Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 1872-1877
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.210

SMART PLIGRIM CENTER: IOT BASED SECURITY SYSTEM AT PLIGRIM CENTER

Mithun B Patil, Assistant Professor, Dept. of CSE , NKOCET,Solapur Maharashtra, mithunpatil@orchidengg.ac.in
Dr. Vipul V Bag, Professor Dept. of CSE NKOCET, Solapur, Maharashtra, vipulbag@orchidengg.ac.in
S A Talekar, Assistant Professor, MVPS's KBT College of Engineering,Nashik, Maharashtra, talekar.sopan@kbtcoe.org

Abstract- The security check is a prime issue in today's era. Especially in pilgrim centers where lakhs of devotees visit daily. Providing security in these pilgrim centers is a highly challenging task for the government and police department. Earlier we have a manual security check where visitors of pilgrim center are checked manually which is not appropriate and secure. To overcome these we have designed an IoT-based application to felicitate the security check in the pilgrim center. We are using raspberry pi and a webcam for capturing every visitor and processing data related to the visitor. Every visitor needs to enter his/her details and contact details at the registration center. After registration, some samples of the visitor's face are captured and processed.When visitors try to enter the Pilgrim center, the visitor's face is captured and crosschecked with a stored database images. If the visitor is unauthenticated or unregistered then it alerts the pilgrim center authority to take necessary security action.

Keywords: Raspberry pi, Internet of Things (IoT), Pilgrim center, Security

I. INTRODUCTION

Pilgrimage isof considerable importance in some of modern times.Safety has become a major issue for most people [2], especially in rural and urban areas.For a common person, the pilgrimage center means a place that represents thehighest level of security. Every day we are involved in the activities of the pilgrimage center.This is an important part of our life. Nowadayswearеusing manualsecurity checkorbiometricsystemfor securitythough they aresecured,therearesomedisadvantages. Themajordisadvantageinthismanual checkmethodisthe rapidly growing crowd and management of the crowd.

Many of the IoT-based and Zig bee-based technologies [1] have been identified to solve the problem of the safe movement of pilgrims in these center solutions. Face identification is one of the key elements in controlling and monitoring terrorist activity during this pilgrimage. We proposed a method to automatically identify and verify the identity of a person from a digital image using a face recognition system. The basic flow of a face recognition system is to capture an image with a camera and the Local Binary pattern (LBPH) algorithm detects the face and extracts features. After extraction, the system matches the captured image with the database image. If the captured image is similar to the database image, provide access to the Pilgrim Center. If it does not match the captured image, than it sends an alert message to the Security Center for appropriate action against unknown users. It can also be used in places such as private workplaces, office locations such as records, servers, document storage, and other security-critical locations. Therefore, we are using this proposed methodology to provide high security.

II. LITERATURE REVIEW

The background about the previous scientific research that has been done with the consideration of current and future security threats are discussed in this session. In the current scenario Pilgrim,centersare underthesurveillanceofCCTVcameras,alert alarmsystems with emergencyenabled buttons.TheCCTVcamerasare usedtomonitor themovement of pilgrim for safety and avoid unauthorized user access to pilgrim center. The footages are to be monitoredby human interventions, which is not a feasible task. The alarm emergency button also needs to be pressed manually to alert the security center. This traditional system requires a lot of manpower. A major requirement is to develop a system that will automatically detect unauthorized motion and inform the security officials of the pilgrim center in different ways without any need of a human being.[3], As **st**ated**,** there are a l**ot** of issues in the Internet of

Things (IoT) s**ecurity t**h**a**t re**quire**s **fixe**s, for example, RFID **t**a**g** security, remote security, organize**d** transmission security, security insurance, data prepar**ati**o**n** security.Also, it **provi**d**e**s another way to deal with specialists in certain IoT application**s** and **sc**h**em**es**, by rese**a**rch**ing and **unde**r**stand**ing **IoT** security **in** different ways.[4] **The** concept of a smart home can be aptly in**teg**rated to make it smarter, safer, and **more** automated.We can build a**nintelligen**t wireless home security system **th**a**t** sends alerts to the owner **overthei**nternet in **th**e **event** of a **b**rea**ch** and **optionally t**ri**gge**r**s** an alarm.The advantage**pro**vi**d**ed by **the vi**r**tu**e **of** this system over similar **type**s of existing systems is that the alerts and status sent by the **W**i**F**i**-**connected microcontroller managed system can be received by the user on **th**ei**r** phone at any distance**,** re**gardl**e**ss** of whether his mobile phone is connected to the **I**nternet. [5], the term Internet of Things for the most part alludes to situations where the organizational network and the ability to record reach ordinary objects, sensors, and things and allow these devices to create an exchange and devour information with negligible human mediation using different systems management and correspondence models. The information created or managed from those shiny elements will eventually pass through doors with availability to IP-based systems or, in general, will be merged into elements that are open via the Internet. **[6],**A fingerprint security system based on ZigBee wireless technology. This system takes a user's fingerprint obtained from a fingerprint sensor module, matches it with the user's fingerprint corresponding to the database details, and displays it on the computer screen. This system is very useful wherever security is the primary concern.

III. IoT based Solution for Security check at pilgrim center

The proposed method consists of two phases mainly registration and then the entry with security check phases. Registration phase's visitor registers himself online or at registration center with all necessary information and image is captured of visitor. The detailed flow of the process in each phase is as follows and the architecture of flow is as shown in fig 1.

Phase1:

- UserRegistration: The useris a known orunknown person. Users need to perform registration with basicpersonal information and registered data is stored inSQLite database.
- Face capture: Some sampleimages of users' faces arecaptured and storedin a database.
- Process &Analysis:All theimages in the databasearetrainedwith the proper specification.
- Aws s3 (Bucket): Trained file and SQLitedatabaseis uploaded to AWS bucket for furtherprocess.

Phase2:

- User(MainEntrance):Person who wants to enter the main entrance. His/her imageis capturedand send for further process.
- FaceCapture:Capturethe live faceof the user who wants to enterinto pilgrim center.
- Aws s3 (Bucket): Download data from AWS bucket forfurtherprocess.
- VerificationandAuthentication. Using LBPH algorithm .We Compare captured livefacewith the trained file downloaded fromAWS bucket.If it match thenthe user is authorized and visitor count is incremented. If a user is authorized then providehim/hersecure entryelsealert the security center for action.

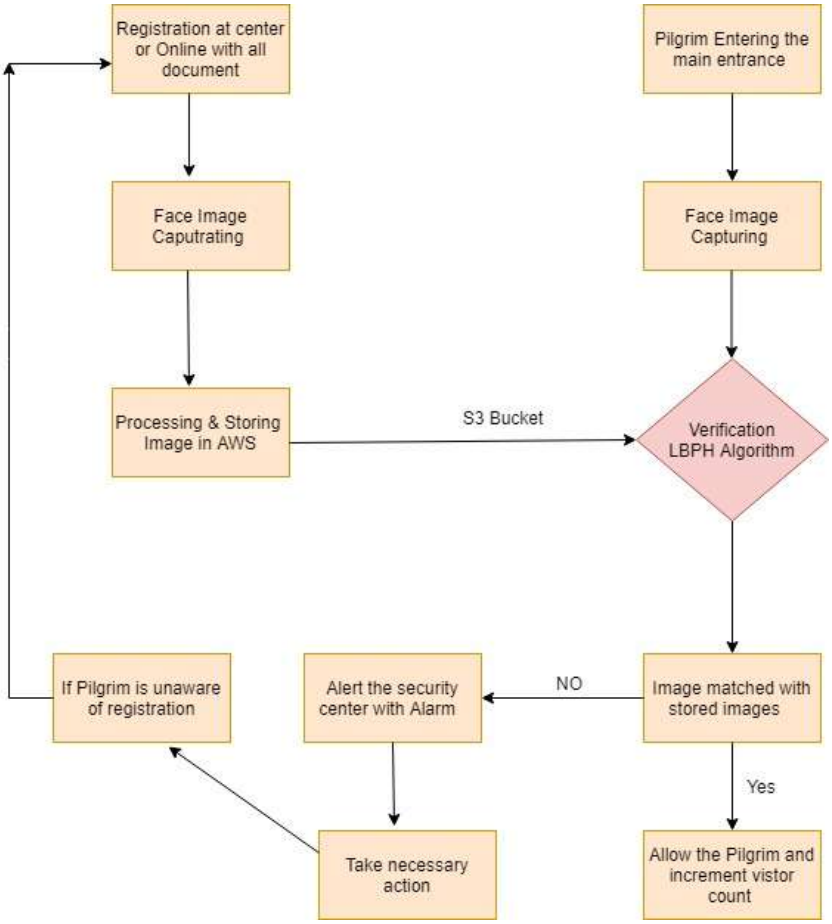

Fig 1: SystemArchitecture for security-enabled IoT system at Pilgrim Center

3.1 LBPH Algorithm (Local Binary Patterns Histogram):

LBPH Algorithm is used for comparing the captured and stored image with Pilgrim visiting the center due to its computational simplicity and discriminative power the steps involved in LBPH are: 1. creating dataset 2.face acquisition 3.feature extraction 4.classification.Suppose we have an image having dimensions N x M.We divide it into regions of same height and width resulting in m x m dimension for every region.Local binary operator is used for every region. The LBP operator is defined in window of 3x3 using equation 1.

$$LBP(Xc, Yc) = \sum_{p=0}^{p-1} 2^p \ (i_P - i_{central}\ )\text{------(1)}$$

Were, LBP(Xc,Yc) central pixel intensity ,i_p intensity of pixel neighbor Pixel $i_{\text{central pixel.}}$

Using median pixel value as threshold, it compares a pixel to its 8 closest pixels using this function as shown in below equation 2

$$G(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases} \text{ ---------- (2)}$$

G(x) is pixel value of image.If the value of neighbor is greater than or equal to the central value it is set as 1 otherwise it is set as 0.Thus, we obtain a total of 8 binary values from the 8 neighbors. After combining these values, we get an 8-bit binary number, which is translated, to decimal number for our convenience. This decimal number is called the pixel LBP value and its range is 0-255. These decimal values are of stored image and captured image are compared for authentication.

Algorithm:

_____

1. Registration of user through online login or at Pilgrim center by entering details of pilgrims and capturing the Image.
2. Processing and storing the AWS S3 Cloud for further data processing.
3. User entering Pilgrim center Image is captured and compare with stored images using LBPH local binary pattern Histogram to authenticate the pilgrim

a. If pilgrim is authenticated than he is allowed to enter the pilgrim center else 3.b and increment visitor count.

b. Security center is alerted by alarm with unauthorized pilgrim entering the center .If pilgrim as missed to registered than go to step 1. Else necessary action by security center

4. When pilgrim exist, the center the image is captured for verification if he is authenticated than reduce the visitor count by 1 else alert the security center.

_____

IV. RESULTSAND DISCUSSION

In this paper, we have implemented a Pilgrim center Security Systemusing IoT. Ifapersonwants to visitthepilgrim centerhis/, herimage willbe captured by the camera andthenitwillbeprocessedinRaspberry Pi andOpenCV using the LBPH algorithm, Ifthepersonintheimageis authenticatedthenitwill provide accessto enter intopilgrim center.Else, the system senda messagetothe authority, andstarts a security alarm.Thusthepilgrim centerwillbehighly securedfrom an unknownpersonor terroristorganization.

