Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.5, No.3, 2015

Biometrics: A New Horizon to Corporate World

Md. Kafil Uddin (Corresponding author)
Lecturer
Department of Human Resource Management, University of Chittagong, Chittagong-4331, Bangladesh
Email: kafiluddin786@gmail.com

Sharmin Akther
Senior Lecturer
Department of Business Administration, East West University, Aftabnagar, Dhaka 1212, Bangladesh.
Email: sharmin333@gmail.com

Abstract
Biometrics technology is used as a powerful tool for solving identification and authentication issues for buddy punching, increased productivity, PC-based biometric time clock software, superior customer service platform, surveillance society, membership management, operational efficiency, superior customer service platform etc. It involves measuring one or more unique physiological human characteristics - the shape of a body, fingerprints, structure of the face, DNA, hand/palm geometry, iris patterns, typing rhythm, voice and even odor/scent be used because they can never be forgotten, lost or copied, unlike the current methods of smart card and passwords. The potential for biometrics is ever swelling in the business areas for ensuring efficient management through minimizing cost in accordance with maximizing profit. In such a context, this study is conducted to identify the application of biometrics in the formulation of management policy and business of the corporate sector. This paper also attempts to focus on some implications of biometrics technology in the corporate sector of Bangladesh as well as salient factors allied with the selection of appropriate biometrics technology in different organizations.
Keywords: Biometrics, Security, Identification, Business, Management Policy.

1. Introduction

The word "Biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). This directly translates into "life measurement". "Biometrics is the automatic identification of a person based on his or her physiological or behavioral characteristics" (Chirillo & Blaul, 2003, P.2). The term, biometric, can be used as a noun in reference to a single technology or measure (e.g., finger scan is a commonly used biometric) or as an adjective as in "a biometric system uses integrated hardware and software to conduct identification or verification" (Nanavati, Thieme, & Nanavati, 2002, p. 11).

Information security technologies continually evolve to meet new security threats. As a reflection of the increased need to protect organizations' information from both internal and external threats, many organizations have begun investigating the adoption of biometric security technologies as a significant component in their overall security architecture. An example of the astounding growth in this market, the International Biometric Group (IBG) expects biometrics industry revenue to increase from under $50 million in 2004 to almost $200 million in 2008 (Reynolds, 2004).

Understandably, a wealth of information exists regarding biometric technologies and the technical trade-offs in implanting biometric solutions. Notwithstanding a substantial body of literature on the technical aspects of biometric security technologies, little scholarly research has been undertaken regarding the critical factors that influence decision makers when they recommend that biometrics be adopted in the organizations. Further, trade magazines differ widely in their surveys of managers and/or their perceptions of information technology security and leave little in the way of data to aid management in making a solid security technology choice for their organization.

Biometric technologies are becoming the groundwork of an extensive array of highly secure identification and personal verification solutions. Human characteristic can be used for biometrics in terms of the parameters such as: Universality – each person should have the characteristic; Uniqueness – is how well the biometric separates individually from another; Permanence – measures how well a biometric resists aging; Collectability – ease of acquisition for measurement; Performance– accuracy, speed, and robustness of technology used; Acceptability – degree of approval of a technology; Circumvention – ease of use of a substitute (Jain, A. K.; Ross, Arun; Prabhakar, Salil , 2004).

2. Literature Review

A number of researchers have ascribed to the rationale for the choice to recommend a new technology to perceptions of its cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig &

Hamidi-Noori, 1985; Ettlie, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987: Roberts & Pick, 2004). Biometric security technology has complex characteristics that often make the process of organizational adoption decisions difficult. Perceptions of a specific security technology, its effectiveness, reliability, and the need for the technology and its cost-effectiveness are important elements in the decision to recommend the technology to an organization (Craig & Hamidi-Noori, 1985; Ettlie, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004). Additionally, organizations are increasingly attentive to the cost of security and demand that IT security expenditures be proportionate to IT security risks (Center for Digital Strategies, 2005; Lanzi, 2002; Lawlor, 2005; Lesk, 2003; Levine, 2004; Richards, 2002; Shore, 2004; Verton, 2003).

Dynes, Brechbuhl, and Johnson (2005) explored the main drivers of private sector organizational adoption of IT security through a field study of a Fortune 500 manufacturing firms and four of its direct suppliers. They found that the primary driver of the firm's selection and adoption of information security was the IT security manager's recommendations on how best to protect their firm's IT assets. In information technology, biometrics is considered as the science of measuring, recording, and applying physical characteristics for the purpose of identification. Unlike traditional security measures, such as passwords and ID cards, biometric systems base authentication on physical characteristics that cannot be shared, lost, or easily compromised. Biometrics is used as a form of identity access management and access control. Biometrics can be defined as follows: Any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual (Rand, 2003, p.1).

Generally, Biometrics can be shaped into physiological Biometrics includes Facial Recognition, Fingerprint Recognition, Hand Geometry, Iris Recognition, DNA etc, measure the inherent physiological characteristics of an individual and behavioral Biometrics includes Keystroke Dynamics, Voice Recognition, Signature Recognition, measures the characteristics that are acquired naturally over a time.

Facial recognition technology identifies people by analyzing features of the face not easily altered—the upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth. Face appearance is a particularly compelling biometric because it is one used every day by nearly everyone as the primary means for recognizing other humans. Because of its naturalness, face recognition is more acceptable than other biometrics (Bolle, Connell, Pankanti, Ratha, and Senior 2004, p. 36). Fingerprint recognition technology extracts features from impressions made by the distinct ridges on the fingertips. The fingerprints can be either flat or rolled. Hand geometry scans refer not to handprints or to any analogy of fingerprints but rather to the geometric structure (or geometric invariants) of the human hand (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Iris scan technology uses the unique pattern formed by the iris – the colored part of the eye bounded by the pupil and the sclera – to identify or verify the identity of individuals (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). The iris pattern is remarkably unique, for even in the same individual, no two irises are alike (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Deoxyribo Nucleic Acid (DNA) one-dimensional ultimate unique code for ones individuality, except identical twins has identical DNA patterns. DNA sampling requires a form of tissue, blood or other bodily sample.

Keystroke technology examines such dynamics as speed and pressure, the total time taken to type particular words, and the time elapsed between hitting certain keys (Rand, 2003, p.5). Signature recognition authenticates identity by measuring handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and pressure flow. Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. This is mostly used for verifying user access over a telephone. Voice recognition biometrics "utilizes the distinctive aspects of the voice to verify the identity of individuals" (Nanavati, Thieme, & Nanavati, 2002, p. 87).

3. Objectives of the Study

The focal point of this study is to investigate the factors that influence managers to recommend biometric security technologies in their organizations. To achieve this objective the following specific objectives are outlined:

i. To elucidate the likelihood of biometrics technology in corporate management policy and business.
ii. To clarify the implications of biometrics technology in the corporate sector of Bangladesh.
iii. To analyze factors affecting the selection of appropriate biometrics technology in organizations.

4. Methodology of the Study

In light of the objectives of the study, the paper has been designed to illustrate the use of biometric security solutions in corporate sectors of Bangladesh. To this end an extensive literature survey has been conducted. The study is based largely on secondary data from published sources including websites of different organizations. Data and information from secondary sources were collected by consulting various relevant journals, studies conducted by various donor and development agencies, and publications of Information Technology Review,

International Biometric Group (IBG) etc.

5. Application of Biometrics in the Corporate Management Policy and Business:

Comparing biometric technology to other point of service and workforce management technologies, it may not initially be the least expensive option, but has proved time and time again to provide higher return on investment, increased employee productivity and enhanced customer loyalty. Today's world business organizations use the biometrics for creating a new horizon at the following business areas:

