Applications of Biometrics Personal Authentication (Mobile & Computers)

G. Ramachandran, S. Kannan, G. Murali, P.M . Murali
Assistant Professor, Department of Electronics and Communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu, India
E-mail: sriramachandrang@gmail.com

T. Sheela
Associate Professor, Department of Electronics and Communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu, India

T.Muthumanickam
Head & Professor, Department of Electronics and Communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu, India

***Abstract*- Nowadays, we are talking more and more about insecurity in various sectors in addition because the computer techniques to be implemented to counter this trend: access control to computers, e-commerce, banking, etc. There are two traditional ways of identifying a private. the primary method may be a knowledge-based method. it's supported the knowledge of an individual's information like the PIN code to permit him/her to activate a portable. The second method is predicated on the possession of token. It will be a bit of identification, a key, a badge, etc. These two methods of identification will be employed in a complementary thanks to obtain increased security like in bank cards. However, they each have their weaknesses. Within the first case, the password will be forgotten or guessed by a 3rd party. Within the second case, the badge (or ID or key) could also be lost or stolen. Biometric features are an alternate solution to the 2 previous identification modes. The advantage of using the biometric features is that they're all universal, measurable, unique, and permanent. The interest of applications using biometrics will be summed up in two classes: to facilitate the way of life and to avoid scam**.

Keywords - Biometric system, Human tongue, Face and voice, PIN Password, One Time Password

1. INTRODUCTION

Multi-Factor Authentication (MFA) was proposed to supply a better level of safety and facilitate continuous protection of computing devices moreover as other critical services from authorized access by using quite two categories of credentials (Scheidt, 2006), (Bhargav-Spantzel, et al., 2007) (Banyal, Jain, & Jain, 2013). For the foremost part, MFA is predicated on biometrics, which is automated recognition of people supported their behavioural (Frank, Biedert, Ma, Martinovic, & Song, 2013), (Jorgensen & Yu, 2011) and biological characteristics (National Research Council;Whither Biometrics Committee. Biometric Recognition: Challenges and Opportunities, 2010). This step offered an improved level of security because the users were required to present the evidence of their identity, which relies on two or more various factors (Huang, Xiang, Bertino, Zhou, & Xu, 2014). the continual growth within the numbers of smart devices and related connectivity loads has impacted mobile services seamlessly offered anywhere round the globe (VNI Cisco Global Mobile Data Traffic Forecast 2016–2021., 2017). In such connected world, the enabler keeping the transmitted data secure is, within the first place, authentication (Roy & Khatwani, 2017).

2. LITERATURE SURVEY

While smart phones with sensors have made biometric technology more accessible and mainstream, giving passwords a run for their money, the transition does come with its share of challenges. One such challenge is the security risk associated with data leakages. The other challenge relates to the overall customer experience and makes it as seamless as possible across all mobile devices. For instance, not too many smart phones offer fingerprint sensors. If banks can offer both fingerprint and the facial recognition options, customers can use a wider range of devices. In fact, smart phones with as little as a 1 mega-pixel front-facing camera can offer the facial recognition option and this covers probably the entire smart phone market.

3. PROPOSED METHODOLOGY

Biometrics in banking is at an inflection point with improvements in technology on an almost daily basis, making it an extremely compelling option for both banks and their clients. While banks have choices to make in terms of routes to pick (facial, voice, Iris, fingerprint etc.), unifactor vs. multifactor, they also need to decide on the preferred implementation that could be in-house, cloud-based or a combination of both with the data being in-house for security reasons. We also believe that biometrics will eventually move from external body traits to internal traits like heart rate or vein recognition that offer higher level of security cover. Then there is the option of behavioural biometrics that looks at the gestures and speed with which users type their passwords (for example) and then combine these with traditional biometrics to offer a more robust solution. These surely are exciting times for banks, customers and technology providers. The application of biometrics and passwords is shown in table 1.

Table 1. Applications of Biometrics and Passwords

Continuous authentication	**Better accuracy (FAR, FRR) through multi-factor, combining**	**Improved speed**
Face	Face and voice	1-2 seconds for facial
Voice	Face, voice and PIN	Even lesser for fingerprint
Behavior	Face, voice and behavior etc.	Voice may be longer

The roll-out biometric options for clients, banks must weigh parameters including accuracy (FAR/FRR), speed, social acceptance, verification vs identification, barriers to attack and simple deployment. as an example, a personal bank that has very high security threshold for his or her high net-worth clients may go for Iris rather than fingerprint or voice, although Iris may score low on simple deployment or social acceptance. Often, we don't see banks restricting to simply one biometric option for his or her clients. supported the transaction risk, they'll prefer to mix and match the choices by requiring only the fingerprint to login but requesting a mixture of Iris and voice to initiate an outsized dollar transaction (multi-factor).Today, three forms of factor groups are available to attach a personal with the established credentials. The block diagram of biometrics is shown in figure 1.

