# Biometrics in banking security: a case study

Sitalakshmi Venkatraman

*School of Information Technology and Mathematical Sciences, University of Ballarat, Ballarat, Australia, and*

Indika Delpachitra

*Information Security Consultant, AXA Australia & New Zealand, Melbourne, Australia*

## Abstract

**Purpose** To identify and discuss the issues and success factors surrounding biometrics, especially in the context of user authentication and controls in the banking sector, using a case study.

**Design/methodology/approach** The literature survey and analysis of the security models of the present information systems and biometric technologies in the banking sector provide the theoretical and practical background for this work. The impact of adopting biometric solutions in banks was analysed by considering the various issues and challenges from technological, managerial, social and ethical angles. These explorations led to identifying the success factors that serve as possible guidelines for a viable implementation of a biometric enabled authentication system in banking organisations, in particular for a major bank in New Zealand.

**Findings** As the level of security breaches and transaction frauds increase day by day, the need for highly secure identification and personal verification information systems is becoming extremely important especially in the banking and finance sector. Biometric technology appeals to many banking organisations as a near perfect solution to such security threats. Though biometric technology has gained traction in areas like healthcare and criminology, its application in banking security is still in its infancy. Due to the close association of biometrics to human, physical and behavioural aspects, such technologies pose a multitude of social, ethical and managerial challenges. The key success factors proposed through the case study served as a guideline for a biometric enabled security project called Bio Sec, which is envisaged in a large banking organisation in New Zealand. This pilot study reveals that more than coping with the technology issues of gelling biometrics into the existing information systems, formulating a viable security plan that addresses user privacy fears, human tolerance levels, organisational change and legal issues is of prime importance.

**Originality/value** Though biometric systems are successfully adopted in areas such as immigration control and criminology, there is a paucity of their implementation and research pertaining to banking environments. Not all banks venture into biometric solutions to enhance their security systems due to their socio technological issues. This paper fulfils the need for a guideline to identify the various issues and success factors for a viable biometric implementation in a bank's access control system. This work is only a starting point for academics to conduct more research in the application of biometrics in the various facets of banking businesses.

**Keywords** Biometrics, Critical success factors, Banks, New Zealand, Data security

**Paper type** Case study

## Introduction

Today, most organisations are aware of the importance of competitive tools and leading edge "information technology" (IT) solutions that could assist in gaining a competitive advantage (Jain *et al.*, 2006; Clarke and Mekala, 2007; Condon, 2007). Biometrics, an emerging technology, is a way of automatically recognising a person by traits such as fingerprints, hand geometry, signature, retina or voice (Bolle *et al.*, 2004; Capoor, 2006; Song *et al.*, 2007). This sophisticated technology could play a major role in protecting banking assets and thereby providing a safe banking environment. However, biometrics is still in its infancy within the banking sector and many unresolved issues are involved in implementing such leading edge technologies (Irvine and Levine, 2001; Zedner, 2003; Barton *et al.*, 2005; Chandra and Calderon, 2005; Lysecki, 2006).

There have been some previous studies conducted on modern IT security applications in postulating the concept and the fundamental elements of systems security models and technology standards (Karger *et al.*, 2000; Krutz and Vines, 2003; Feng and Wah, 2002). There have also been many studies on security processes and strategic concepts for improving the security system solutions to cater to the individual business needs (Rosenbloom, 2000; Harris and Yen, 2002; Woodward *et al.*, 2003; Boukhonine *et al.*, 2005; Riley and Kleist, 2005). However, there has been little research conducted in the direction of studying the issues and success factors of biometric solutions and in proposing strategies for a viable biometric implementation towards achieving a more secure banking environment.

The structure of the paper is as follows. The next section gives a background of the case study development and the research methodology adopted. Following this, we present a snapshot of the state-of-the-art of biometrics-related emerging technologies from literature, identifying the current IS security models that are predominantly adopted in the banking industry. In this context, we examine the applicability of biometric-enabled security systems and access controls in such models. The subsequent section describes the outcomes of the pilot study conducted within the New Zealand banking organisations resulting in identifying the major issues and key success factors that encompass the adoption of a biometric solution. We then discuss one such project, called Bio-Sec, where biometric-enabled access controls are being ventured in a large banking organisation. Finally, we highlight future research possibilities and the conclusion derived.

## Case study background

Major banks including New Zealand are focussing in a new breed of online-based virtual banking services, wireless and mobile phone banking systems and the like (Costanzo, 2006; Clarke and Mekala, 2007) to meet the business competitiveness. However, while the benefits of using such anywhere and anytime services are high, they result in a much higher exposure to common cyber-related risks (Zorkadis and Donos, 2004; Barton *et al.*, 2005). Risks such as viruses, worms, denial of service, malware, web site defacements, information hacking, cyber-sabotage and cyber-terrorism have unique styles of attacking which require equally unique treatments to be put in place as preventive measures. A preliminary survey that we performed recently with the major banks of New Zealand indicates that the majority of

the security breaches are due to unauthorised access by internal staff or external partners (Figure 1).

