Lampyrid 2023: Volume 13, 90–96
ISSN: 2041-4900
https://lampyridjournal.com

Study the Impact of Adopting Biometric Technology Authentication Systems in Organizations

Monika Nagar, Dr. Akansha Verma
RKGIT, Ghaziabad, India,
BM Group of Institutions Farrukhnagar, Gurgaon, India,
monika91nagar@gmail.com, drvermakansha7@gmail.com

Abstract
Identification and access is a impression that has developed over time as the requisite to constantly detect individuals and grant access to confidential and sensitive data has become so important. Its impact can be felt in most organizations, specially multinational corporations engaged in top-secret research related to security-related pharmaceuticals, technology, power, and human biology. Recent vulnerabilities have highlighted the significance of extending validation protocols in sensitive areas of the economy for instance financial services and banking. Furthermore, new regulatory necessities for secondary authentication mechanisms emphasize the usage of biometric technology as an optional but reliable means of authentication. The focus of this research is to examine the impact of introducing biometric authentication systems within an organization. This study uses a secondary (exploratory) research methodology, a purely research study examining the implications and implications associated with the adoption of biometric systems within organizations. Managers of these institutions say their intentions to introduce competitive factors are determined by the organizations financial resources and perceived advantages related to technology. This study expands our understanding of the recruitment literature by showing how structural factors influence organizational actor decisions and by applying recruitment theory to a new technology, biometrics. The integration of these biometrics has increased their impact and impact on organizations.

Keywords: Validation, Biometrics Technology, Substantiations, Efficiency

I. INTRODUCTION

Without a doubt, biometrics, as a technology, has become part of our daily lives, providing us with the security we requisite. As termed by Margaret (2017) "Biometrics is the statistical dimension and analysis of a person's exclusive physical and behavioral features. "Biometric technology is specifically used for two main purposes: identification as well as access control, two processes that effort together to deliver security at diverse levels. It also depends on the type of embedded biometrics to be used. The applications of biometrics are abundant and span diverse industries, ensuring security for dissimilar entities. The outcome and influence of biometric incorporation on our lives is that it can enhance security, open up new areas to look at for further research, and too highlight the statistic that the human body people are much more progressive than we can envisage and possible with emerging technologies like biometrics. Current claims and effects are supposed to foresee future effects and waves on our daily lives. Biometrics is the Greek expression made up of two terms, biological and metric. Bio means life and metric means measurement. Biometric system means a system built on physiological or behavioral characteristics, where explicit measurements are preserved as specimens to act as tokens to confirm individuality. Physiological features embrace hand or finger imaging, facial features, gait, palm shape, and IRIS recognition. Behavioral traits are erudite or acquired traits, such as dynamic signature verification, voice verification, and typing dynamics.

Biometric system, an identification system that built on human physiological or behavioral attributes (e.g. iris, fingerprint, voice), are drawing great concern due to their accuracy. , responsive and easy to use with identification and authentication functions according to L. Coventry, A. De Angeli and G. Johnson, (2003). According to Dugelay S. Marcel, (2017); today, biometric authentication systems are very accurate and easy to use, which translates into superior user-friendliness on the technical side of the system. Biometric technology has been widely studied as a method of security management and control, and there are many documents from academic and trade journals documenting the many benefits and problems encountered by users. When applying this technology. This section looks at some of the features and related applications of this technology to highlight the important factors that promote or hinder adoption. As a result, Harris and Yen conclude that biometric technology provides a level of security unmatched by traditional authentication methods. Ahmed (2005) build on the premise of biometric superiority by developing a private key security enforcement system that is a non-biometric security protocol, with biometric technology.

