics, unlike PINs, cannot change but remain constant; therefore banks that provide full application details in terms of the securitization of the biometrics data are favored. Canadians have become more aware of their privacy rights under the law [13], which shifts the need to create more secure systems that can protect the privacy of customers.

7.3 Steps to Transition

In the larger context, the decisions to implement biometrics technologies of the banks are solely at their disposal, although the penetration level of biometrics will depend on end-users' acceptance. Due to their perceived protections within the industry and the infancy of legislation that can purely assess the impacts that biometrics can have on the industry and protect firms over customers, Canadian banks are moving at a slower rate in terms of adopting biometrics for end-user security systems than many other financial institutions in the world. Up until recent days, it could be the case that the overall environment has not created much need for fast adaptation of biometrics in Canadian banking sector. However, since the public is now being more educated with the ease and perceived security of biometrics technologies (i.e., two most important factors for biometrics adoption suggested in the literature) in their smartphone applications, we believe that the general public in Canada will change the overall environment which should accelerate the speed of implementation of biometrics in Canadian banks.

7.4 Accommodation for Biometrics in Banking

The results of our interviews show that professionals on biometrics find that there is a conjunction between privacy laws and laws related to biometrics. The comparisons are clear as privacy laws deal with the personal information of individuals, with which banks would be dealing with to a greater extent. It seems that there might be hesitation on that aspect by the banks because the laws are not very clear. A reason banks may not want to act very quickly on biometric technology could be that the banks feel they are not sufficiently hedged by the law, and that the risks might be too large to take than the gain they would receive in return. This study demonstrates an aspect of calculation that could be a factor that contributes to the slow-down of adoption of biometric technologies.

This study has helped understand that the banking industry has the means for the full application of the technology which can gain feedback quickly as there is acceptance of biometrics security by the general population. However, until there is increased public demand and the risks and costs accounted for by fraud outweigh the bank's perceived transition costs, the banks will stay behind in the global context.

8. CONCLUSIONS

One of the limitations of this study is that this study focuses on only one country, Canada. However, we believe that current situation of biometrics implementation in Canada is a good example of any country where 1) a few major banks dominate the industry and 2) the banking industry is highly coordinated and regulated by the government. We believe that the banking industries of many other countries probably face similar situations right now. In addition, in general, end users of banking and credit card services are now experiencing fast changes in the ways financial technologies are evolving, with emerging trends of mobile payment solutions with biometrics (fingerprint readers in smartphones), P2P (Peer-to-Peer) lending and money transfer (e.g., LendingClub and Alipay), and voice recognition enabled in call centers of banks. Another limitation of this study is that this study collected interview data from journalists and technology vendors, not the representatives of banks or other financial institutes. Therefore, further data collection is needed to provide a more detailed description regarding the adoption of biometrics technology in the Canadian banking industry.

Based on our literature review on the adoption of biometrics as well as interviews with key informants, we found that what makes the implementation of biometrics in Canada (or probably in other countries that have similar technological, regulatory, and industrial situations) slow (if not behind the leading countries) are not technological issues per se, but the issues like *1) public concerns about privacy, 2) lack of education about the easiness and perceived security of biometrics technologies, 3) unclear privacy laws which might directly influence the implementation of biometrics in banking industry, and 4) highly coordinated industry members and regulatory boards in government.* Therefore, in order to implement biometrics technologies in banking services, which can solve many security problems and reduce the cost of frauds associated with traditional method ID/Password methods, we suggest that both industry members and government regulators work together to address these four above mentioned issues.

9. REFERENCES

[1] AHMAD, D.T. and HARIRI, M., 2012. User Acceptance of Biometrics in E-banking to improve Security. *Business Management Dynamics 2*, 1, 01-04.

[2] AMIT, 2015. 7 Trends in Biometric Technology as It Applies to FinTech letstalkpayments.com.

[3] ASHFORD, W., 2016. HSBC launches biometric security for mobile banking in the UK. In *Computer Weekly*.

[4] BARCLAYS, 2012. Banking on the power of speech Barclays.

[5] BELTON, P., 2015. In your irises: The new rise of biometric banking. In *BBC*.

[6] BEVAN, K., 2015. At the speed of sound: RBC conversational voice biometrics a Canadian first RBC.com.

[7] BIOMETRIC-SOLUTIONS, unknown. Biometric Applications Biometric-solutions.com.

[8] BIOMETRICS.GOV, 2006. Privacy & Biometrics: Building a Conceptual Foundation Biometrics.gov.

[9] BUSTARD, J., 2015. The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. *Signal Processing Magazine, IEEE 32*, 5, 101-108.

[10] BYUN, S. and BYUN, S.-E., 2013. Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters. *Behaviour & Information Technology 32*, 3, 217-230.

[11] CALDWELL, T., 2012. Voice and facial recognition will drive mobile finance. *Biometric Technology Today 2012*, 10, 2-3.

[12] CALDWELL, T., 2015. Market report: border biometrics. *Biometric Technology Today 2015*, 5, 5-11.

[13] CANADA, O.O.T.P.C.O., 2013. Survey of Canadians on Privacy-Related Issues; Final Report www.priv.gc.ca.

[14] CANADIAN-BANKERS-ASSOCIATION, 2015. Credit Card Fraud and Interac Debit Card Statistics - Canadian Issued Cards, cba.ca.