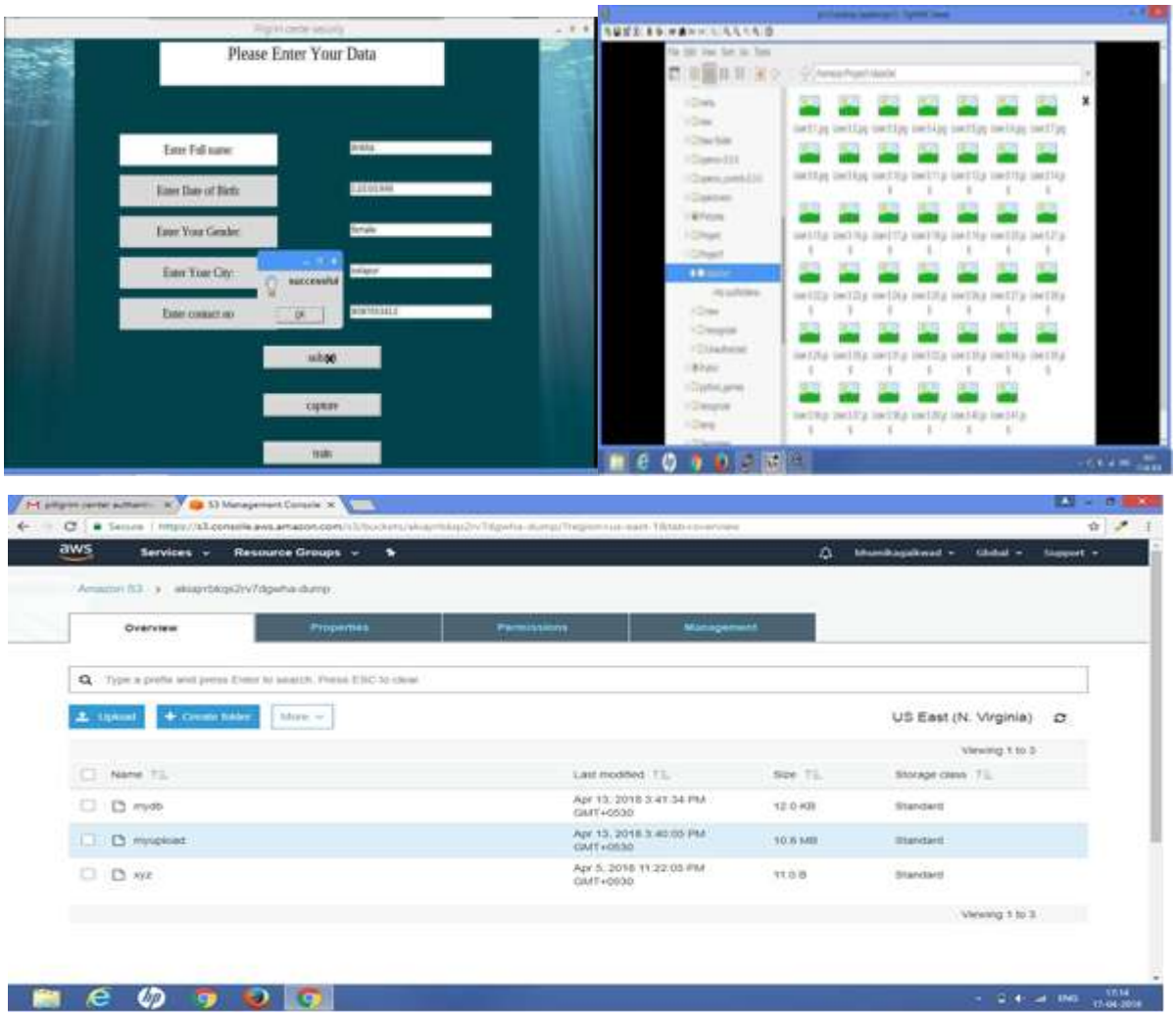

FIG 2: (a) Userinterfacefor registration page (b) Users facedatabasepage (c)aws s3 cloud

Accuracy of Image comparison-using LBPH found that the system is plotted with different user with for varying number of users is plotted below which show the system

Fig 3: Accuracy Graph

The graphs shows that with increasing number of visitors from 100 to 1000 user shows that accuracy up to 99.5 to 98 percentage .On varying the number of visitors or user we can see slight vary in accuracy but it negligible since system is checked with more than 100 user and found only 1-2% vary in results.

V. CONCLUSION

Security threats in pilgrim center is a major concern nowadays so in this research article .we have designed an IoT-basedapplication for securityand management of crowd in pilgrimcenter. Thissystem consists of two different modules, Registration, and Verification.Users can be able to register at one locationand verification at someother location.Itmaintains a total count of visitors in asingle dayandmaintains information of everyvisitor in the pilgrim center. Thissystem also maintains information about unauthorized users,who aretrying to enter without registration.

REFERENCE

[1]. S. K. Shah. "A Review: Monitoring And Safety Of Pilgrims Using Stampede Detection And Pilgrim Tracking." International Journal of Research in Engineering and Technology, vol. 04, no. 04, 2015, pp. 328–332., doi:10.15623/ijret.2015.0404058.

[2]. C, Sunitha, et al. "Need of Internet of Things for Smart Cities." *International Journal of Trend in Scientific Research and Development*, Volume-3, no. Issue-4, 2019, pp. 218–222., doi:10.31142/ijtsrd23597.

[3]. Gupta, Aditya & Mishra, S. & Bokde, Neeraj & Kulat, K.D.. "Need of smart water systems in India" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 4 (2016) pp 2216-2223 .

[4]. Kodali, Ravi & Jain, Vishal & Bose, Suvadeep & Boppana, Lakshmi. (2016). IoT based smart security and home automation system. 1286-1289. 10.1109/CCAA.2016.7813916..

[5]. Mane S.P., Kavathekar G.S., Jadhav S.T., "A Zigbee Based Smart Sensing Platform for Environmental Monitoring", International Journal of Science and Research (IJSR), Volume 3 Issue 5, May 2014, 735 - 738.

[6]. Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar & Raju Kumar 2013, „Wireless Fingerprint Based Security System Using Zigbee Technology", International Journal of Inventive Engineering and Sciences, vol. 1, no. 5, pp. 14-17.

[7]. Hashim, NMZ, Halim, MHA, Bakri, H, Husin, SH & Said, MM 2013, „Vehicle Security System Using Zigbee", International Journal of Scientific and Research Publications, vol. 3, no. 9, pp. 1-6.

[8]. "The History and Future of the Internet of Things." Itransition, www.itransition.com/blog/iot-history.

[9]. Conti, Mauro, et al. "Internet of Things Security and Forensics: Challenges and Opportunities." Future Generation Computer Systems, North-Holland, 26 July 2017, www.sciencedirect.com/science/article/pii/S0167739X17316667.

[10]. Makhdoom, Imran, et al. “Anatomy of Threats to the Internet of Things.” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, 2019, pp. 1636–1675., doi:10.1109/comst.2018.2874978.Monther, A.A.; Tawalbeh, L. “Security techniques for intelligent spam sensing and anomaly detection in online social platforms” , Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708.
[11]. Makhdoom, Imran, et al. “Anatomy of Threats to the Internet of Things.” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, 2019, pp. 1636–1675., doi:10.1109/comst.2018.2874978.
[12]. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. 2018, 25, 53–59. [CrossRef]
[13]. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.
[14]. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294. 8. Leloglu, E. A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136.
[15]. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet 2017, 9, 27.
[16]. Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018.
[17]. Pupunwiwat, Prapassara, and Bela Stantic. “Managing Tag Collision in RFID Data Streams Using Smart Tag Anti-Collision Techniques.” Advanced RFID Systems, Security, and Applications, pp. 155–186. doi:10.4018/978-1-4666-2080-3.ch008.
[18]. Bhardwaj, Manish. “Research on IoT Governance, Security, and Privacy Issues of Internet of Things.” Privacy Vulnerabilities and Data Security Challenges in the IoT, 2020, pp. 115–134., doi:10.1201/9780429322969-7.