- **Buddy Punching:** When a business owner elects to use biometric technology for time and attendance, they essentially draw a line in the sand that demonstrates their commitment to stop buddy punching lower payroll inflation and boost employee productivity by eliminating unnecessary time spent clocking in/out and reconciling paper timesheets. Biometric solutions not only eradicate the costs associated with buddy-punching but also increase employee accountability with the provision of a concrete biometric audit trail, resulting in a more productive and efficient work staff (Trader, 2010a).
- **Increased productivity:** Only two words are the magic potion that all retailers seek. They are the secret sauce that lower expenses and drive revenues higher. The grease that makes the wheels of the business turns faster. Those two words are: increased productivity. All retailers seek it. (Trader, 2010b). Implementing biometric technology will directly lead to increased employee productivity.
- **PC-based biometric time clock software**: A PC-based biometric time clock software helps employers reduce unnecessary labor costs, ensure compliance, and increase employee productivity. An affordable and flexible PC-based biometric time clock software solution designed to help reduce payroll error rates, reduce unnecessary labor costs, ensure compliance, and increase employee productivity by eliminating buddy punching (Trader, 2013).
- **Membership management**: Modern day membership management software is designed to help create efficiencies that antiquated methods simply can't provide. In an effort to eliminate ID cards, prevent identity fraud, and create a more convenient user experience, many membership management facilities are evaluating vascular biometrics (finger vein and palm vein) for identification because of the distinct advantages it offers (Trader, 2012)**.**
- **A Surveillance Society:** For example, one sat in Heathrow waiting for an early morning departure for a business trip. Sipping in his coffee, he looks casually around trying to spot the cameras. They're cleverly hidden. Is he being watched? Doubtful. Is he being recorded? Almost certainly.
- **Superior customer service platform:** All businesses strive to create a loyal customer base. Loyal customers not only bring repeat business, but they also act as own army of evangelists, telling their friends, coworkers, family and even strangers to buy from satisfied establishment. The dawn of social and digital media has had a huge impact on communication for loyal customers, providing them with a platform and a seamless distribution network to sing their praises and draw attention to business through reviews, recommendations and opinions. Usually, this requires a superior customer service platform that quickly and efficiently responds to customer requests, complaints and issues. Coupled with that is normally a campaign that rewards customers for purchases and provides them with incentives to purchase more through discounts and special offers. It may also establish a referral program which encourages loyal, happy customers to refer their friends, family or co-workers to buy products or use services in return for a finder's fee or a discount on an upcoming purchase. There are a million and one initiatives that can concoct and put into action to nurture customer loyalty, but often times the secret to consistently creating and maintaining loyal customers lies within their experience and interactions while they visit frequently buying place of business. (Trader, 2010).
- **Biometric technology help boost operational efficiency**: Operational efficiency is – what occurs when the right combination of people, process, and technology come together to enhance the productivity and value of any business operation, while driving down the cost of routine operations to a desired level. The end result is that resources previously needed to manage operational tasks can be redirected to new, high value initiatives that bring additional capabilities to the organization. Biometric technology for time and attendance resulting in a massive boost in operational efficiency. This technology eliminates the need for payroll staff to input data and reconcile discrepancies enabling them to allocate time to other initiatives that were more productive (Trader, 2011).

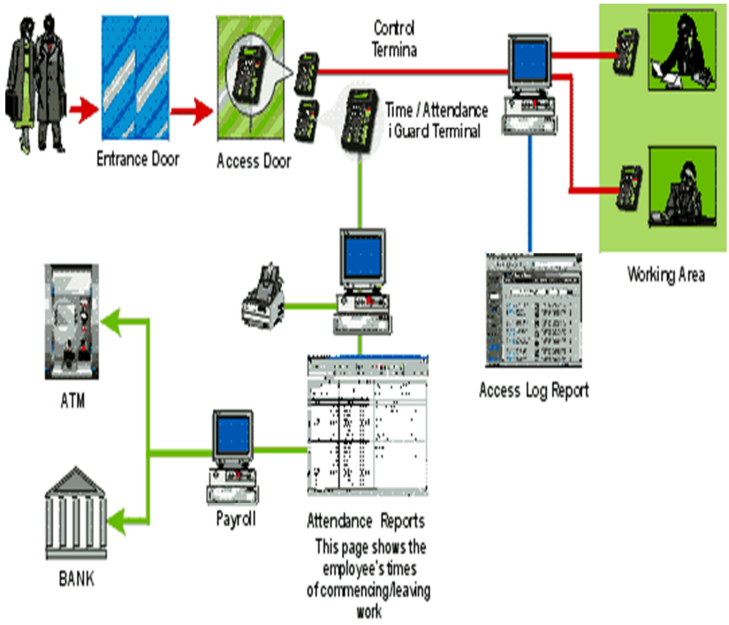
6. Implications of Biometrics Technology in the Corporate Sector of Bangladesh

Biometrics technologies are used in the corporate sector of Bangladesh by different ways as described below:

- **Physical Access Control:** Biometric systems can be used to complement or replace badges and keys in controlling access to entire facilities or specific areas in any organization. Biometric ID badges are widely used in different industries and organizations in Bangladesh such as- HeidelbergCement

Bangladesh Ltd., GrammenPhone, Banglalink, Robi, Airtel, GLAXOSMITHKLINE Bangladesh Ltd. etc. Id badges contain unique code to identify authorized clients.

- **Banking and Financial:** In banking sector, biometric devices are also used in Bangladesh. In ATM booth of HSBC Bank, fingerprint recognition is used for identifying authorized clients.
- **Advanced Time and Attendance Solutions:** Biometric time clock systems usually utilize fingerprint recognition for the employees to "mark in" or "mark out". Many organizations are now able to verify the time and attendance of their employees by using biometrics technology. Now employee labor theft is minimized and business profitability is maximized by using biometric time and attendance systems in a number of ways.