1. Knowledge factor—something the user knows, like a password or, simply, a “secret”;
2. Ownership factor—something the user has, like cards, smart phones, or other tokens;
3. Biometric factor—something the user is, i.e., biometric data or behavior pattern.

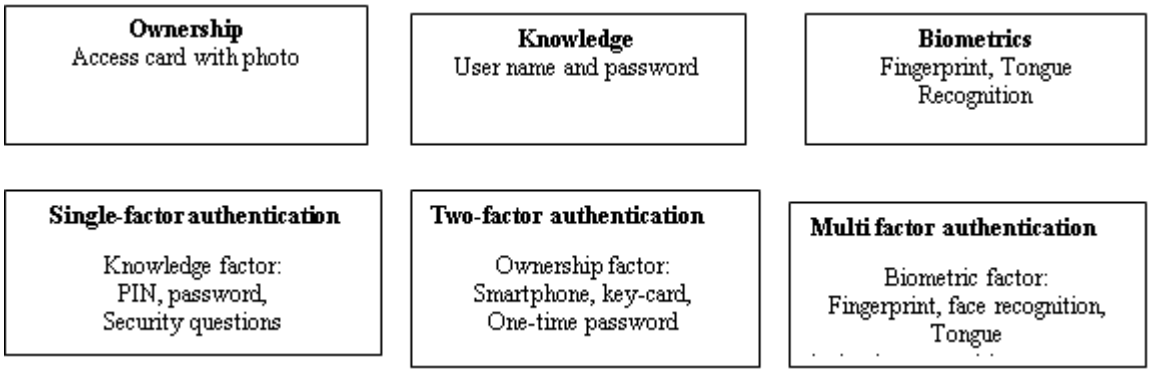

Figure 1. Block Diagram of Biometrics

The Customers first register and authenticate with the service provider to activate and manage services they're willing to access. Once accessing the service, the user is required to pass a straightforward SFA with the fingerprint/token signed beforehand by the service provider. Once initially accepted by the system, the customer authenticates by logging in with the identical username and password as setup previously within the customer portal (or social login).Cryptography for added security, the managing platform can enable secondary authentication factors. Once the user has successfully passed all the tests, the framework automatically authenticates to the service platform. The secondary Authentication occurs automatically supported the biometric MFA, that the user would be requested to enter a further code or provide a token password only just in case the MFA fails.

4. CONCLUSION AND FUTUREWORK

Although such a big amount of biometrics are used and developed, to our greatest knowledge, there's not so work has been tired tongue biometric recognition system and its use in any application .In this paper we are propsing safer tongue identification system using visual cryptography. Various research works are moving into this field and in future we are going to specialize in the subsequent aspects.. we are going to extend this public use system with personal use system so an individual can log in to checking account from home by sending tongue images using personal camera via internet using visual cryptography.. Since human tongue is non-rigid when it moves. We expect to gather the video of tongue to extract some rules of its movements . Towards application of tongue biometric in other areas also, as an example in security systems etc. Every soul has some unique features about a number of his body organs and one in all them is tongue, which may be used as secure and safer way for authentication. The authentication system is developed for many beneficial and accurate results for the acceptance of this technique worldwide

REFERENCES

Banyal, R., Jain, P., & Jain, V. (2013). Multi-factor authentication framework for cloud computing. Fifth International Conference on Computational Intelligence, Modelling and Simulation(CIMSim), (pp. 105–110). Seoul, Korea,.

Bhargav-Spantzel, A., Squicciarini, A., Modi, S., Young, M., Bertino, E., & Elliott, S. (2007). Privacy preserving multi-factor authentication with biometrics. J. Comput. Secur., 15, 529–560.

Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. T. (2013). On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE, 136–148.

Harini, N., & Padmanabhan, T. (2013). 2CAuth: A new two factor authentication scheme using QR-code. Int. J. Eng. Technol., 5, 1087–1094.

Huang, X., Xiang, Y., Bertino, E., Zhou, J., & Xu, L. (2014). Robust multi-factor authentication for fragile communications. IEEE, (pp. 568–581.).

Jorgensen, Z., & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. 6th ACM Symposium on Information, Computer and Communications Security,, (pp. 476–482.). New York, NY, USA, Hong Kong, China,.

National Research Council;Whither Biometrics Committee. Biometric Recognition: Challenges and Opportunities. (2010)., (p. National Academies Press). Washington, DC,.

Roy, S., & Khatwani, C. (2017). Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols. 1(9).

Scheidt, E. a. (2006). Multiple Factor-Based User Identification and Authentication. U.S. Patent, 7(131)

(2017). VNI Cisco Global Mobile Data Traffic Forecast 2016–2021. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete.