ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse88852019.pdf
https://doi.org/10.30534/ijatcse/2019/88852019

IoT Enabled Visual Recognition Model for Biometric Authentication

S.Arunpandian[1], S.S.Dhenakaran[2], S. Santhosh Kumar[3]
[1, 2,3] Department of Computer Science,
Alagappa University, Karaikudi, Tamilnadu, India, [1]spandiyan01@gmail.com, [2]ssdarvind@yahoo.com

ABSTRACT

Biometric authentication is one of the highly secured and feasible techniques in many applications .it requires Physiological evidences as input and with behavioral references. The authentication has done by matching the submitted evidences along with physical current input. Today Aadhar is a widely using biometric database allows India for bank transaction card to avail the PDS services etc. The present system can be efficiently used when IoT is implemented on it. The present system requires photographs, fingerprint or Aadhar number for personal verification .It is a partial automated technique, which requires human support. However, in real time certain applications like surveillance search of personalized information in a group which requires automated authentication process. This paper is focus on to implement the IoT supported Aadhar biometric authentication for real time application.

Keywords: Biometric Authentication, Visual cryptography, Aadhar database, IoT.

1. INTRODUCTION

Biometric authentication is widely used techniques for small to large applications. The range of applications includes administration, employee attendance, transportation and POS services etc [1-6]. Although it gives better results the aadhar like centralize database have utilized for some other extended Application, which are very needful application for current situation. According to the Indian statistics the total number of aadhar card holders in India 89% in the total population. And also people records are digitized [7-9]. These biological data is unique can be used for other applications like public surveillance, crowed monitoring, socio and personal Psychological behavioral monitoring etc.

Countries like China and America are having biometric authentication system. The system gets input as images, fingerprints automatically and compares with the database. It is very useful to track the individual and their behavioral in the public. The continuous monitoring of results increased security. Integration of services and collaborative services like traffic clearance, insurance service, customized health care of supports and assistance. In India, the aadhar verification system has also utilized by the police department to identify the suspects by matching his records with the crime database it requires a photograph of a person for instant matching with the aadhar & crime records from data repositories.

2. RELATED STUDY

Jose Sanchez del Rio et al. [10] have focused on Automated Border Control the problems of electronic gate congestions or arrival of late time by the rapid growth of passenger worldwide at aerodrome of USA and China. In real time situations, face recognition system is preferred and installed in kiosk small devices by the authorities. The devices connected to cloud storage, in which biometric detailed information are preserved. Comparisons have done by facial recognition algorithm instantly by the automated system. By the low quality images are captured comparison will be failed. So that improve an automated border control algorithm is made for capturing the data clearly with modified comparative components. Kenneth Lai et.al [11], typically, watch-list have contained high quality images when compare of visitors either genuine or not in border control. Sometimes if watch-list own low quality images, them may happen a incidents drastically. The propose model is give a better solution to match the visitor with watch-list by the use of taxonomical view, risk assessment technique and Doddington metrics. Hisham Al-Assam et al. [12] developed an Automated Biometric Authentication system for Cloud Computing. The author developed Fuzzy Identity-Based Encryption and Biometric identity-based encryption (BIO-IBE) techniques for cloud based authentication system. However, biometric-based cloud authentication manages the resources to cloud. The security is a major concern because of confidential information, which is related to health, gender, ethnicity can be stolen. Tracey Caldwell [13] states market report on border biometrics. According to the author, the main problems for introducing border biometrics in the past were cost and feasibility. Accenture, Atkins Global, Aurora, Aware, Cognetic,

and many other suppliers are working on this market border biometrics. Biometric solutions have proven their speed, accuracy and security in international airports around the world and look set to continue to do so.

3. THE PROPOSED WORK

The proposed work contains IoT enabled devices with supported cloud storage database. The model gets inputs as captured images, fingerprints, eye prints and which compares instantly with the aadhaar database. The role of IoT [14-15] is to get the unique or customized input from the device connected for input. The additional IoT enable devices may also used for data manipulation when the input devices are IoT enabled then the current data can be sent to the database and possible to compare with the existing authentication system instantly.