Along with the growing interest in the security assistances of biometric technology, there is furthermore growing interest in studying privacy concerns. Zorkadis and Donos (2004) reviewed the growing regulatory apprehensions allied to the personal nature of biometric data. This study builds on previous work by Prabhakar, Pankanti and Jain (2003) that addresses three explicit concerns: inadvertent functional coverage, unpremeditated application range, and secret identity. Zorkadis and Donos have suggested a number of applicable guidelines that they recommend must be followed in order for biometric systems to comply with applicable legislation. They also propose a manner to secure an individual's info stored in a biometric database. The researchers concluded that in order for biometric data to be kept confidential and to comply with the rules of applicable law, the following conditions must be met: (1) biometric identification data can merely be used for the purpose for which it is used. initially collected, (2) the data is less likely to be accessed by others for additional processing if the data is store in a device retained by the data subject (for instance a smart card), and (3) IT staff have to effusively aware of customers' legal honesties to biometric information in addition to be adequately trained in the management of proper security technologies. In accumulation, Jain, Nandakumar, and Nagar (2008) scrutinized existing biometric template fortification plans to improve the safety of biometric authentication with identity management systems. They addressed the risk of attacks on stowed biometric templates, nonetheless established that a single protection system might not be adequate in large-scale deployments. User confidentiality is a recurring theme in exploration that has observed biometric technologies.

Alterman (2003) and Langenderfer and Linnhoff (2005) have shown that subsequent extensive deployment of biometric executions must have to offer a means to protect data from misappropriation. Ratha, Connell and Bolle (2001) termed the susceptibilities of biometric systems and in what way to safeguard them with methods which if they executed, would reduce the risk of statistics being stolen. Sticha and Ford (1999) studied how biometric technology could be used to combat duplicate registration and fraud in food stamp programs. They furthermore find that the biometric technology used need to be user-acceptable, accurate, fraud-proof, and have a fast retort time. Jain and colleagues (2004) reviewed pattern recognition technologies and recognized privacy, accuracy, security as the key issues faced by organizations when employing the technology biometrics. Elliott and colleagues (2004) acknowledged that they consider being imperative dynamics affecting the accuracy, consistency, and practicality of biometric technology. Explicitly, they point out that the atmosphere in which the biometric scanner is located, the eminence of the images attained, and the choice of device that used for acquire the individual's biometric identification are all essential aspects in the image of an individual which will affect the way technology works as expected. These works pull consideration to numerous factors which are significant operational deliberations in the espousal of biometrics.

II. BIOMERTRIC SYSTEM: ADVANTAGES AND COMPONENTS

2.1 Advantages of Biometric

- Existing security contexts are rare and built on exclusive passwords, unique identifiers; many new biometric approaches aid us to attain accurateness and precision in understanding the concept.
- Using the native features like retina scans, fingerprints to form a distinctive and diverse proof system under different circumstances. The process can’t be imitative from one to another system because everyone has their own set of features.
- Biometric systems affect an individual and an entire organization where an individual operator can be concomitant with a specific occurrence. Biometrics is deliberated as transparent and clear and it is generally expedient for security devotions, mainly in the case of surveillance systems in schools, colleges and offices.
- The main use of biometrics is safety and also simplicity as it provides numerous innovative methods for retrieving the database of registered people. The software is easy to use and can be prepared in several steps.
- Biometric framework today is being effectively presented in different organizations and is reflected the best among recent tools due to the help of these corporations and administrations has the ability to easily get rid of expensive physical heads. In this case, it’s also advantageous for those who cannot process physical data competently and have no proficiency in letters, words, images, etc. making it difficult for them to prepare reports.

- Nevertheless, there would be no obligation for biometric characteristics without data duplication, distortion of records and illegal data sharing. There is no necessity for individual ID cards and their maintenance, as in the event of ID card loss, this can cause problems for customers' security approaches.

2.2 Components of Biometric System

To fully comprehend a classic biometric system, it is necessary to scrutinize the modules of a biometric device. The modules of a biometric device essentially form the basis of a biometric system including:

- Sensor

It's something that collects an individual's biometric data, be it a fingerprint scan, voice or voice prompts, an iris scan, or some other form of biometric scan. Data is collected and transformed into a digital format.

- Data storage

This is where the biometric records of individuals or certified users is located. Biometric scanners are used to scan individuals, take biometric measurements, and then convert the resulting data into a digital format. The data is then stored in the database

- Matching algorithm

This is used for compare the data previously stored in the database thru the new digitized data. Verification is performed on the individual to identify authorized users.

- Decision making process

This process is used to elect the next validation step. If the user is authenticated, the device will grant entree within system.

III. IMPLEMENTATION STRATEGIES

While some biometric technologies have been in widespread use for a decade, restricted research has looked at the adoption of biometrics in organizations. Most of literature related to this expertise has been described and specified, giving theoretical recommendations for application and use. They proposed a stratagem for decision-making procedure using a step-by-step approach to develop a concrete business case for implementing biometric technologies. Riley and Pearson, (2005) have acknowledged how biometric technology can become a appreciated instrument in mitigating an organization's risk depending on the level of threat and the type of biometrics used. Calderon (2005) made commendations to organizations seeing the enactment of biometric authentication systems by outlining the disregards, limitations of the company. Each organization must have to consider Biometric technology. Perhaps due to the fact that automated biometric technology is new, limited research has been done on organizations already using biometric technology. In a case study of biometric systems deployed, Heracleous (2006) investigated the role of biometric technology and how it can drive service fineness, efficiency, and safety in the service industry. Organization ought not to deploy a fresh technology just to do so; in its place, administrations must be able to align strategy and innovative strategy.

Coventry and colleagues (2003a, 2003b) studied customer-focused usability regarding iris scan validation at automated teller machines (ATMs). This study looked at a prototype that used in field testing, and the investigators initiate that consumer input in addition to acquaintance to prototype testing of the technology provides detailed information on how to advance user approval of biometric systems. Likewise, Breckenridge (2005) looked at the deployment of biometric technology in South Africa. He suggested that previously the US embarks on a plan to implement a widespread rollout of the biometric system, it would be wise to consider the lessons which can be erudite from South Africa's difficulty in moving warehouses and Paper-based government archives to biometric archives. . For ex., Breckenridge cited the loss of power by local officials in the data-driven system, along with the escalating data-related privacy concern in the security of biometrics data. While prescribing strategies and regulations are helpful, it is vital to comprehend how the process applies in a theoretical context. The following section assessments the limited experimental and theoretical study that has been done to test the application of biometrics.

IV. PRIOR BIOMETRIC ADOPTION RESEARCH

An imperative contemplation in the embracing of an organization's technology is the acceptance of the technology by each of its stakeholders. Consequently, most of research investigative the adoption of biometrics has dedicated on individual attitudes and perceptions. For instance, James et al. (2006) used the Technology Acceptance Model (TAM) to regulate intent to use security technologies in the form of biometric technologies. The results specify that apparent security needs and perceived ease of use have a positive influence on individuals' perceptions of the usefulness of biometric devices, but the possibility of physical compromise is Device perception has a negative impact on intention to use. Jones (2007) also used TAM in a pilot study of business students to recognize users' perceptions of digital identity technology, including biometric technology. Inclusive, they conclude that there is great ambiguity regarding authentication technologies and that these worries negatively affect adoption.

Moody (2004) studied the factors that led to the slow implementation of biometric technologies. In accumulation, she also tries to determine the public perception of biometric technology. She finished that her survey respondents were not equipped to engage in profitable use of biometric technology owing to a misunderstanding of how the technology workings and lack of revelation of technology (94% of respondents were Survey; participants have not ever used a system biometric tool). Chandra (2008) took a similar method to Moody's when reviewing people's feelings about the probable uses and restrictions of biometrics in healthcare. They find that health-care providers (physicians, nurses, and related health specialists) and customers have worries about confidentiality and the prerequisite to limit their ability to provide information they believe. Venkatraman (2008) used a case-study methodology to identify concerns and attainment influences surrounding the use of biometrics in banking. They found that although biometric technology is appealing to many banking institutions as a solution to safety threats, there is still a reluctance to adopt the technology because of social technology concerns.

In summary, most of research inspecting biometric adoption and use is vivid and emphases on technology characteristics. No study has empirically studied the implementation of biometrics in a large, illustrative sample of organizations.

Additional, though numerous researchers have conversed the role of biometrics in security applications for financial associations, no methodical empirical research has been apply to reviewing the role of organizational features, contextual aspects, and perceived aids of the technology in this or associated industries.

V. ORGANIZATIONAL ADOPTION RESEARCH

The innovation decision-making process comprises a series of varieties and activities that made over time as individuals or members of an organization estimate a new idea and decide whether to integrate innovation into practice or not (Rogers 2003). The critical stage of the innovation decision-making process is at which an association accepts or rejects innovation and thus has multiple perspectives on how innovation affects efficiency, persistence, growth and a firm's performance (Gopala Krishnan 1997).

The IT innovation acceptance literature comprises a wealth of research which can be used to notify ongoing applied research. In a comprehensive review, Jeyaraj and Lacity, (2006) examined 51 previous publications on IT adoption by organizations between 1992 and 2003 and found that among the independent variables used Most often, the best predictors of organizations' IT embracing include Pressure and size of the organization. In addition, they suggest that the features of organizations adopting the technology must be inspected in future studies of organizational adoption. Likewise, Frambach & Schillewaert , (2002) also suggest that future research on adoption will integrate adopter characteristics. Precisely, they note that in addition to individual and administrative factors, whichever factor used to determine whether a latest innovation should be adopted and implemented begins with considerate the customer potential and factors influencing their adoption decisions. An important mutable they identified was the nature of the organizational culture in expressions of innovation (Deshpande & Webster, 1993; Srinivasan & Rangaswamy, 2002). This is related to the outcomes found by Deshpande and colleagues, where organizational innovation is considered an vital factor of organizational performance. Grandon & Pearson (2004) observed the factors affecting the adoption of e-commerce in small and medium-sized enterprises converging on the perception of senior management about the application of e-commerce technology. The factors they scrutinized included administrative readiness, external pressures, usefulness, and usability of TAM concepts (Davis 1989). They find that exterior pressure, seeming ease of use, and apparent efficacy were important when persuading adoption, but legislative readiness was not. In an empirical study on factors contributing to the embracing of electronic processes by service companies, Tsikriktsis & Frohlich, (2004) added the notion of exterior pressure to their study model. They describe exterior pressure as finest defined as the “train” effect, in which challengers and further market players follow a prominent innovator in technology adoption. Other dynamics in their model include expected aids, market access, interior barriers, and customer barriers. All factors except customer barriers have a significant effect on adoption. The investigators determined that the forces driving performance far outweigh the barriers that prevent organizations from adopting processes.

Srinivasan and his colleagues (2002) considered the adoption of innovative technologies by administrations. This includes factors for instance technological deviousness, institutional (stakeholder and competitive) pressures, corresponding assets, supposed usefulness, administrative innovation, and managing advocacy. Senior administration advocacy has been defined by investigators as "the leadership team's effort to highlight the prominence of the organization's ability to respond to new technologies". This turned out to be an important factor in the expansion of a new structure: technological speculation. In a related study by Ramamurthy & Crum, (1999), executive support was found to be obligatory to deal with competitive compressions and facilitate the attainment of financial resources. Appropriate when companies are faced with decisions regarding the adoption of innovative technology. For senior management support, another influence perspective is a descriptive study of the impact of management impact and the interplay amid perceived management behavior and worker characteristics when promote innovative use by consumers (Leonard-Barton, 1988). This study shows that although there is no direct association between management actions to promote use and ensuing increase in use, noteworthy associations were detected when they were used. Taking into account the refereeing role of the manager's personal characteristics and intervention skills. Therefore, if an worker already owns an innovative personality, the influence of administration will be less significant. Also, if an employee is hesitant about using a new innovation, it's important to encourage management. This evaluation provides a summary of a number of illustrative applied studies that have been performed over the past two decades. Although many variables have been considered in these studies, three general concepts stand out as having a significant impact on adoption: organizational pressure to adopt, organizational willingness to accept, and alleged benefits of innovation to the organization.