Biometric technologies have the capability of becoming the *de facto* method for secure identification and personal verification activities in banks (Bielski, 2000). However, there are significant amount of security risks involved in implementing such leading edge technologies (Irvine and Levine, 2001; Zedner, 2003; Prabhakar *et al.*, 2003; Kay, 2005). Further, information security policies and compliance statutes have also undergone considerable changes over the last few years both locally and globally (Karger *et al.*, 2000; Mortlock, 2003; Hunter *et al.*, 2006). Hence, banking organisations are surrounded by various techno-economic factors that contribute towards the success or failure of any new security strategy that could be introduced within the prevailing global constraints and standards.

*Case study objectives*

This case study was developed to provide an in-depth analysis of the security factors and issues with regard to formulating a biometric-enabled secure banking environment in New Zealand. We explore the information security models that currently exist within the banking sector and how these could be improved using biometric solutions. Through the study, we identify the applicability of biometric-security systems and access controls in banking environment and evaluate the security strategies and processes from both user perspective as well as technology viability. We examine the key success factors and prevailing constraints that could create significant impact on acquiring a biometric solution for banking organisations.

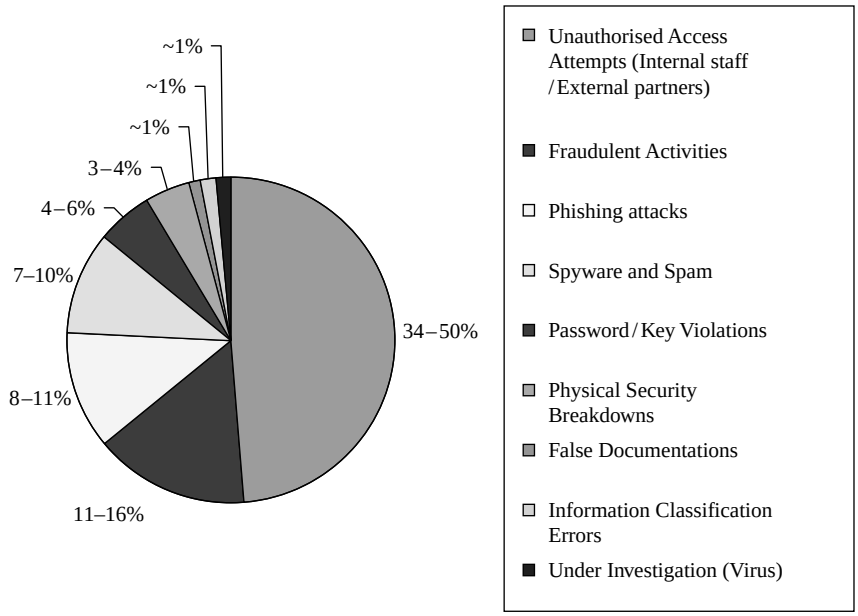


**Figure 1.**
Security breaches within New Zealand banks (2006 2007)

*Research methodology*

In this case study, a survey-type research methodology was chosen to examine the current banking environment in New Zealand. It consists of two parts, namely:

(1) Analysis of the security models *vis-à-vis* suitable biometrics envisaged in banking industry.

(2) Case-based analysis of a particular biometric project implementation in a New Zealand bank.

We conducted such analysis within New Zealand banking industry through interviews that were verified using supporting data and findings collected from a number of secondary sources such as journal articles, textbooks and other reference materials from organisations related to this case study.

We designed a questionnaire consisting of qualitative as well as quantitative questions for interviewing the participants from the major New Zealand banks. The questionnaire was structured in a way to ascertain the prevailing security issues in banking environment so that an appropriate biometric solution could be worked out. The questionnaire was aimed at addressing the following five objectives with respect to the banking environment:

(1) To understand the prevailing IT security processes and policies.

(2) To understand the prevailing IT security infrastructure.

(3) To obtain the leadership aspects of the IT security.

(4) To acquire the level of knowledge and appreciation of biometric-enabled security access solutions by the employees and the management.

(5) To identify the key issues and concerns.

Altogether, there were about 30 qualitative-type questions and ten quantitative-type questions. The participants of the survey were from three different categories, namely, security management, operations management and information security architecture of the major banks of New Zealand. Three major banks with three to four participants from each bank were considered for the study. Structured interviews were also carried out with key participants involved in the areas of system security and product development subsequently.

## Analysis of biometric technologies

Most of the biometric systems are combinations of "hardware" such as sensors and "pattern matching software". Both of these components have to be accurate and error-free in order to have a perfect solution in place (Lomax, 2000; Maltoni and Maio, 2003). However, the effectiveness of these biometric solutions can be dependent on the quality of the censoring hardware devices, the speed, and accuracy of the pattern matching software. We identified and compared some of the biometric technologies used commercially, based on the views obtained from the survey participants as well published work from secondary sources. We performed a strength-weakness-opportunity-threat (SWOT) analysis of these biometric technologies and this is summarised in Table I.

There was much similarity in the findings between participant feedback and those results published in secondary sources (National Science and Technology Council, 2006;

| Biometrics | Single-node cost (includes hardware) | Strengths | Weaknesses | Opportunities | Threats |
|---|---|---|---|---|---|
| Face recognition | Low | Easy; fast; one of the least expensive methods | Subject to spoofing attempts; awkward lighting in the image can affect authentication | General | Reliability (changes in lighting and photo angles affect the reliability of data) |
| Fingerprint | Low | Inexpensive, very secure, uniqueness, ease of capture | Latent prints, cuts and dirt can mar image | Law enforcement corporate databases; long standing reputation | Validity of matching accuracy (masking the finger to avoid the match; ability to force a false match) |
| Palm scanning/hand geometry | Moderate | Tiny storage requirement; intuitive operation | Slow, less accurate than finger scanning | Manufacturing/shop floors | Confidentiality (hijacking of contour data that are simple could affect privacy) |
| Iris/retina scanning | High | Extremely difficult to fool | Intrusive and inconvenient | Nuclear facilities, medical services, correctional institutions | Ability to presenting a photo of the target's iris. (lack of liveliness testing), printing iris pattern on contact lenses |
| Thermal image | Extremely high | Extremely difficult to fool | Requires expensive infrared cameras | Sites requiring ultra high security | User acceptance (involves infrared imaging that could be seen intrusive) |
| Voice print | Low | Inexpensive; good for remote access | Slow; can be affected by physical condition or emotional state | Remote banking, remote database access | Reliability (vulnerable to replay attacks) |
| Signature recognition | Low | Inexpensive | Can be affected by physical condition or emotional state | Industrial | Data accuracy and reliability (variable trait data; vulnerable to replay attacks) |

**Table I.**
A SWOT analysis of the biometric techniques used commercially

International Biometric Group, 2006). In Table I, the most common attributes such as cost, data accuracy, reliability, privacy, etc. have been considered for comparisons. Though all these attributes have an impact in the strength, weakness, opportunity and threat of each biometric technology, only the most predominant features have been cited in Table I. For example, the reliability feature is considered as a threat much more for face recognition than for fingerprint. This is because changes in lighting could affect facial image as compared to fingerprints. Similarly, though user acceptance is a concern for each technology, it is more prominent in the case of thermal image technology as it involves infrared, which could be regarded as intrusive to users' health. Detailed results and discussions on the comparison of these technologies are available from international secondary sources published in the Web (National Science and Technology Council, 2006; International Biometric Group, 2006).

Overall, with conventional facial, fingerprint, iris and palm biometrics, we observe that issues such as reliability and privacy arise since the technologies use information from the visible surface of the user. Such issues exist due to the fact that information could be affected by external factors and are relatively easy to copy and manipulate. However, recent vein-based techniques for biometrics could eliminate such concerns as the information collected from the veins would be invisible to the human eye and could not be easily altered. Such vein-based facial, finger, iris and palm biometrics are being investigated and much research is underway (International Biometric Group, 2006).

*Analysis of information security models used in banking systems*

Providing a secure computer environment is a major concern for most banking organisations at present (Boukhonine *et al.*, 2005). In terms of formulating a security policy in banking systems, the five main objectives of information security, namely availability, confidentiality, integrity, accountability and non-repudiation are to be satisfied with the primary goals being the ability to provide originality and controlled availability of information with appropriate audit mechanisms. Such access controls are currently implemented in banking systems using physical devices that can support access control cards/keypads, and monitoring by people or automated systems that have the ability to permit or deny the usage of an object (a passive entity, such as a system or file) by a subject (an active entity, such as an individual or process).

We compare eight different security models from literature (Bell and LaPadula, 1973; Biba, 1977; Krause *et al.*, 2000; Krutz and Vines, 2003) that are widely used in banking organisations. We compared these commonly used security/access control models in terms of their objectives, main features, strengths and weaknesses and identified suitable biometric solutions that can incorporate such IS security theories in a banking environment. Table II provides a summary of the findings.

Even though from a theoretical viewpoint, any of the security models could be adopted for any of the biometric solutions, certain features in each model go hand-in-hand with certain requirements of the biometric technology. For example, in iris biometrics, even though data accuracy is high and does not deteriorate over time, the iris recognition software is required to make calls to the private ID driver and this extra time imposes that the user's eye remains open long enough. In RBAC model, since roles are assigned to users, restricting them to perform only certain tasks (Ferraiolo *et al.*, 1999), the iris recognition software requires only restricted time for the

**Table II.** Comparison of security models and access controls adopted in banking sectors

| Security/access control models | Description of the model | Main features | Advantages | Weaknesses | Suitable biometric solution |
|---|---|---|---|---|---|
| Bell-LaPadula model (BLM) | Defines the modes of data access, along with the rules for granting access | Access based on subject, object, operations and related security level; only static infrastructure | Privacy focus. No mention of recent security attacks | Not suited for dynamic financial institutions with network systems; limited documentation available | Face recognition fingerprint palm scanning/hand geometry |
| Biba model (BM) | Addresses data integrity levels | Covers inappropriate modification of data with subject and object accesses | Prevents unauthorised users from making alterations or modifications | Same as BLM; subjects cannot read or write to objects of higher integrity | Face recognition fingerprint palm scanning/hand geometry |
| Clark-Wilson model (CWM) | Addresses data integrity levels within two major areas: data objects and roles (selected roles assigned to different users) | Addresses the relationship between the subjects and the acceptance of their information | Prevents unauthorised users from making any alterations or modifications; maintains data consistency | Same as BLM; performs exactly the steps listed with no flexibility | Face recognition fingerprint |
| Brewer-Nash access model (BNAM) | Allows information security access controls that can change dynamically | Refers how subjects and objects should be created or deleted; addresses how to assign specific access rights | Suited for network systems; provides controls that mitigate conflict of interest in commercial organizations | Requires some kind of dynamic labelling; does not provide adequate protection against illegal information flows | Palm scanning/hand geometry |
| Nash-Graham-Denning model (NGDM) | Addresses access rights for creating and deleting objects and subjects | Access controls with tight primitive protection rights | Uses access matrix; access control within the OS; explores DAC | Storing the access matrix; conflict of interests in access control roles | Fingerprint |
| Role-based access control (RBAC) | Roles represent functions within a given organisation with authorisations granted based on the roles | Roles are based on the least privileges. A user has access to objects based on the assigned role | Roles are defined based on job functions. Suited for network systems | Users can perform only the given set of tasks. The object concern-ed with the user's role and not the user | Ideal for profile creation and authentications with any type of biometrics |
| Mandatory access control (MAC) | Decides how the data will be shared | Everything assigns with sensitivity level and related label | More secure than DAC (can be used in critical systems) | Relies too much on system. Hard to configure. Downgrade in performance | Thermal image |
| Discretionary access control (DAC) | Owner decides how data can be protected and shared | Access is restricted based on authorisation granted to users | Higher protection for user to data. Suited for network systems | Relies too much on object, owner to decide on controls | Fingerprint Face recognition |

matching process and hence iris biometrics is more suited for RBAC model than any other model. Similarly, since NGDM model has eight primitive protection rights with "owner" and "controller" access checks (Gopinath, 2006), fingerprint matching being more advanced and faster than other techniques, this is recommended here. On the other hand, due to the feature of MAC model to deny the users full control over the access to resources that they create, it is mostly commonly applicable for classified sensitive information (ICAO NTWG, 2004). Thermal imaging is recommended here as the user need not be in very close contact and information could be captured in complete darkness even. Overall, we find that each model mentioned in Table II has its own advantages and disadvantages with certain biometric technologies suiting its objectives. The main aspects such as confidentiality, integrity, reliability, accountability and non-repudiation contribute to determining the most suitable model from these alternatives.

In this pilot study, we conducted preliminary research on certain major banking organisations in New Zealand with regard to their access control techniques. We observed that majority of them use the DAC model with some aspects of the RBAC model as the foundation for their security controls. In some instances the organisation also uses the MAC model for lower level staff whose user tasks are controlled by a selected set of rules and permissions. Both DAC and MAC techniques are being used with the application of the RBAC model as the permissions can be assigned based on organisational or functional roles. This strategy greatly simplifies the usage of biometrics as it helps to identify the authentication of a user and determines the access-right privileges that a user can possess.

## Discussion on case study findings

In this pilot study conducted in the banking sector of New Zealand, the feedback gathered through questionnaires and interviews conducted with the survey participants was analysed. We observe that more than coping with the technology issues of gelling biometrics into the existing information systems, formulating a viable security plan that addresses user privacy fears, human tolerance levels, organisational change and legal issues is of prime importance. From the case study we identify the critical success factors for a viable adoption of biometric-based security solutions in banking organisations. We also identify and discuss the prime issues faced by banking organisations and these need to be addressed as they impact the success factors. We group these success factors under four main categories as follows:

(1) Technology factors.

(2) Monetary factors.

(3) Management factors.

(4) Legal and ethical factors.

Table III shows a summary of these critical success factors along with their related issues, and possible solutions. These have been compiled based on the feedback gathered from the case study. The relative rating of importance for each success factor as perceived by the survey participants is also summarised in Table III. We discuss each of these critical success factors below.

| Critical success factors | Issues | Possible solutions | Importance |
|---|---|---|---|
| Technology factors | (1) Ability to provide a flexible but robust solution | (1) Consider biometrics that promote flexibility to accommodate sufficient tolerance levels and future enhancements (prepare a "Roadmap" for evolving biometric solution for future needs) | High |
| | (2) Capability for gaining a competitive advantage | (2) Adopt a collaborative approach through an accepted model in preserving existing privacy but improving security measures | |
| | (3) Integrating with the existing "Legacy" systems | (3) Evaluate the risks in applications using thorough testing | |
| | (4) Availability of support IT infrastructure | (4) Develop an operational model that integrates biometrics with legacy systems | |
| | | (5) Develop tools for evaluating combinations of authentication techniques | |
| Monetary factors | (1) Measuring the cost effectiveness in relation to its tangible/intangible benefits | (1) Produce "Financial Recommendations and Requirements" including a comprehensive assessment of the project with a cost/benefit analysis | Moderate |
| | (2) Ability to provide long-term sustainability | (2) Evaluate "Interoperability and Process Efficiency" | |
| Management and leadership factors | (1) The long-term sustainability of the biometric solution | (1) To encourage and be a role model for challenges needing a top-down lead | Moderate |
| | (2) Unsatisfactory level of performance for financial institutions with certain biometrics | (2) Discourage the "silo mentality" culture within the organisation and promote innovations and constructive approach to new security solutions | |
| | (3) Other financial institutions may not implement similar solutions hence the efforts will be isolated and deprived of being the marker leader | (3) Promote comprehensive strategies to embrace new technological solutions which will address security requirements | |
| | | (4) Maintain a "transparently manageable" process so that the users are not kept in the dark | |
| | | (5) Make necessary changes to "Security Policy" framework to meet the requirements | |
| Legal and ethical factors | (1) Legal issues concerning the protection of user privacy and rights | (1) Establish controls to ensure that the solution adhere to, and comply with all laid down laws and regulations | High |
| | (2) Reluctance of users to accept biometrics as a trustworthy and reliable solution | (2) Ensuring the safety of information and security standards | |
| | | (3) Promote new authentication techniques that will not displace, but only complement traditional techniques | |
| | | (4) Promote positive and secure culture and awareness programs to welcome biometrics | |

**Table III.**
Summary of related success factors and related issues with biometrics

*Technology factors*

*Accuracy*. Accuracy of a biometric system is measured in terms of false rejection, false acceptance rate, false rejection rate, false match rate, false non-match rate, failure to acquire, failure to enrol, equal error rate, ability to verify (ATV) (Woodward *et al.*, 2003). In the banking environment, the ATV measure is given utmost importance and a biometric authentication system that provides robust accountability and superior fraud detection are considered as the basic success factors.

*Flexibility*. Biometric systems are required to deal with fault-tolerance, mainly the characteristic changes in individuals such as developing wrinkles, developing poor blood circulation, etc. (Lysecki, 2006). A 100 per cent digital translation and matching of the data may not always be a requirement. Furthermore, it may not always be efficient from a usability perspective to set the comparison threshold very tight. Due to this reason, in banking environments, biometrics is often used as a verification mechanism in conjunction with another form of identification (e.g. a swipe card or PIN), which could cater to user changes and user control. Hence, the study reveals that technological flexibility and tolerance levels that biometric solutions offer impact to a great extent on their success of adoption. According to one feedback obtained, "new technology developments should also be complementing the bank's existing IT infrastructure and traditional delivery methods".

*Privacy and confidentiality issues*. There is some risk associated with privacy and confidentiality if biometric signature gets stolen or misused. Hence, organisations should determine the level of security needed for their specific application: low, moderate, or high (Lysecki, 2006). This decision will greatly influence the selection of the most appropriate biometrics. Generally, behavioural biometrics is sufficient for low-to-moderate security applications while physical biometrics would be required for high-security applications (Nanni and Maio, 2006). Further, the feedback from the survey indicates that trade-off exists between the banks using a distributed closed system and centralised data storage as users could be greatly inconvenienced trying to update their biometric data in many systems if appropriate fault-tolerant procedures are not in place. These are some of the technological factors contributing towards privacy and confidentiality issues.

*Monetary factors*

*Tangibles*. Biometric solutions are significantly more expensive than conventional security solutions (Dass *et al.*, 2006). The banks under study regard two costs as major success factors, namely:

(1) User systems integration and testing costs.

(2) Highly skilled training and maintenance costs required to exploit the capabilities of this new technology to its maximum potential.

*Intangibles*. The survey indicates that some of the intangible benefits in banks would be competitive business advantage, productivity and profitability as there would be a major reduction in security risks that would boost up user confidence level. According to a participant, "the bank tries to drive down internal costs and improve business processes without compromising the IT security, though these initiatives appear to be considerably costly".

*Long-term stability and sustainability issues*. It is evident that some of the major banks in New Zealand have already started the smart card operations for internal security. However, the feedback from the present bank management reveals that majority of the banks would compromise the cost factor to some extent if biometrics delivers long-term stability and sustainability.

*Management and leadership factors*

*Management support*. The employee survey indicates that the following management support factors have a clear impact on the success of a biometric-enabled security in the banks:

- Senior management's willingness to support the biometric innovation.
- Availability of the capital outlay for the biometrics project.
- Appreciation of the working ethics and culture that would support such innovations by the staff.

*Availability of resources*. The following resources-related factors form the backbone of such a project innovation:

- Availability of highly skilled, trained and motivated staff for the project.
- Suitable robust infrastructure for the security framework.
- Suitable staff training programmes.

*Issues of coping with new technologies*. The case study indicates that in general, the operations management has less amount of appreciation towards biometrics: "there is a lack of knowledge and appreciation for biometric tools among the IT staff and management". There is a common feedback that the management should be willing to make the cultural and organisational adjustments necessary to derive any benefit from biometric access control changes.

*Legal and ethical factors*

*Government law*. According to the European Convention on Human Rights (Article 8), the use of unique characteristics of a human being such as fingerprint, Iris or hand geometry, could limit certain individual liberties. New Zealand banks are required to comply with government consolidated initiatives such as the Credit Contracts and Consumer Finance Act (2003), Consumer Guarantee Act, Privacy Act, Fair Trading Act, and the Contract Enforcements and Contractual Mistakes Act. These could impact the biometrics adoption process in the banks.

