IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 12, December 2020
DOI 10.17148/IJARCCE.2020.91210

# Crux in IoT Devices Access Control Modules Using Finger Print and Overcome Approach

**Istiaque Ahmed[1], Sk. Mehedi Hasan[2], Farzana Morium[3]**

Guest Lecturer, National Academy for Computer Training And Research, Bangladesh[1]

Dept. of Computer Science and Engineering, Khulna University, Bangladesh[2]

Dept. of Computer Science and Engineering, Pundra University of Science and Technology, Bangladesh[3]

**Abstract:** Security is a challenge in every secured areas and devices access. IoT devices with modern AI are using in access control modules to permit it verified authority. In this paper we consider user experience from their daily uses of IoT devices. Finger print based access control module handle images from users with seasonal skin issues, pressure of fingers, placement angels of fingers and carelessness of users. Existing IoT devices access control module domains highly concern on better matching of pattern. Though person is verified, some issue arises to access control that generate negative mind to users of IoT devices. Institutions maintains manual register book to support the crux of IoT devices access control failure. We design a repeated partial and adaptive model to overcome the problems of existing models. This approach will help to assure better access control in IoT devices and users experience. IoT and AI industries will be highly beneficiary from this research to assure quality production.

Keywords: AI, IoT, Access Control, Pattern Matching

## I. INTRODUCTION

Direct measurement of a body part (i.e. fingerprints, retina, iris face) is Physiological biometrics, while human action (i.e. gait and signature) [1] behavioral biometrics. Modern offices use IoT and AI devices [12] with faster computational power in separate access control modules, even in smart phones, personal digital assistants, laptops and others. User authentication for IoT and AI devices has become an important consideration [2] [13]. User authentication module inside devices confirms identity of a person. Three major factors for user authentication, firstly something you know based (user name, password), secondly something you have (smart card, device, and equipment, security token), finally something you are (fingerprint, voice, DNA, gait and other biometrics). These factors are used in modern authentication modules to authenticate a person in offices and devices. IoT and AI scientists select biometrics for devices and systems from the comparison of biometrics base on universality, uniqueness, permanence, collectability, performance, acceptability and circumvention. Considering that finger print is the most use biometric in devices or separate access and attendance modules. Area of uses and device facilities also play an important role in the selection on biometrics. The following table is the comparison of biometrics and researches have made this comparisons base on some valuable accepted research.

TABLE 1: COMPARISON OF BIOMETRIC TECHNOLOGIES [3]

H-High, M-Medium, L-Low, U1-Universality, U2-Uniqueness, P1-Permanence, C1-Collectability, P2-Performance, A-Acceptability, C2-Ciecumvension

| Biometrics | U1 | U2 | P1 | C1 | P2 | A | C2 |
|---|---|---|---|---|---|---|---|
| Face | H | L | M | H | L | H | L |
| Fingerprint | M | H | H | M | H | M | H |
| Hand Geometry | M | M | M | H | M | M | M |
| Key Strokes | L | L | L | M | L | M | M |
| Hand Vein | M | M | M | M | M | M | H |
| Irish | H | H | H | M | H | L | H |
| Retinal Scan | H | H | M | L | H | L | H |

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 12, December 2020
DOI 10.17148/IJARCCE.2020.91210

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Signature | L | L | L | H | L | H | L |
| Voice | M | L | L | M | L | H | L |
| F.Thermogram | H | H | L | H | M | H | H |

Small and medium devices from well-known production companies use finger print in their devices that attract users very much. Recently we conduct a survey on 37 institutions that use finger print access control in their institution and personal IoT devices. We found the user experience is very poor as bellow. A large amount of the user don not feels comfort with the finger print access control system and devices as bellow.

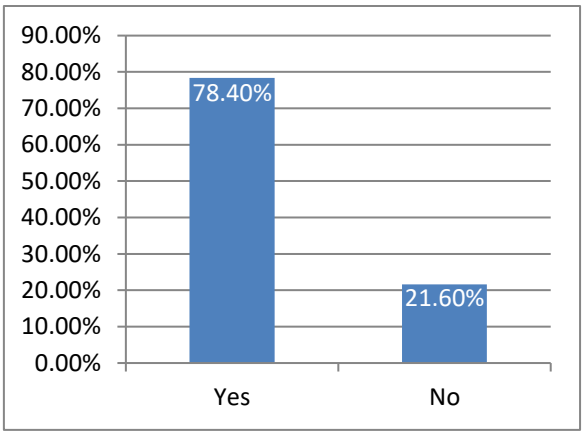


Fig. 1. A number of people do not feel comfort with the access control system

## II. EXISTING MODELS

Existing devices and modules for access control use Fingerprint Recognition (FPR) System [6] as Figure 2. Biometric matcher takes the decision based on DB and current template [7].

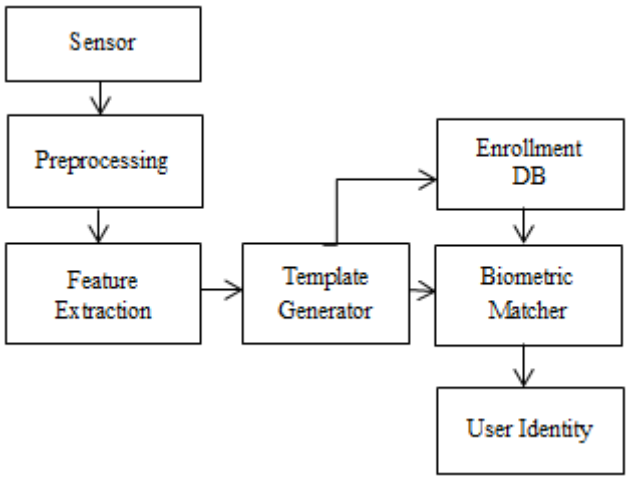


Fig 2. Existing finger print access module [4]

Three pattern class whorls, arch, and loop are widely used to identify a person. About 60% people have loops, 35% have whorls and 5% have arches in their finger pattern.

| Whorls | Plain Arch | Tented Arch | Right Loop | Left Loop |
|---|---|---|---|---|

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 12, December 2020
DOI 10.17148/IJARCCE.2020.91210

Fig. 3. Visual Pattern Classes [5]

Different techniques are used for data classification. Classification plays a vital contribution in FRS. Modules try to reduce search time at the time of matching template that a positive achievement of the existing module. Classification ensures the search time reduction efficiency of the identification system. Minutiae are basically line patterns and ridges, which give unique identity of a person. Systems can identify pattern difference of twins fingerprints. Bifurcation, arch, loop, ellipse, sweat gland, island, tented arch, rod and spiral are line type classifications of fingerprints that shown in Figure 4.

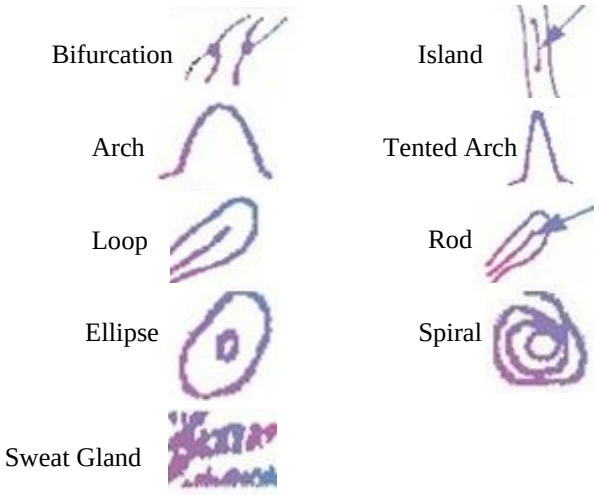


Fig. 4. Line type Classification

Various techniques are used and matching techniques are responsible for identification of a person [8] in areas and devices. Different fingerprint matching techniques and identification keys are shown in Table 2.

TABLE 2: MATCHING TECHNIQUE AND IDENTIFYING KEY [4]

| **Matching Technique** | **Identifying Key** |
|---|---|
| Minutiae Based | Ending Ridge |
| Pattern Based | Bifurcation |
| Featured Based | Island |
| ROI(Region of Interest) Based | Crossover |
| Correlation Based | Core |
| Statistics Based | Delta |
| ONNC (Optical Neural Network Computer) | Ridge Pore |

## III. CRUX OF EXISTING MODEL

There are technical issues and challenges [9] in modern access control tools. In our survey we found larger group keep alternative register book to support the failure of existing system.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 12, December 2020
DOI 10.17148/IJARCCE.2020.91210

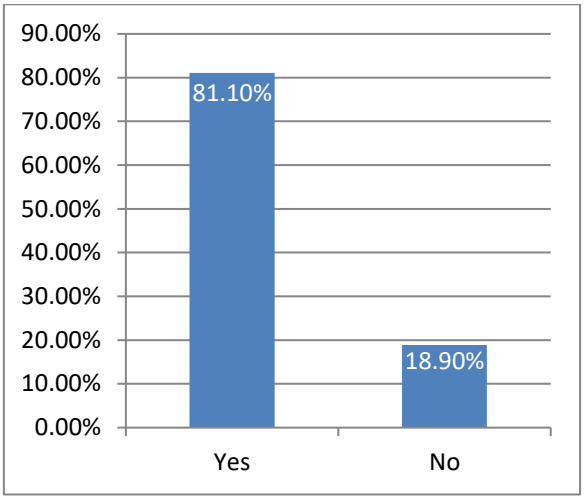


Fig. 5. Register book keeping supporting of access control system

Institutions loss trust on IoT and AI based finger print access control modules because of keeping extra manual register book. This user expression is a big challenge for access control module production companies and researchers. Age is an issue [10] for long term user of a system to match from the old database. Seasonal weather [11] also a reason of low performance of finger print based access control system. It is possible to make duplicate artificial finger print of a person, though cooperation is needed. This duplicate finger print can allow unwanted access to a system and this is a big issue in student attendance and employee attendance.

## IV. OVERCOME APPROACH

Survey on the users how that 83.8% of them think the device should be more comfortable. This percentage of users is a large proportion. Evaluation the survey we consider the issues for the low performance of access control devices. In our designed model we propose repeated partial matching approach.

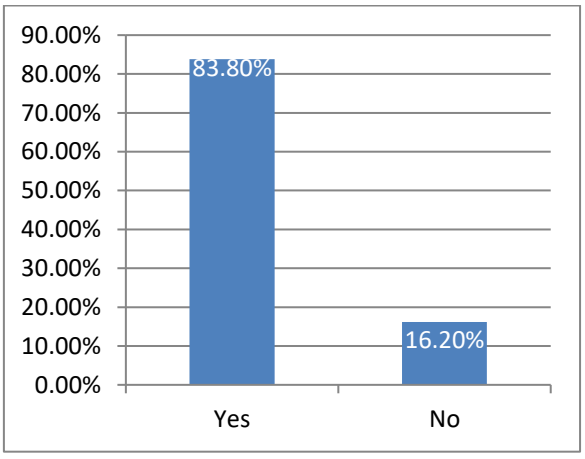


Fig. 6. Users expectation to device should be comfortable

Repeated partial matching and the selected parts for final identification. In the template generator a part selector cooperate to part the finger print and temple generator ask to matcher to select the parts and generate the template. In this module we consider the age and weather issue of a user of the system.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 12, December 2020
DOI 10.17148/IJARCCE.2020.91210

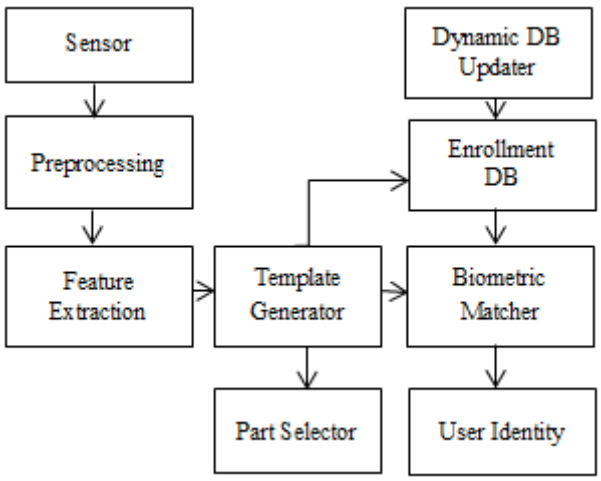


Fig. 7. Proposed access control module in IoT and AI device

TABLE 3: NOTATION USED IN THIS PAPER

| Symbol | Significance |
|---|---|
| $I$ | Template Image |
| $I_1, I_2, I_3, I_4$ | Parts of Input Image |
| $T_i$ | Threshold |
| $I_p$ | Processed Image for matching |

Input images are taken by the users and make an standard template $I$, I is divided into four sections $I_1$, $I_2$, $I_3$, $I_4$ and try to match to the database using *K-NN* algorithm. Parts are selected considering threshold $T_i$ and process template image $I_p$ is prepared for final matching. Keeping multiple databases RAID [14] to use in different purpose. Continues monitoring the variation of data and match to threshold value and extra threshold for database updating dynamically as well as try to take decision about updating issue like age or weather. This dynamic database updating [15] helps to overcome the problems of long term system users. We divide a standard template into four parts as Figure 8 and matcher select the most alike parts and from multiple cooperation templates generate the template for final matching as bellow.


Fig. 10. Part selection and matching approach

This approach not time consuming for all approaches, for the data with enough information this module work as present system. Only when data don not carry enough information and that is bellow to the threshold value the AI of this module go to repeated part wise and matching approach. Multiple RAID database of this system also store variation in time variant and weather variant data recommended by the AI system. Enrollment DB also updated by the decision of AI, when continuous variation is observed. A separate threshold is the main yardstick for this decision. This enrollment DB is mainly based on frequency of variation and help of prime threshold value of matcher. User

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 12, December 2020
DOI 10.17148/IJARCCE.2020.91210

cooperation is a challenge for this module. As per survey data 86.5% of users are agree to cooperate. Users try to become success at failure that is advantage for this system. This user behavior subconsciously helps this module.

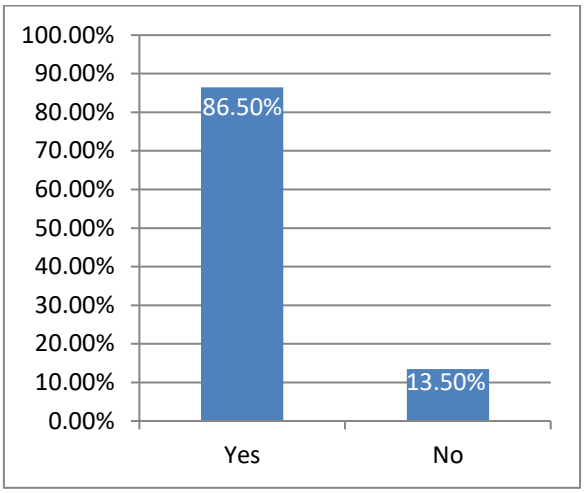


Fig. 9. User thinks they should be more cooperative to the devices

## V. CONCLUSION

This research has positive impact on IoT and AI devices access control module. Automatic DB updating is a new research in this field, here is opportunity to develop efficient algorithm for repeated partitioning of data and automatic updating. User cooperation is a big challenge for this module. Though subconscious behavior overcome the issue. Extraction data from image and matching of multiple parts is time consuming but success rate bears users satisfaction. Industries related to production of access control module will be highly benefitted from this module with some existing adaptive module. User satisfaction will play a role to generate positive concept of users to the technology products.

## REFERENCES

[1] A User Authentication Scheme Using Physiological and Behavioral Biometrics
for Multitouch Devices
[2] D. A. Ortiz-Yepes, R. J. Hermann, H. Steinauer, and P. Buhler, “Bringing strong authentication and transaction security to the realm of mobile devices,” IBM Journal of Research and Development,vol.58,no.1,pp.1–11,2014.
[3] A.K. Jain, R. Bolle, and S. Pankanti (eds.). Biometrics: Personal Identification in Networked Society. Kluwer, New York, (to appear) 1998
[4] Fingerprint Recognition System: Issues and Challenges, International Journal for Research in Applied Science & Engineering Technology (IJRASET ), ISSN: 2321-9653; IC Value: 45.98; SJ, Volume 6 Issue II, February 2018- Available at www.ijraset.com
[5] https://en.wikipedia.org/wiki/Fingerprint
[6] Fingerprint Recognition System : Design & Analysis, Conference: International Conference on Scientific Paradigm Shift In Information Technology & Management, SPSITM'11
[7] Biometric – Theory Bio-Metrica, LLC. http://bio-metrica.com/biometric-theory
[8] Kribashnee Dorasamy, Leandra Webb, Prof. Jules Tapamo, Nontokozo P. Khanyile “Fingerprint Classification Using a Simplified Rule-Set Based on Directional Patterns and Singularity Features” 978-1-4799-7824-3/15/$31.00 ©2015 IEEE.
[9] Technical issues and challenges of biometric applications as access control tools of information security, International journal of innovative computing, information & control: IJICIC 8(11):7983-7999
[10] A Study of Age and Ageing in Fingerprint Biometrics, IEEE Transactions on Information Forensics and Security PP(99):1-1DOI: 10.1109/TIFS.2018.2878160
[11] Impact of Time, Weathering and Surface Type on Fingerprinting Tosha Gray College of Arts and Science Dakota State University Madison, SD 57042, The National Conference On Undergraduate Research (NCUR) 2012 Weber State University, Ogden Utah March 29-31, 2012
[12] https://itchronicles.com/iot/iot-devices-office/
[13] https://www.sciencedirect.com/topics/computer-science/authentication-factor
[14] Reliability model of disk arrays RAID-5 with data striping, P A Rahman and G D’K Novikova Freyre Shavier 2018 IOP Conf. Ser.: Mater. Sci. Eng. 327 022087
[15] Dynamic On-Demand Updating of Data in Real-Time Database Systems, January 2004, DOI: 10.1145/967900.968074, Conference: Proceedings of the 2004 ACM Symposium on Applied Computing (SAC), Nicosia, Cyprus, March 14-17, 2004

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91210

## BIOGRAPHY

**Istaique Ahmed** completed his MSc and BSc degree from the dept. of Computer Science and Engineering (CSE) from University of Rajshahi, Bangladesh. Currently he is doing his job as a guest lecturer in National Academy for Computer Training And Research (NACTAR), Bangladesh. He is also a software developer at Research and Development team of RedDevs, Bangladesh. Formerly, he was lecturer in Computer Science and Engineering (CSE) dept. of Pundra University of Science and Technology, Bangladesh. He was research fellow of ICT ministry of Bangladesh in 2014. His research fields are IoT and Secure Communication, AI, HCI and Pattern Recognition.

**Sk. Mehedi Hasan** completed his BSc degree in Computer Science and Engineering from North Western University, Bangladesh. Now he is doing his MSc in Computer Science and Engineering in Khulna University, Bangladesh. His research interests are IoT, AI and Software Engineering.

**Farzana Morium** completed his BSc in Computer Science and Engineering (CSE) from Pundra University of Science and Technology, Bangladesh. Currently she is doing her job as a member of research and development team of RedDevs, Bangladesh. Her research fields are AI, HCI, Networking and Secure Communication.