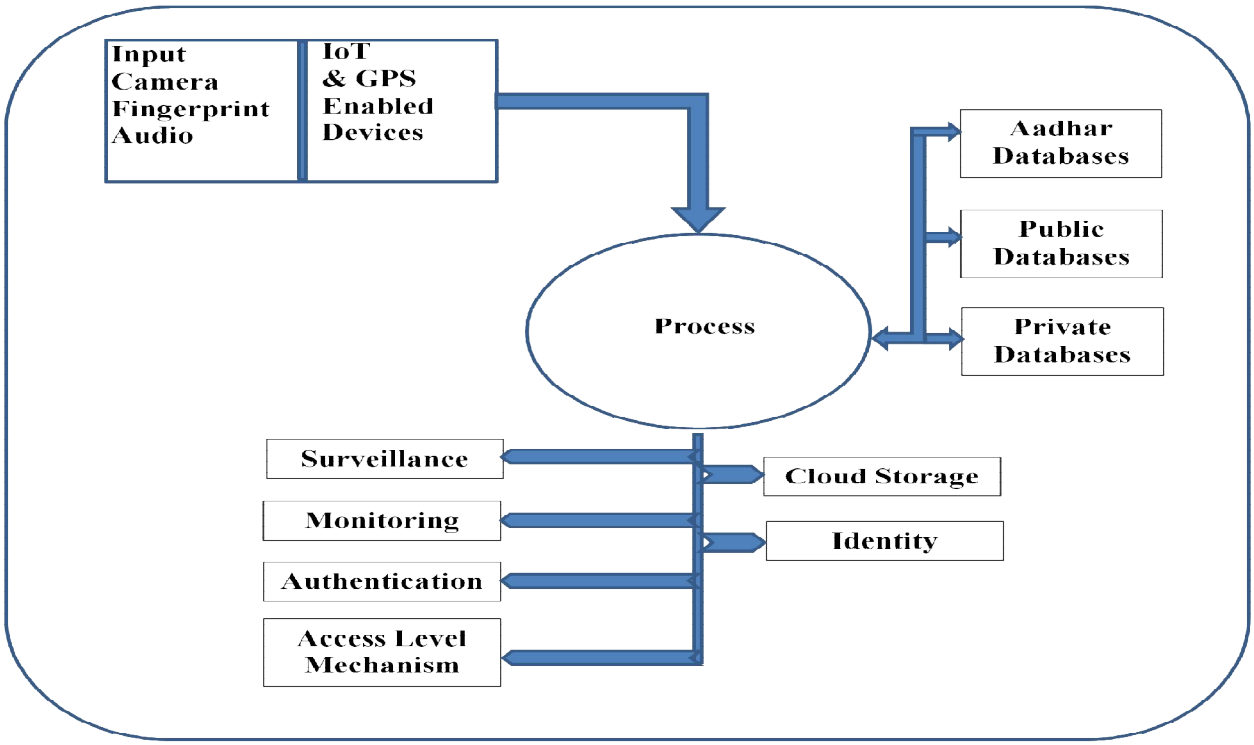

Figure 1: Model for IoT Enabled Biometric system

The model is an integration process of existing database and resources with the authentication system Figure 1. For example in a toll-plaza, the vehicle registration numbers have used for accounting the transportation of a vehicle based on the time intervals. For that image capturing cameras are used to identify the vehicle number and a person who travelling in the vehicle when the authentication system is IOT enabled and connected with the public database such as Aadhar , transport then the authentication can easily doe to identify the person who is travelling in the car and also get vehicle and its owner details. The overall data are gathered and stored in the cloud environment. This model gives better solution to achieve high-level authentication and ensures to predict the security threats in advance. The stored data may also used for further analysis or other applications. The proposed model can also able to notify or inform the message to the relevant concern authorities to alert what is happening in the environment.

Pros and cons of proposed model

Pros

- The proposed model is the integration of existing technologies, which gives better results with least investments for Identification and Authentication.
- The model supports digitization of the information and can used as a reference at each level in the mechanism, which provides high level security in the environment.
- It provides customized monitoring service and identification of unique person in a crowd without disturbing the environmental activities.
- When more databases have integrated in the proposed model then it will give the fully automated authentication and success level service to all the users in the society.

Cons

- Security

  The proposed model requires accessing many public and private databases hence high level of security mechanism to be developed for ensure high- level security.

- The hardware and high speed internet facility is the basic requirement of the model hence the performance many vary due to internet speed.
- The organization who are going to integrate with if common policies and should ensure appropriate security among the large amount of temporary and permanent data storage is needed in this model.

4. CONCLUSION

The IOT is one of the magic word used in many domains. The data can be generated, monitored and analyzed anywhere with the use IoT. Biometric authentication is one of traditional computation technique used in wide range of applications. The integration of these two technologies can give better solutions for many real world problems. The proposed model is a initial for customized identification and authentication. The proposed model can be enhanced with respect to the relevant application domains.

Acknowledgement

This article has been with the financial support of RUSA – phase 2.0 grant sanctioned via Letter No F.24-51 / 2014-U, Policy (TNMulti-Gen), Dept. of Edn. Govt. of India, Dt. 09.10.2018.

References

1. Gupta, A., Kundu, A., & Das, R. (2019). AUTOMATED ATTENDANCE SYSTEM FOR EFFICIENT EMPLOYEE MANAGEMENT: A BIOMETRY BASED APPROACH. *International Journal on Recent Trends in Business and Tourism*, *3*(3), 117-121.**3.**
2. Garg, V., Singhal, A., & Tiwari, P. (2018, January). A Study on Transformation in Technological Based Biometrics Attendance System: Human Resource Management Practice. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 809-813). IEEE. https://doi.org/10.1109/CONFLUENCE.2018.8442957
3. Abikoye, O. C., Afolabi, G. K., & Aro, T. O. (2019). BIOMETRIC BASED POINT-OF-SALE AUTHENTICATION SYSTEM. *International Journal of Software Engineering and Computer Systems*, *5*(1), 36-51.
4. Okokpujie, K., Noma-Osaghae, E., Okesola, O., Omoruyi, O., Okereke, C., John, S., & Okokpujie, I. P. (2018, June). Fingerprint Biometric Authentication Based Point of Sale Terminal. In *International Conference on Information Science and Applications* (pp. 229-237). Springer, Singapore. https://doi.org/10.1007/978-981-13-1056-0_24
5. Trehan, U., Awasthi, A. K., Gupta, S., & Singh, P. (2018). Security Authentication System Using Facial Recognition. *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org*, *8*(4).
6. Singh, I., Kumar, D., & Khatri, S. K. (2019, February). Improving The Efficiency of E-Healthcare System Based on Cloud. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 930-933). IEEE. https://doi.org/10.1109/AICAI.2019.8701387
7. Thilagavathi, S., Vimala, S., Valarmathi, K., Priya, R., & Sathya, S. (2018, February). Massive Data Processing Using Mapreduce Aggregation To Make Digitized India. In *International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)*. Atlantis Press. https://doi.org/10.2991/pecteam-18.2018.17
8. Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2018). The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *European Business Organization Law Review, Forthcoming*, 18-45. https://doi.org/10.2139/ssrn.3224115
9. Goel, S. K., & Shukla, M. (2018). Enforcement of Automatic Penalty (e-Penalty) to Govern the Traffic Rule Violators in Digitized INDIA Using ICT. In *Computational Vision and Bio Inspired Computing* (pp. 788-802). Springer, Cham. https://doi.org/10.1007/978-3-319-71767-8_68
10. del Rio, J. S., Moctezuma, D., Conde, C., de Diego, I. M., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. *computers & security*, *62*, 49-72. https://doi.org/10.1016/j.cose.2016.07.001
11. Lai, K., Kanich, O., Dvořák, M., Drahanský, M., Yanushkevich, S., & Shmerko, V. (2017). Biometric-enabled watchlists technology. *IET Biometrics*, *7*(2), 163-172. https://doi.org/10.1049/iet-bmt.2017.0036
12. Al-Assam, H., Hassan, W., & Zeadally, S. (2019). Automated Biometric Authentication with Cloud Computing. In *Biometric-Based Physical and Cybersecurity Systems* (pp. 455-475). Springer, Cham. https://doi.org/10.1007/978-3-319-98734-7_18
13. Caldwell, T. (2015). Market report: border biometrics. *Biometric Technology Today*, *2015*(5), 5-11. https://doi.org/10.1016/S0969-4765(15)30079-5

14. **S**.V.R.K.Rao (2018), Wireless sensor Network based industrial Automation using Internet of Things(IoT), *International journal of Advanced Trends in computer science and Engineering, 2018 7*(6),pp 82-86.Available at: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01762018.pdf https://doi.org/10.30534/ijatcse/2018/01762018
15. N.SarithaDevi (2018), Safty and security for school children's vehicles using GPS and IoT Technology International journal of Advanced Trends in computer science and Engineering, 2018 7(6),pp 91-95.Available at: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse03762018.pdf https://doi.org/10.30534/ijatcse/2018/03762018