[15] CANADIAN-BANKERS-ASSOCIATION, 2016. Credit Card Delinquency - VISA and MasterCard, cba.ca.

[16] CLARK, B., 2015. The History of Biometric Security, and How It's Being Used Today www.makeuseof.com.

[17] CRAWFORD, C.M., 1998. Internet online backup system provides remote storage for customers using IDs and passwords which were interactively established when signing up for backup services Google Patents.

[18] CUNNINGHAM, I., 2015. UK Now Ready for Biometric Banking www.experianplc.com.

[19] DUNKER, M., 2003. Dont blink: Iris recognition for biometric identification. *SANS Institute*.

[20] GELB, A. and DECKER, C., 2012. Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries*. *Review of Policy Research 29*, 1, 91-117.

[21] GILMORE, W. and ERDEM, S.A., 2011. The Future Of Online Internet Marketing: A Solution To Behavioral Marketing Using Biometrics. *Journal of Business & Economics Research (JBER) 6*, 2.

[22] GOLD, S., 2011. Biometrics–a global review. *Biometric Technology Today 2011*, 4, 5-8.

[23] GOLD, S., 2012. Biometrics at the ATM–the need for customer authentication. *Biometric Technology Today 2012*, 6, 7-10.

[24] HASSANEIN, K., HEAD, M., HAROLD, A., and IVANOV, A., 2012. Intention to Use Biometrics For Automated Banking Machine Access: The impact of Educational Interventions. In *Emcis 2012*.

[25] HOANG, B. and CAUDILL, A., 2008. What Is Biometrics?, docs.askiven.com.

[26] IRITECH, 2015. Biometric Attendance System: Iris versa Fingerprint iritech.com.

[27] JAIN, A., ROSS, A.A., and NANDAKUMAR, K., 2011. *Introduction to biometrics*. Springer Science & Business Media.

[28] KILADZE, T., 2014. Too Big To Disrupt? In *The globe and mail*.

[29] LAWSON, W.J., 2003. Enhancing Assistive Technologies: Through the Theoretical Adaptation of Biometric Technologies to People of Variable Abilities Western University.

[30] LE, C. and JAIN, R., 2009. A survey of biometrics security systems. *EEUU. Washington University in St. Louis*.

[31] LEE, J., 2016. Ford R&D lab exploring the integration of wearables and vehicles biometricupdate.com.

[32] LOCKHART, B., 2015. In Biometrics, Which Error Rate Matters? tractica.com.

[33] M2SYS, 2014. Biometrics For Financial Service Identity M2sys.com.

[34] MOST, C.M., 2004. Bioemtrics and Financial Services-Show Me the Money! *Digital ID World*, 20-23.

[35] MURALIDHARAN, K., NIEHAUS, P., and SUKHTANKAR, S., 2014. *Payments infrastructure and the performance of public programs: Evidence from biometric smartcards in india*. National Bureau of Economic Research.

[36] NANAVATI, S., THIEME, M., and NANAVATI, R., 2002. *Biometrics, Identity Verification in a Networked World*, . Wiley Computer Publishing.

[37] NORMALINI, M. and RAMAYAH, T., 2015. A Proposed Biometrics Technologies Implementation in Malaysia Internet Banking Services. In *Innovation, Finance, and the Economy* Springer, 79-87.

[38] PALMER, K., 2015. Pins 'obsolete within five years' - and pay with mobile or fingerprints instead www.telegraph.co.uk.

[39] PERALA, A., 2016. Global Biometrics Market to Reach $41.5B by 2020: BCC Research findbiometrics.com.

[40] PRASAD, R.S., AL-ANI, M.S., and NEJRES, S.M., 2015. An Efficient Approach for Fingerprint Recognition. *Image 4*, 5.

[41] PRUSS, L., 2015. The Differences Between Banking in the US and Canada thefinancialbrand.com.

[42] ROUSE, M., 2015. DEFINITION: biometrics techtarget.com.

[43] SCALLAN, N., 2012. Bay Street law firm uses fingerprint technology to monitor employees' comings and goings. In *The Star*.

[44] SOLTANE, M., 2015. FACE, VOICE AND SIGNATURE MULTI-MODAL BIOMETRIC VERIFICATION FUSION SYSTEMS. *Annals of the Faculty of Engineering Hunedoara 13*, 4, 139.

[45] TASSABEHJI, R. and KAMALA, M.A., 2009. Improving e-banking security with biometrics: modelling user attitudes and acceptance. In *New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on* IEEE, 1-6.

[46] TASSABEHJI, R. and KAMALA, M.A., 2012. Evaluating biometrics for online banking: The case for usability. *International Journal of Information Management 32*, 5, 489-494.

[47] TRADER, J., 2014. The Impact of Biometrics in Banking M2Sys.com.

[48] UNKNOWN, A., 2006. Biometric statistics in focus. *Biometric Technology Today 14*, 2, 7-9. DOI= http://dx.doi.org/http://dx.doi.org/10.1016/S0969-4765(06)70471-4.

[49] VENKATRAMAN, S. and DELPACHITRA, I., 2008. Biometrics in banking security: a case study. *Information Management & Computer Security 16*, 4, 415-430.

[50] WAYMAN, J., JAIN, A., MALTONI, D., and MAIO, D., 2005. *An introduction to biometric authentication systems*. Springer.

[51] WONG, C., 2015. Canadian banks are putting their fingers on the benefits of biometrics blog.allstream.com.