Securing Sensitive eDatabases using Multi-Biometric Technology

Shahzad Memon[1], Syed Ghulam Sarwar Shah[2], Khalil Khoumbati[3], and Imadad Ali Ismaili[4]

***Abstract*— Governments in several countries such as Pakistan are adopting the latest information and communication technologies to increase the efficiency of organizations and services. One of the major reasons for this is to transfer and store a large amount of very important government records as eDatabases (G-eDbases) such as the database managed by the National Database Registration Authority in Pakistan. This type of data is highly confidential therefore needs to be protected from an unauthorized access. Presently, access to these databases is based on software based authentication technologies such as password based encryption schemes, which can protect from an unauthorized access to some extent. This mode of authentication access can however be compromised. It is therefore important to use more secured and reliable methods to access to the G-eDbases, which is increasingly important in the current situation of security in the country. In this paper, the authors suggest a hypothetical model of securing sensitive eDatabases using multi-biometric technology that will replace the traditional password based access scheme and prevent unauthorized access to G-eDbases.**

***Index Terms*— E-security, e-Databases, Multibiometric, Pakistan.**

I. INTRODUCTION

During the last decades, rapid adoption of Information and Communication Technologies (ICT) has increased in developing countries such as Pakistan. These modern technologies includes both hardware and software solutions, which have revolutionized and improved many traditional methods of management in both private and public sectors. Consequently, public and private organizations nowadays manage their records using databases software, store them into electronic storage devices, and provide access to the users, both locally and remotely. These electronic databases (eDatabases) are collection of organized data in a systematic way with searchable elements. This listing of information makes the search of records simple and quick. A single eDatabase may refer to a variety of sources, including periodical articles, books, government documents, industry reports, financial documents, papers at meetings, newspaper items, films, video recordings etc [1].

In addition, eDatabses are major sources of information. As an information source, thousands of users may share a single eDatabase simultaneously, and it can be made available to the users whenever the retrieval service is in operation [2]. There is no limit to the number of times a database can be searched or the number of times an item can be displayed. Unlike paper-based databases, eDatabases do not deteriorate physically, nor can they be misplaced, stolen, or vandalized [3]. Resultantly, more and more information is being published only in electronic formats and it covers virtually all areas of data such as engineering, medicine, agriculture, business, law, education and more [4]. With the Internet connectivity, it is possible to access these eDatabses from anywhere. Security of eDatabases is more critical as networks have become more open, organizations therefore increasingly face challenges in protecting confidential information contained in their eDatabases.

Traditionally eDatabases are protected from external threats using hardware/software based intrusion detection systems and firewalls. Also at application level, the authentication and authorization mechanisms such as single sign-on are considered as an effective means of providing abstraction from data layer [1, 3]. The key advantage of single sign-on capability across multiple databases and database platforms is that it stores the user's credentials i.e. login ID and password and authenticates the user to access the database. This type of security system is very fragile, especially in the government sector where a higher level of secured 'access system' is required [2, 4]. There are many possibilities to steal or guess the login IDs and passwords, which can be used by an unauthorized person at anytime and anywhere.

Biometrics technology offers a new and better approach to user authentication. Biometrics authentication is an automated method whereby an individual's identity is confirmed by examining his/her unique physiological trait(s) or behavioral characteristic(s) [5, 6]. Biometric security based systems are thus successfully deployed for different applications such as the border and immigration services, and access control systems to secured establishments. An overview of existing biometric technology is presented in the following section.

[1]Centre for Electronics Systems Research, Electronics and Computer Engineering, School of Engineering and Design, Brunel University, London, UB8 3PH, UK, email: shahzad.memon@brunel.ac.uk
[2]Department of Information Systems and Computing, Brunel University, London, UB8 3PH, UK, e-mail: sarwar.shah@brunel.ac.uk
[3]Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan, e-mail: khalil.khoumbati@googlemail.com
[4]Institute of Information and Communication Technology, University of Sindh, Jamshoro, Sindh, Pakistan, e-mail: iai_a@yahoo.com

II. BIOMETRIC TECHNOLOGIES

Traditionally, knowledge and token based security such as passwords and ID cards have been used to manage access to restricted systems [5, 6]. However, this type of security can be easily breached in these systems when a password is disclosed to an unauthorized user or an ID card is stolen. Furthermore, simple passwords are easy to guess by an impostor and difficult passwords may be hard to recall by a legitimate user [6, 7]. In recent years, biometric authentication has seen considerable improvements in the reliability and accuracy, with some biometrics offering reasonably good overall performance.

The emergence of biometrics technology has addressed the problems that plague the traditional identification and verification methods. Biometrics is automated method that refers to the automatic recognition of individuals based on their physiological and/or behavioural traits such as the recognition of the face, fingerprints, hand geometry, handwriting, iris, retina, veins and voice (Figure 1).

Nowadays, when people are regularly using passwords, biometric identification offers a suitable and attractive option in order to check someone's identity. By using biometrics, it is possible to authenticate or establish an individual's identity based on "who s/he is", rather than by "what s/he possesses" (e.g. an ID card) or "what s/he memorizes" (e.g. a password) [6].