*Social and psychological issues*. The main social and psychological issue about biometrics is the "fear" of exposing the human bodies to radioactive waves (Alterman, 2003; Barton *et al.*, 2005; Condon, 2007). Although most biometric technologies have been proven not to interfere with human biological systems, these myths have to be dispelled. Also, one of the participants opine: "Our faces and irises are visible and our voices are being recorded and also fingerprints and DNA samples can be left everywhere and it can be a real threat to protect them".

Overall, establishing a sustainable biometric security infrastructure and addressing legal and ethical issues are the key concerns related to the banking organisations under study. Although management and leadership support and cost factors are perceived to

have only a moderate degree of importance, such factors should be given due consideration as well as they could impact the implementation stage to a great extent.

*Project Bio-Sec development*

In this section, we describe one particular banking organisation proposing to venture into a project (called Bio-Sec) of adopting biometric-enabled security access controls. The findings from the literature survey and industry analysis of this pilot study served as inputs to the Bio-Sec framework. Hence, addressing the security issues due to unauthorised access (internal staff/external partners) has been given utmost priority. The Bio-Sec project is initially aimed at integrating biometrics into a standard access card for a secure and comfortable authentication and identification of internal staff. Figure 2 shows the components of a proposed biometric-enabled security system for project Bio-Sec. The ultimate goal is to provide access to the bank's resources for the three categories of users, namely, bank's employee/contractors, bank's business partners and bank's support partners.

In this Bio-Sec project, the roles and responsibilities were clearly defined as revolving around access provisions and authentication processes. The preliminary analysis of biometric technologies and access security models along with the findings of the case study conducted in this research work paved way in deriving the security framework of the Bo-sec project. An overview of the security framework indicating the RSA token process map that is aimed to support both security management policies and user guidelines is shown in Figure 3. Bio-Sec is proposed to provide two basic types of access control tools using finger print technology with Smartcards or Bio-Secure Integrated ID cards to be utilised for access to this service and SSL.

A Bio-Sec user group with 15 members was formed for providing feedback, testing and making recommendations on behalf of their own business transactions. Amendments to the security guidelines for the Bank's existing security framework were developed in consultation with the Bio-Sec user group. An action plan was developed to train the employees formally on the introduction and the integration of biometrics to their work environment.