- **Organization's Security:** Biometrics can be used in Bangladesh for ensuring organization's security such as- improving entry security, strengthening border security, in travel documents, visas and in preventing ID theft.
- **Mobile Biometrics:** Mobile Biometrics systems can be implemented in Bangladesh that helps public officials - access to fingerprints, facial/iris images and data records, across agency, jurisdictional and country boundaries.

7. Salient Criteria for Choosing the Right Biometrics Technology

Key criteria for selecting the appropriate biometrics technology include:

- **Accuracy:** Accuracy is considered as the basic measure of the biometrics technology. Yet, biometrics accuracy often comes with a price - in the form of "false negatives" or improper rejection of individuals who should have been successfully authenticated and require manual resolution.
- **Maturity:** In order to ensure long-term availability and continued enhancement of biometrics technology as a national system, the selected biometrics technology must have "legs," in the form of a track record of success and wide industry acceptance. A "bleeding edge" biometrics solution, even if it's potentially more effective, may never get out of pilot.
- **Cost-Effectiveness:** An obvious consideration is the cost of equipment and training. The cost of implementing a biometric security system is fairly large, which is may be why we do not see them being used on a wider scale today. Current biometric solutions are very costly making and very expensive for the normal user. Most solutions also require extra gadgets, which would also increase the costs. However, prices for these devices as well as for the biometric application program interfaces are coming down.
- **Scalability:** A national system must be able to quickly and accurately verify that the biometrics data for a new enrollee aren't already stored under a different name, which means matching against the entire database of millions of records. The selected biometric approach must possess scalability of authentication capability.
- **Ease of Use:** No technology will be widely adopted unless it's easy to use. Otherwise, employers and employees find confusing, cumbersome or time-consuming may not even make out of pilot, even if it is more accurate.
- **User Acceptance:** A fixed national system will depend on employees to willingly provide the selected biometric for initial enrollment and ongoing verification.

The table helps to rank the relative strength of each of these criteria for the most common biometrics technologies in comparison with smart card, as High (H), Medium (M) or Low (L). Of the different types of commercially available biometrics solutions, finger biometrics is unquestionably the most appropriate for new hire identity verification.

	Finger	Iris	Smart Card	Face	Vein
Accuracy	H	H	M-H	M-L	M
Cost-Effectiveness	H	L	L	H	M
Maturity	H	L	M	M-L	L
Scalability	H	H	H	M	L
Ease of Use	M-H	L-M	L	H	M-H
Public Acceptance	M-H	M	M	M-H	M-L

Figure 1: Comparison of Smart Card and Common Trait-Based Biometric Technologies
Source: BIO-key International, Inc., 2010

Conclusion

In a world where freedom, security and justice is recognized as paramount to peace and prosperity, biometrics can enhance the freedom of the individual by ensuring the security and well being of citizens from all nations. Today, biometric technology is capable of providing a sophisticated technology that can ensure a most secure way of making profit through minimizing enormous unnecessary costs. Besides, biometrics can provide an effective measure against fraud and identity theft in different areas such as personal access (e.g., buildings, computers), banking security, business-to-business transactions and e-commerce. Biometrics can be used by various organizations to increase security levels and protect their data and patents. But in reality, it demands a multifaceted arrangement to maintain this technology. It also demands superior and highly experienced personnel to control this technology and provide enough benefit to the organization. Nonetheless, considering this technology through ensuring a pool of experienced and skilled employees can ensure a high profit, a high security, and a high performance rather than other conventional technologies used in the organizations. Without doubt the era of biometrics is here and the technology will directly affect everyone over the next few decades. Purchasing biometric scanners and other devices can provide an organization a bloodthirsty rim over others and make it accountable towards big profit earning.

References

BIO-key International, Inc. (2010). *Reducing Illegal Employment through the Use of Biometrics: Options and Recommendations.*

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., & Senior, A.W. (2004). Guide to biometrics. New York: Springer-Verlag.

Center for Digital Strategies (2005). Information security field study. Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business, Dartmouth University. Retrieved August 27, 2005, from http://mba.tuck.dartmouth.edu/digital/Research/ResarchHighlights/Security.

Chirillo, J. & Blaul, S. (2003). Implementing biometric security. Indianapolis, IN: Wiley.

Craig, R. & Hamidi-Noori, A. (1985). Recognition and use of automation: A comparison of small and large organizations. Journal of Small Business and Entrepreneurship, 3(1), 37-44.