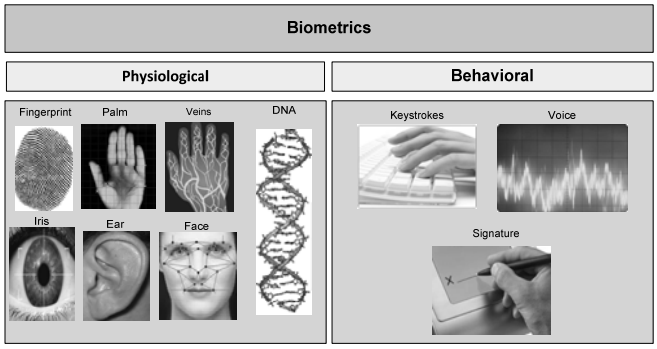

Fig.1. Human Physiological and behavioural traits.

This technology broadly includes the recording and recognition of biological and behavioral traits of an individual. It has been proved that individual biometric characteristics are unique and cannot be transferred and information related to these traits cannot be lost, stolen or forgotten [5]. Biometric solutions ensure an extremely high standard for different security applications. A biometric system offers excellent convenience and a very high level of security. Biometric technologies are becoming the foundation of an extensive array of highly secured identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secured identification and personal verification technologies is becoming apparent. Biometric-based access is capable of providing the necessary security in many contexts such as workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security [8].

Biometric systems can be uni-modal and multimodal [5]. Uni-model biometric systems are applicable in low to moderate security applications. As security needs increase and terrorists and criminals gain more expertise in biometrics technologies, uni-modal systems may not be adequate [9]. In addition, research in the biometric has proved that single biometric trait based system have to contend with noisy data, restricted degrees of freedom, failure-to-enroll problems, spoof attacks, and unacceptable error rates[10] .

Multibiometric is a relatively new approach to overcome those problems. Driven by lower hardware costs, a multibiometric system uses multiple sensors for data acquisition [9]. This allows it to capture multiple samples of a single biometric trait called multi-sample biometrics and/or samples of multiple biometric traits called multi-source or multimodal biometrics [11]. Multi-biometric systems combine the data and the features of uni-modal systems and can provide higher levels of security [12]. Multibiometric systems are therefore expected to enhance the recognition accuracy of a personal authentication system by reconciling the evidence presented by multiple sources of information [13]. The use of multiple traits of an individual for authentication thus alleviates some of these problems while improving verification performance. Multi-biometrics therefore seems to be the most convenient where higher security access is required to get an access to a system.

III. PROBLEM IDENTIFICATION

Around the world, the security measures are becoming important issues for the governments and industry. Governments for personal identification and to control access to their internal and external services and places implement various electronic systems. Since the last decade, in Pakistan many organizations, such as Government, Defense, Financial, Academic, National Identity Records and Forensic departments, have switched from manual databases to electronic databases (eDatabases). However, switch from manual databases to eDatabases adds on many features and benefits to organizations with many issues.

One of the major issues is secured access of the eDatabases. Although the authenticated users (having text based Password) and services are allowed to access important eDatabases at any time and from anywhere using passwords. In addition, they are allowed to view, edit and search the Databases. At present, the rising issues of security in Pakistan have not only created threats for the important building, places and people but also for the government eDatabses, such as database managed by the National Database Registration Authority (NADRA), in the context of unauthorized access. As these databases are stored online and/or offline so it is easy to criminally access these databases by hacking and decrypt the text-based passwords. Ensuring the security vis-à-vis access to these eDatabases from any place is important especially in the current security issues in the country.

User authentication, a key component of any eDatabase system, ensures that only those with specific rights are able to access the stored data. At this level the biometrics play an

1999-4974©2010BUJICT

essential role [2]. It strengthens protection where user authentication is needed. The biometric recognition as a means of personal authentication is focused on increasing security and convenience of use for purposes where users need to be securely identified.

IV. HYPOTHETICAL MODEL FOR SECURED ACCESS TO SENSITIVE G-EDBASES

The authors propose a multi-biometric technology based method to access G-eDbases as illustrated in Figure 2. This hypothetical model is based on four steps. In the first step, the proposed model will scan multiple biometric features of a new user who has permission to access to a G-eDbases. The multibiometric Scanning (MBS) will acquire the user's four features i.e. fingerprint, hand geometry, iris and face using multiple sensors on to the system. These four biometric traits are suggested for the model because these technologies are used in many applications and are considered as mature biometrics.

In the second step, the acquired biometric data will be sent for Multibiometric Enrolment (MBE) and then the data will be transferred for storage in Multi-Biometric template storage (MBTS). After these steps, the user becomes an authenticated person whose multiple biometric traits are stored on the system forever. Now onwards, whenever the authenticated user wants to access the system, s/he only needs to pass through the third step i.e. the verification step. The verification process will check the MBTS of the user and when found matched with a valid record, then the user will be transferred to the last step where the user will get access to the central G-eDbases stored on the Internet, intranet or LAN as well as offline access. After gaining access to the G-eDbases, the user will be able to view, edit and search the G-eDbases.