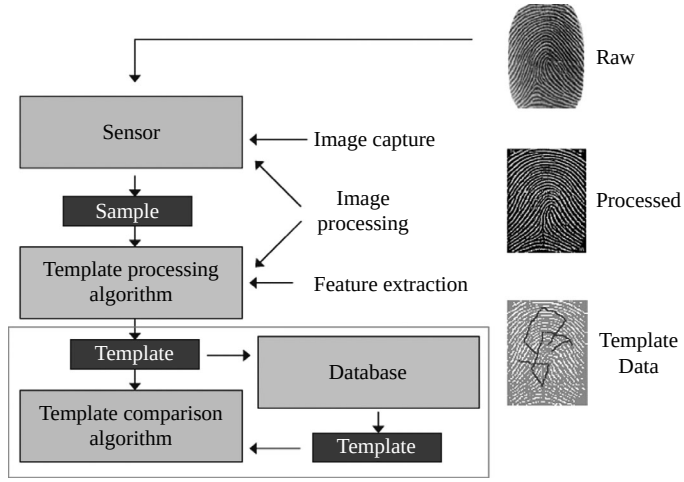


**Figure 2.**
Proposed biometrics security components (Bio Sec project)

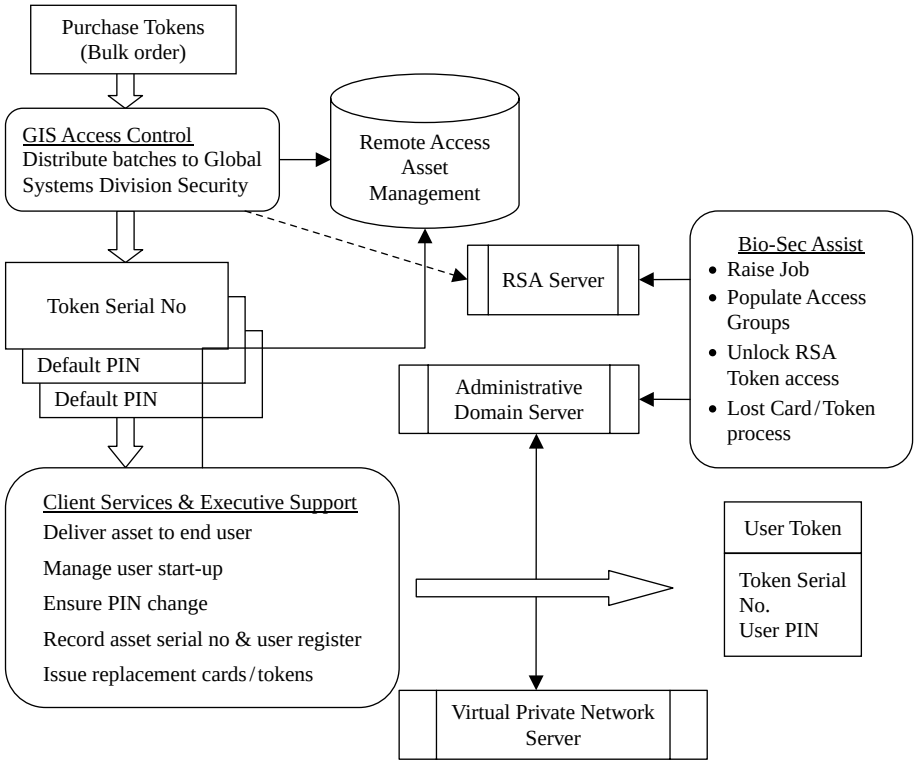


**Figure 3.**
Bio Sec RSA token process map

Any security programme must include other managerial controls, means of recovering from breaches of security, and above all awareness and acceptance by the users to make an information system trustworthy. This study reveals that when qualities such as accuracy, ease of use, adaptability, and technological advantage are offered together, there is no question that biometrics will ensure a highly secure banking environment. Hence, project Bio-Sec was initiated to create a positive and secure data management policy by giving importance to human rights protection. It adopts a combination of biometric techniques with data management policies that could abide by data protection standards and laws (Figure 3).

## Future research

Due to the fact that the bank considered in the case study is operating in such a highly competitive banking environment, the survey details and data values (including cost implications) are not provided here. Also, in order to ascertain all the success factors identified in this work, the Bio-Sec project has been envisaged to be piloted with certain group of internal staff of the bank. It does not include provisioning the biometric access and identification for customers or front-end staff (tellers) of the bank. Once project Bio-Sec takes up the implementation phase, it is our aim to conduct studies with external subjects including customers, staff and other partners of the bank.

## Conclusion

This case study was aimed at identifying the issues and challenges required to be overcome prior to determining the usage of biometric technology. The study conducted in the banking environment revealed that attaining high levels of business information integrity and overcoming users' security fears were of utmost concern. The study has also clearly established that more than coping with a technology change, a risk management strategy should address the issues related to the ethical and social areas. The success factors proposed in this paper would help banking organisations to plan their business strategies and processes with the required flexibility and adjustments that are warranted for a successful biometric security implementation.

This paper also described one such biometric project, called Bio-Sec, which was developed based on the proposed success factors. Bio-Sec had created appropriate security systems that utilised biometric technologies as complementary and supplementary mechanisms so that their reliance on biometrics was limited and accountable.

We conclude that a strategic fit with an appropriate, adaptable and sustainable biometric solution that addresses various social, ethical and technological issues would create a positive and secure environment that would welcome biometrics in banking sectors. In addition, well-formulated management strategies, security policies and data management processes that are developed with the required flexibility are the key aspects to a faultless biometric-enabled security solution that could meet tomorrow's needs as well.

## References


Alterman, A. (2003), "A piece of yourself: ethical issues in biometric identification", *Ethics and Information Technology*, Vol. 5 No. 3, pp. 1139 50.

Barton, B., Byciuk, S., Harris, C., Schumack, D. and Webster, K. (2005), "The emerging cyber risks of biometrics", *Risk Management*, Vol. 52 No. 10, pp. 26 31.

Bell, D.E. and LaPadula, L. (1973), "Secure computer systems: mathematical foundations and model", MITRE Corp, Bedford, MA (technical report).

Biba, K.J. (1977), "Integrity considerations for secure computer systems", MITRE Corp, Bedford, MA (technical report ESD).

Bielski, L. (2000), "Time to start biometrics", *American Bankers Association Journal*, Vol. 92 No. 10, pp. 54 9.

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K. and Senior, A.W. (2004), *Guide to Biometrics*, Springer Verlag, New York, NY.

Boukhonine, S., Krotov, V. and Rupert, B. (2005), "Future security approaches and biometrics", *Communications of the Association for Information Systems*, Vol. 16 No. 1, pp. 937 66.

Capoor, S. (2006), "Biometrics as a convenience", *Security*, Vol. 43 No. 12, pp. 48 50.

Chandra, A. and Calderon, T. (2005), "Challenges and constraints to the diffusion of biometrics in information systems", *Communications of the ACM*, Vol. 48 No. 12, pp. 101 6.

Clarke, N.L. and Mekala, A.R. (2007), "The application of signature recognition to transparent handwriting verification for mobile devices", *Information Management & Computer Security*, Vol. 15 No. 3, pp. 214 25.

Condon, R. (2007), "New biometrics see right through you", *Information Security*, Vol. 4 No. 1, pp. 24 6.

Costanzo, C. (2006), "Suddenly, biometric ID doesn't seem like science fiction", *American Banker*, Vol. 171 No. 107, pp. 6 11.

Dass, S.C., Zhu, Y. and Jain, A.K. (2006), "Validating a biometric authentication system: sample size requirements", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 28 No. 12, pp. 1902 13.

Feng, H. and Wah, C.C. (2002), "Private key generation from on line handwritten signatures", *Information Management & Computer Security*, Vol. 10 No. 4, pp. 159 64.

Ferraiolo, D., Barkley, J. and Kuhn, R. (1999), "A role based access control model and reference implementation within a corporate intranet", *ACM Transactions on Information and System Security*, Vol. 2 No. 1, pp. 34 64.

Gopinath, K. (2006), "Access control in communication systems", *Proceedings of the 1st International Conference on Communication System Software and Middleware, New Delhi, India*.

Harris, A.J. and Yen, D.C. (2002), "Biometric authentication: assuring access to information", *Information Management & Computer Security*, Vol. 10 No. 1, pp. 12 19.

Hunter, L., Orr, A. and White, B. (2006), "Towards a framework for promoting financial stability", *Reserve Bank of New Zealand Research Bulletin*, Vol. 69 No. 1, pp. 5 17.

ICAO NTWG (2004), "PKI for machine readable travel documents offering ICC read only access", Technical Report Version 1.1.

International Biometric Group (2006), "Comparative biometric testing", Round 6 Public Report, available at: www.biometric group.com (accessed January 2007).

Irvine, C. and Levine, T. (2001), "Data integrity limitations in highly secure systems", *Proceedings of the International Systems Security Engineering Conference, Orlando, FL*.

Jain, A.K., Ross, A. and Pankanti, S. (2006), "Biometrics: A tool for information security", *Transactions on Information Forensics and Security*, Vol. 1 No. 2, pp. 125 43.

Karger, P., Austel, V. and Toll, D. (2000), "A new mandatory security policy combining secrecy and integrity", IBM Research Division, Yorktown Heights, NY (technical report RC 21717(97406)).

Kay, R. (2005), "Biometric authentication", *Computerworld*, Vol. 39 No. 14, pp. 26 33.

Krause, M., Tipton, H.F. and Harold, F. (2000), *Information Security Management Handbook*, Chapter 3, 4th ed., Vol. II, Auerbach Publications, Boston, MA, pp. 103 58.

Krutz, R.L. and Vines, R.D. (2003), *The CISM Prep Guide: Mastering the Five Domains of Information Security Management*, Wiley Publications, Indianapolis, IN.

Lomax, V. (2000), "Fingerprint security goes live", *Banking Technology*, Vol. 16 No. 10, pp. 7 10.

Lysecki, S. (2006), "Federal facial recognition project raises privacy fears", *Computing Canada*, Vol. 32 No. 13, p. 14.

Maltoni, D. and Maio, D. (2003), "Real time face location on gray scale static images", *Pattern Recognition*, Vol. 33 No. 9, pp. 1525 39.

Mortlock, G. (2003), "New Zealand's financial sector regulations", *Reserve Bank of New Zealand Research Bulletin*, Vol. 66 No. 4, pp. 5 49.

Nanni, L. and Maio, D. (2006), "Combination of different fingerprint systems: a case study FVC2004", *Sensor Review*, Vol. 26 No. 1, pp. 51 5.

National Science and Technology Council (2006), "Privacy and biometrics building a conceptual foundation", NTSC Biometrics Publications, available at: www.biometrics.gov (accessed January 2007).

Prabhakar, S., Pankanti, S. and Jain, A.K. (2003), "Biometric recognition: security and privacy concerns", *Security & Privacy Magazine*, Vol. 1 No. 2, pp. 33 42.

Riley, R.A. Jr and Kleist, V.F. (2005), "The biometric technologies business case: a systematic approach", *Information Management & Computer Security*, Vol. 13 Nos 2/3, pp. 89-106.

Rosenbloom, A. (2000), "Trusting technology", *Association for Computer Machinery Journal*, Vol. 43 No. 12, pp. 30-3.

Song, O.T., Jin, A.T.B. and Connie, T. (2007), "Personalized biometric key using fingerprint biometrics", *Information Management & Computer Security*, Vol. 15 No. 4, pp. 313-28.

Woodward, J., Orlans, N. and Higgins, P. (2003), *Biometrics: Identity Assurance in the Information Age*, McGraw-Hill, Berkeley, CA.

Zedner, L. (2003), "The concept of security: an agenda for comparative analysis", *Legal Studies Journal*, Vol. 23 No. 1, pp. 153-76.

Zorkadis, V. and Donos, P. (2004), "On biometrics-based authentication and identification from a privacy-protection perspective: deriving privacy-enhancing requirements", *Information Management & Computer Security*, Vol. 12 No. 1, pp. 125-37.

## Further reading

Crosbie, M. (2005), "Biometrics for enterprise security", *Network Security*, Vol. 12 No. 11, pp. 4-8.

Strohm, C. (2005), "A new identity", *Government Executive*, Vol. 37 No. 3, pp. 63-9.

Zviran, M. and Erlich, Z. (2006), "Identification and authentication: technology and implementation issues", *Communications of the Association for Information Systems*, Vol. 17 No. 1, pp. 90-105.

## Corresponding author

Sitalakshmi Venkatraman can be contacted at: s.venkatraman@ballarat.edu.au