VI. CONCLUSION

In conclusion, the effectiveness and impact of biometric technology cannot be overemphasized, it is also a part of our daily lives. The importance of usability measurement is heightened as biometric systems become more prevalent in everyday life. Biometric technology will become a standard in the future as more industries begin to make every effort to fully integrate it into their respective businesses to improve and enhance the services provided. and revolutionize business processes. This study suggests that it is important to consider the nature of the technology in conjunction with company characteristics and industry position when considering stand-alone technologies such as biometrics. Additionally, it is important to realize that biometrics, as a security technology, does not have the “network” impact that technologies such as EDI have; therefore, managers may have difficulty quantifying the benefits to their organization. As Dutta, (2002) have noted, senior managers are largely not involved in safety decisions because they often perceive little or no association between safety and profitability. As a result, the adoption of biometrics would be more likely to be positioned as a tactical security response to an impending regulatory or threat rather than a broader and fundamental strategic direction. In other words, another important finding of our study is that it highlights that the nature of the technology and the context of other external regulatory pressures are important when determining whether senior management support or not to make technology adoption decisions (e.g. Weil and Aral 2006). On a broader note, as Dutta and McCrohen (2002) have pointed out, many senior executives see security decisions as an IT function; therefore, for senior management to support the adoption of security technologies such as biometrics, it is important to change existing attitudes about the role of security technologies in the organization. In this regard, our results are consistent with the recommendations of Dutta and McCrohen and Austin and Darby (2003) to encourage senior management to participate in decisions regarding the adoption of processes and security technology. Biometric innovation is certainly a global ICT system that can be used to improve employee engagement. In this sense, this survey has come to the conclusion that the biometric innovation framework is the best framework that can solve the problem of employee expectations in associations economically.

References

[1] Ahmed, F., and M. Y. Siyal. 2005. “A novel approach for regenerating a private key using password, fingerprint and smart card. *Information Management & Computer Security* 13(1):39-54.

[2] Alterman, A. 2003. “A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology* 5(3):139–150.

[3] Breckenridge, K. 2005. “The biometric state: The promise and peril of digital government in the new South Africa.” *Journal of Southern African Studies* 31(2):267–282.

[4] Coventry, L., A. De Angeli, and G. Johnson. 2003a. “Honest it’s me! Self service verification.” Paper read at CHI Workshop on Human-Computer Interaction, Adoption Study and Security Systems, at Fort Lauderdale, FL.

[5] Chandra, A., R. Durand, and S. Weaver. 2008. “The uses and potential of biometrics in health care: Are consumers and providers ready for it?” *International Journal of Pharmaceutical and Healthcare Marketing* 2(1):22–34.

[6] Davis, F. D. 1989. “Perceived usefulness, perceived ease of use, and user acceptance of information technology.” *MIS Quarterly* 13(3):319–340.

[7] Deshpande, R., J. Farley, and F. Webster, Jr. 1993. “Corporate culture, customer orientation, and innovativeness in Japanese firms: A quadrad analysis.” *Journal of Marketing* 57: 23–27.

[8] Down, M. P., and R. J. Sands. 2004. “Biometrics: An overview of the technology, challenges and control considerations.” *Information System Control Journal* 4:53–56.

[9] Elliott, S., E. P. Kukula, and N. C. Sickler. 2004. “The challenges of the environment and the human/biometric device interaction on biometric system performance.” Paper read at International Workshop on Biometric Technologies—Special Forum on Modeling and Simulation in Biometric Technology, at Calgary, Alberta, Canada.

[10]Frambach, R. T., and N. Schillewaert. 2002. “Organizational innovation adoption: A multi-level framework of determinants and opportunities for future research.” *Journal of Business Research* 55(2):163–176.

[11]Gopalakrishnan, S., and F. Damanpour. 1997. “A review of innovation research in economics, sociology and technology management.” *Omega, International Journal of Management Science* 25(1):15–28.

[12]Grandon, E., and M. Pearson. 2004. “Electronic commerce adoption: An empirical study of small and medium US businesses.” *Information & Management* 42(1):197–216.

[13]Harris, A. J., and D. C. Yen. 2002. “Biometric authentication: Assuring access to information.” *Information Management & Computer Security* 10(1):12-19.

[14]Heracleous, L., and J.Wirtz. 2006. “Biometrics: The next frontier in service excellence, productivity and security in the service sector.” *Managing Service Quality* 16(1):12–22.

[15]James, T., T. Pirim, K. Boswell, B. Reithel, and R. Barkhi. 2006. “Determining the intention to use biometric devices: An application and extension of the technology acceptance model.” *Journal of Organizational and End User Computing* 18(3):1–24.

[16]Kleist, V., R. Riley Jr., and T. Pearson. 2005. “Evaluating biometrics as internal control solutions to organizational risk.” *Journal of American Academy of Business* 6(2):339–343.

[17]Langenderfer, J., and S. Linnhoff. 2005. “The emergence of biometrics and its effect on consumers.” *Journal of Consumer Affairs* 39(2):314–338.

[18]Leonard-Barton, D., and I. Deschamps. 1988. “Managerial influence in the implementation of new technology.” *Management Science* 34(10):1252–1265.

[19]L. Coventry, A. De Angeli, and G. Johnson, “Usability and biometric verification at the ATM interface,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*, vol. 5, pp. 153-160, ACM, Paris, France, April 2003.

[20]Margaret. R (2017) Biometrics. Available at: https://searchsecurity.techtarget.com/definition/biometrics. Accessed on the 1st of July, 2018

[21]Moody, J. 2004. “Public perceptions of biometric devices: The effect of misinformation on acceptance and use.” *Journal of Issues in Informing Science and Information Technology* 1:753-761.

[22]Ramamurthy, K., G. Premkumar, and M. Crum. 1999. “Organizational and inter organizational determinants of EDI diffusion and organizational performance: A causal model.” *Journal of Organizational Computing and Electronic Commerce* 9(4):253–285.

[23]Ratha, N. K., J. H. Connell, and R. M. Bolle. 2001. “Enhancing security and privacy in biometrics based authentication systems.” *IBM Systems Journal* 40(3):614–634.

[24]Riley Jr., R. A., and V. F. Kleist. 2005. “The biometric technologies business case: A systematic approach.” *Information Management & Computer Security* 13(2):89–105.

[25]Rogers, E. M. 2003. *Diffusion of Innovations*. 5th Ed. New York: Free Press.

[26]Srinivasan, R., G. Lilien, and A. Rangaswamy. 2002. “Technological opportunism and radical technology adoption: An application to e-business.” *Journal of Marketing* 66(3):47–60.

[27]Sticha, P. J., and J. P. Ford. 1999. “Introduction to biometric technology: Capabilities and applications to the food stamp program.” In *U.S. Department of Agriculture contract no: FCS 53-3198-6- 025* (pp. 1–39). Arlington, VA: R. Lewis & Co., Inc.

[28]Tsikriktsis, N., G. Lanzolla, and M. Frohlich. 2004. “Adoption of e-processes by service firms: An empirical study of antecedents.” *Production and Operations Management* 13(3):216–229.

[29]Venkatraman, S., and I. Delpachitra. 2008. “Biometrics in banking security: A case study.” *Information Management and Computer Security* 16(4):415–430.

[30]Zorkadis, V., and P. Donos. 2004. “On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements.” *Information Management & Computer Security* 12(1):125–137.

[31]Z. Akhtar, A. Hadid, M. Nixon, M. Tistarelli, J.-L. Dugelay, and S. Marcel, “Biometrics: In Search of Identity and Security (Q & A),” *IEEE MultiMedia*, 2017.

[32]“ISO 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs),” 45: 9, The international organization for standardization, 1998.