In the proposed model, the multi biometric information of authenticated user will be available permanently after the first login. The multiple biometric data will be stored in a coded template form, which cannot be easily stolen or decrypted. When an authenticated user will access the system again, the user will be verified with his/her biometric traits, which remain unchangeable.

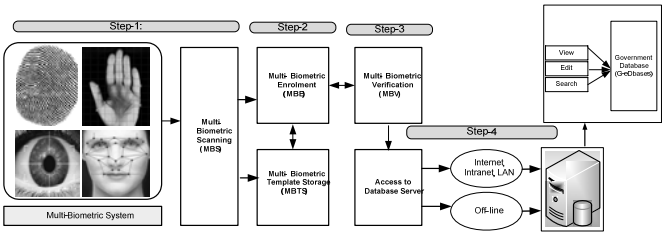

Fig.2. Multi-Biometric based hypothetical model for securing access to G-eDbases.

V. IMPLICATIONS

The one of the benefits of this system is that authenticated user needs not to remember his/her passwords all the time to login. This system will never provide direct access to a user on G-eDbases without having a multi biometric trait record on the MBTS. As a result, the Multi-biometric-based solution is able to provide security for authorized access and Governmental data privacy vis-à-vis the G-eDbases.

The physical development and adoption of this hypothetical model will be useful not only for the governmental databases but also for the databases in the private organizations in order to greatly secure and protect the databases from an unauthorized access. Implementation of the proposed model will thus meet the future challenges of security of G-eDbases in Pakistan, it is therefore important for government authorities to think and plan from now onwards to protect their databases, which are vulnerable under present set of accessing mechanisms.

The use of the proposed Multi-biometric based access to protect G-eDbases can thus be useful in countries such as Pakistan that can be adopted for federal, state and local governments, military and law enforcement agencies, national data registration organizations, health, education, land records and social services.

VI. CONCLUSION

In this paper, the authors have proposed a Multi-Biometric based Hypothetical Model for securing access to G-eDbases in Pakistan. The security situation in the country is forcing implementation of state of art and secured mechanisms and methods for accessing governmental confidential information including G-eDbases. The proposed model is based on the use of multi-biometrics technology for access authentication to the governmental data. The authors intend to develop and test the model.

VII. REFERENCES

[1] L. Duranti, "Concepts, principles, and methods for the management of electronic records," *The Information Society*, vol. 17, no. 4, pp. 271-279, 2001.

[2] T. Uemura and T. Dohi, "Optimizing security measures in an intrusion tolerant database system," *Lecture Notes in Computer Science*, vol. 5017, pp. 26-42, 2008.

[3] R. M. Stair, and G. W. Reynolds, *Principles of Information Systems*. , Boston: Course Technology, 2010.

[4] K. Thibodeau, "The Electronic Records Archives Program at the National Archives and Records Administration," *First Monday*, vol. 12, no. 7, July 2007. URL: http://firstmonday.org/issues/issue12_7/thibodeau/index.html

[5] N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou, *Biometrics: Theory, Methods, and Applications*. Hoboken, NJ.: Wiley-IEEE Press, 2010.

[6] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125-143, 2006.

[7] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky and A. Smith, "Secure remote authentication using biometric data", *Advances in Cryptology (EUROCRYPT 2005)*, In: *Lecture Notes in computer Science*, vol. 3494, pp. 147-163, 2005.

[8] A. Ross, K. Nandakumar and A. Jain, "Introduction to Multibiometrics," In: A. K. Jain; P. Flynn and A. A. Ross, Eds., New York, NY.: *Handbook of Biometrics*, pp. 271-292, 2008.

[9] J. Kiltter and N. Poh, "Multibiometrics for identity authentication: Issues, benefits and challenges," In *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2008)*, pp. 1-6, 2008.

[10] M. De Marsico, M. Nappi and D. Riccio, "Multibiometric People Identification: A Self-tuning Architecture," *Advances in Biometrics*, In: *Lecture Notes in Computer Science*, vol. 5558, pp. 980-989, 2009.

[11] A. Ross and N. Poh, "Multibiometric Systems: Overview, Case Studies, and Open Issues," In: M. Tistarelli; S. Z. Li and R. Chellappa, Eds., London: *Handbook of Remote Biometrics*, pp. 273-292, 2009.

[12] A. Rattani and M. Tistarelli, "Robust multi-modal and multi-unit feature level fusion of face and iris biometrics," *Advances in Biometrics*, In: *Lecture Notes in Computer Science*, vol. 5558, pp. 960-969, 2009.
[13] M. Monwar and M. Gavrilova, "A robust authentication system using multiple biometrics," *Computer and Information Science, Studies*, In: *Computational Intelligence*, vol. 131, pp. 189-201, 2008.