Dynes, S., Brechbuhl, H., & Johnson, M.E. (2005). Information security in the extended enterprise: Some initial results from a field study of an industrial firm. Working Paper Series 05-1.

Ettlie, J.E. (2000). Managing technological innovation. New York: John Wiley & Sons. Ettlie, J.E. (1986). Implementing manufacturing technologies: Lessons form experience. In D.D. Davis (Ed.), Managing Technological Innovation. San Francisco: Jossey-Bass, 72-104.

Ettlie, J.E. (1986). Implementing manufacturing technologies: Lessons form experience. In D.D. Davis (Ed.), Managing Technological Innovation. San Francisco: Jossey-Bass, 72-104.

Gerwin, D. (1982, March-April). Do's and don'ts of computerized manufacturing. Harvard Business Review, 60(2), 107-116.

Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth. Retrieved August 26, 2005 from http://mba.tuck.dartmouth.edu/digital/Research/AcademicPublications/InfoSecurity.pdf

Gunn, T.G. (1982, September). The mechanization of design and manufacturing. Scientific American, 115-130.

Jain, A. K.; Ross, Arun; Prabhakar, Salil. (2004), "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology 14th (1): 4–20, doi:10.1109/TCSVT.2003.818349.

Lanzi, S. (2002, June). Determining worthwhile IT security efforts. Pulp & Paper, 76(1), 25-26.

Lawlor, M. (2005, February). Debunking information security myths. Signal, 59(6), 39-42.

Lesk, M. (2003). The mindset of dependability. Communications of the ACM, 46(1), 136.

Levine, L. (2004, March). Cost-justifying managed security for financial institutions. Community Banker, 13(3), 64-65.

Liu, S. & Silverman, M. (2001). A practical guide to biometric security technology. IT Pro, 27-32.

Matyáš, V. & Riha, Z. (2003, May/June). Toward reliable user authentication through biometrics. IEEE Security & Privacy, 45-49.

Meredith, J.R. & Hill, M.M. (1987, Summer). Justifying new manufacturing systems: A managerial approach. Sloan Management Review, 28(4), 49-61.

Nanavati, S., Thieme, M., & Nanavati, R. (2002). Biometrics: Identity verification in a networked world. New York: John Wiley & Sons, Inc.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

Putnam, R.G. (1987, Winter). Selling modernization within your company. COMMLINE, 13.

Rand, Biometrics (2003). Retrieved April 25, 2009 from http://rand.org/pubs/documented_briefings/DB396.pdf

Richards, N. (2002). The critical importance of information security to financial institutions. Business Credit, 104(9), 35-36.

Reynolds, P. (2004, December). The keys to identity: As healthcare organizations strive for greater security, some are using a very personal approach in the form of biometrics. Health Management Technology, 25(12), 12-16.

Roberts, G.K. & Pick, J.B. (2004). Technology factors in corporate adoption of mobile cell phones: A case study analysis. Proceedings of the IEEE 37th Annual Hawaii International Conference on System Sciences, 9(9), 90287-90296.

Shore, J. (2004). Security summit. Network World. Retrieved August 25, 2005 from http://www.networkworld.com/cgi-bin/mailbox/x.cgi.

Trader . J. (2012). Finger Vein Biometrics Identification for Membership Management Software

Trader . J. (2010a). The Top 15 Reasons To Use Biometric Technology In Workforce Management And Retail Point Of Sal.

Trader . J. (2010b). The Top 15 Reasons To Use Biometric Technology In Workforce Management And Retail Point Of Sal.

Trader.J. (2013). The Top 15 Reasons To Use Biometric Technology In Workforce Management And Retail Point Of Sal.

Trader.J.(2012). Finger Vein Biometrics Identification for Membership Management Software.

Trader . J. (2010). The Top 15 Reasons To Use Biometric Technology In Workforce Management And Retail Point Of Sale – Reason #6 – Build Customer Loyalty.

Trader . J. (2011). The Top 15 Reasons To Use Biometric Technology ITn Workforce Management And Retail Point Of Sale – Reason #10 – Boost Operational Efficiencyanagement And Retail Point Of Sal.

Verton, D. (2003). Scare tactics no longer guarantee security funding. Computerworld, 37(41), 10.

Woodward, J.D., Orlans, N.M., & Higgins, P.T. (2003). Biometrics. New York: McGraw-Hill/Osborne.

Zhang, D. (Ed.) (2002). Biometric solutions for authentication in an e-world. Boston: Kluwer Academy

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar