

Easy and Secure Hostel Hub

Mrs. Anita S Patil¹, Abhilasha², Akshata Maruti³, Anusha⁴, J Yashaswini⁵

Associate Professor, Department of Computer Science & Engineering¹

Students, Department of Computer Science & Engineering^{2,3,4,5}

Ballari Institute of Technology and Management, Ballari, India

anitha.bijapur@gmail.com, abhilashahiremath3@gmail.com, akshataangadi2809@gmail.com

anuhiremathanusha@gmail.com, yashwinj10@gmail.com

Abstract: *The main objective of our project is to secure the hostel hub using fingerprint authentication mechanism technology. In olden days, hostel management system was used for managing all the hostel related transaction such as student admission, food supply, food menu, payment, etc. This will not capture the check in and checkout in our system, this needs either Radio-Frequency Identification (RFID card) or Finger Print scanner. These sorts of devices and its software were cost too much to install and utilize it. In this paper, we are going to record the check in and checkout time of hostel student using fingerprint authentication. Our literature survey, confirmed that finger-print authentication is more secure than RFID card authentication, henceforth we used finger-print authentication in our project. In future depending upon the trends and techniques we will be upgrading the “Easy & Secure Hostel Hub”, system*

Keywords: hostel hub

I. INTRODUCTION

Web-based applications refer to those which function on a Web browser on different kinds of devices, include desktops, laptops, tablets, smartphones, and mobile phones, and are distributed over a network [1]. This application performs on client-server architecture, featuring the user interface and client-side logic processing via a Web browser. Online sales, Webmail, push notices, and numerous additional functions employing the Internet and mobile network are characteristic functions of web-based applications. These characteristics can be obtainable with great accessibility and adaptability from any location at any time[2, 3]. A person who admits in an institution of higher learning and conducts courses for the purpose to gain the necessary level of authority in a subject under the supervision of an educator is usually referred to as a student. In a more general sense, an understudy is any individual who commits a significant amount of time to a serious educational endeavor on a topic sufficiently significant to be ranked significantly as an important part of a determined endeavor in which such authority is crucial or persuasive[4]. offering adequate accommodation for the students is one of the most efficient methods to manage them successfully. It is essential to develop a method for designating accommodations in hostels which would enable management to make conclusions through offering a greater awareness as to which apartments are habitable and by transporting the necessary data, is the inspiration behind this project.

In addition, there are several methods for addressing HSAP, which includes rule-based models [5, 6], heuristic modeling [7-9], and met heuristic algorithms [11–13]. These approaches can find optimal solutions in an appropriate period of computational time, but they frequently become trapped in the local optimal, which renders them ineffective for domain-specific knowledge [10].

1.1 Hostel Hub Problem Statement

A hostel management system had previously been utilized for managing all of the transactions affiliated with that hostel, involving student enrollment, food supplies, menu items, payments, etc. This precludes our system devices via registering the check-in and check-out.

1.2 Objective

In this paper, we are going to record the check in and checkout time of hostel student using fingerprint authentication. Our literature survey, confirmed that finger-print authentication is more secure than RFID card authentication, henceforth we used finger-print authentication in our project. In future depending upon the trends and techniques we will be upgrading the "Easy & Secure Hostel Hub", system.

II. RELATED WORK

1. Fingerprint Authentication in Smart Home Environment based on Embedded System

The theoretical idea of a "smart home" has increased prominence in the security sector since. One area of concern is the application of biometric fingerprint technology to identity systems, like those used for home access. In a smart home setting, this study created a fingerprint-based identification system using fingerprints and PINs. As an aspect of the hardware, an Arduino Mega

The microcontroller and input/output includes are called 2560. In addition, a fingerprint sensor is a component that can be used for collecting customer satisfaction fingerprints. The study evaluated implementation costs for PIN-and fingerprint-based authentication systems in an embedded system the context with lower implementation costs based on the hardware building design. It illustrates how to link a fingerprint sensor, Arduino microcontroller, mathematical keypad, door lock, and door lock employing an easy-to-understand program.

2. Deep Learning based Radio Frequency Fingerprint Authentication with Chaotic Antenna Arrays.

Employing distinctive and occasional distortions in a received signal—which are contingent on the transmitter's characteristics—radio frequency (RF) fingerprinting is a procedure that offers authentication. We develop a deep learning based authentication technique for Physically Unclonable Wireless Systems (PUWS), which is a significant technological advancement in RF fingerprinting. The basic concept underpinning PUWS is Chaotic Antenna Arrays (CAAs), that can be manufactured at an affordable rate alongside the help of mask-free laser-enhanced direct print Manufacturing simultaneously (LE-DPAM). Using simulation data of 300 CAAs with 4 antenna elements each, we test 5 different convolutional neural network (CNN) architectures under different periods channel conditions in our experiments and compare their authentication performance to those of the most sophisticated RF fingerprinting methods of authentication that are available.

3. Secure and Efficient Online Fingerprint Authentication Scheme Based on Cloud Computing

Protection of biometrics-based cloud computing privacy has grown more and more important. For data outsourcing company e-Finga, Zhu et al. (2018) demonstrated an efficient online fingerprint authentication system which safeguards privacy. Under the presumption that the user's fingerprint data privacy and message security authentication have been safeguarded, the e-Finga mechanism is capable of providing accurate and efficient fingerprint identity authentication services.

Nevertheless, the research we conducted indicates that the deterministic encryption algorithm is utilized by this scheme's temporary fingerprint, therefore diminishes its likelihood of compromising the user's fingerprint characteristics. As a consequence, we offer an e-Finga fingerprint attack the mechanism that is brief in duration. Investigations demonstrate that adversaries can listen in on a user's temporary fingerprint ciphertext and evaluate particular secret settings and fingerprint characteristics.

To prevent the Temporary Fingerprint Attack, we suggest the Secure e-fingerprint methodology. It makes use of learning with oversights samples, that possess homomorphic addition characteristics, to encrypt user's temporary fingerprints.

Analyses demonstrate that that the secure e-finger methodology is able endure an unexpected fingerprint assaults. Whereas the client running time increased by approximately six percent as compared to the unprotected e-Finga scheme, the user's communication cost increased by only 0.3125%. As a result, our method may accomplish efficient safe online fingerprint authentication.

The usage of single user authentication may have played a role in the issue of excessive authority. We suggest applying the Secure e-finger methodology as a framework for a threshold evaluation based on generic traits.

4. Effect of Smaller Fingerprint Sensors on the Security of Fingerprint Authentication

A fingerprint that has been partially as opposed to completely captured will have been received if an insufficient fingerprint sensor has been employed. The amount of characteristics that are compared during matching diminishes as the size of the partial fingerprints maintained in the database becomes reduced. Unfortunately, it is possible to generate "Masterprints" for a few details.

Many individuals which have been saved in the database can be pretending to be employing masterprints. A Masterprint can be developed if a partial image is 15% of the whole image's size. We investigate the vulnerability various smaller partial images are to the Masterprint. We use partial images which vary from 9% to 48% of a full image since different sensors have different sizes. Our findings demonstrate that the sizes of partial pictures and sensors have an important effect on the security of partial fingerprint authentication. With diminishing partial envision size, the fraudulent matching rate increases; alternatively, the more significant the increase in the counterfeiting matching rate, resulting in decreased false matching rates.

5. Fast Fingerprint Authentication Based on Ultrasonic Guided Waves

A combination of the technology's outstanding precision and trustworthiness, fingerprint scanning is a biometric technology which is utilized extensively in a variety of sectors, particularly mobile payment and intelligent security. When fingertips are humid, slippery, or dusty, ultrasonic fingerprint scanning will solve the authentication challenge more effectively than capacitive and optical fingerprint scanning.

It can be challenging to deliver quick and accurate ultrasonic fingerprint scanning and authentication in an extensive physical domain, although. The paper suggests an original approach for dealing with the aforementioned problems by combining tomography via deep learning. In the present research, ultrasonic guided waves have been employed to monitor the wave field changes of a plate-like structure, facilitating fingerprint reconstruction at any location throughout an extensive physical domain.

Mask region convolutional neural network (Mask R-CNN) and fast inversion tomography (FIT) can be employed to precisely evaluate and identify the fingerprint. Data and image processing processes demonstrate that the FIT has the capability of accurately defining fingerprint aspects in the array, and that ultrasonic fingerprint matching in an expansive physical geographical area can be performed quickly and precisely using a post-processing methodology based on the Mask R-CNN model. This enhances the security and comfort of fingerprint-identifying devices substantially.

Architecture Diagram

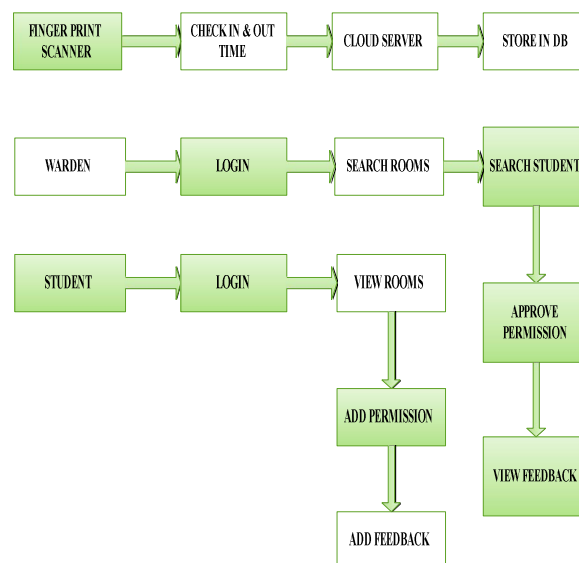


Fig 1:Architecture diagram

III. RESULT AND ANALYSIS

Enhance the security and efficiency of hostel management through the implementation of a fingerprint authentication mechanism. This is a great initiative, especially considering the limitations of traditional hostel management systems and the need for more secure methods of authentication. Using fingerprint authentication over RFID cards is well-founded, as it offers higher security and eliminates the need for physical cards that can be lost or stolen. Additionally, while initial installation costs may be higher for fingerprint scanners, the long-term benefits in terms of security and convenience can outweigh these expenses.

Screenshots

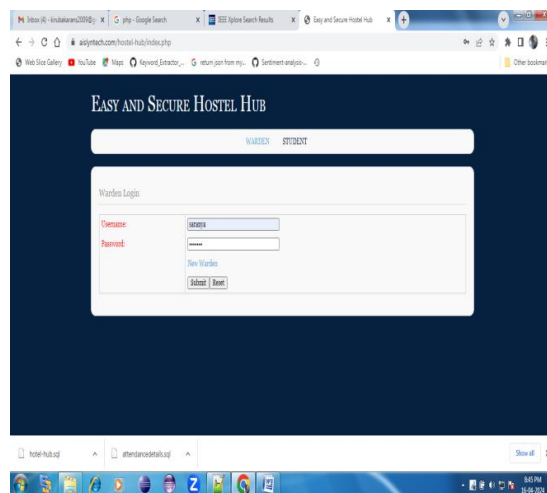


Fig 2: Login with credentials

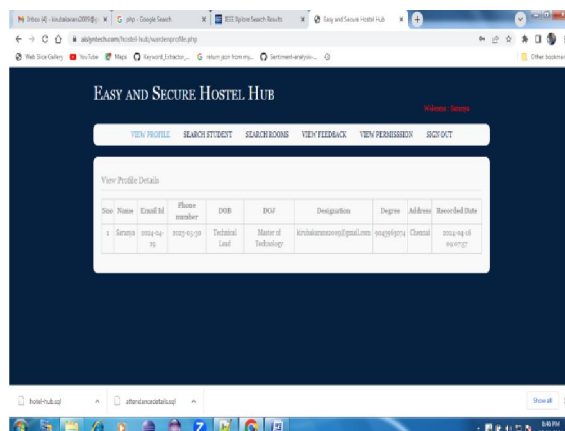


Fig 3: View profile

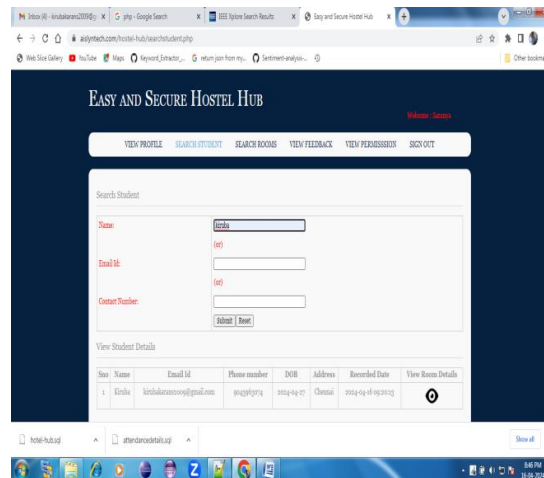


Fig 4: Search Student

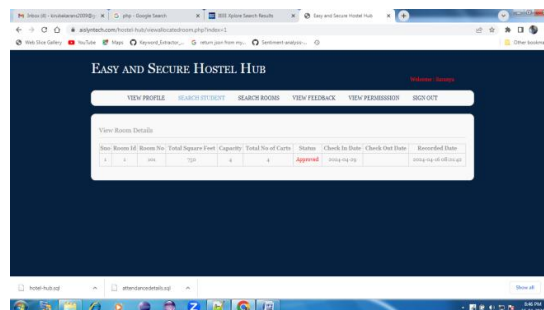


Fig 5: Displays Status Approved

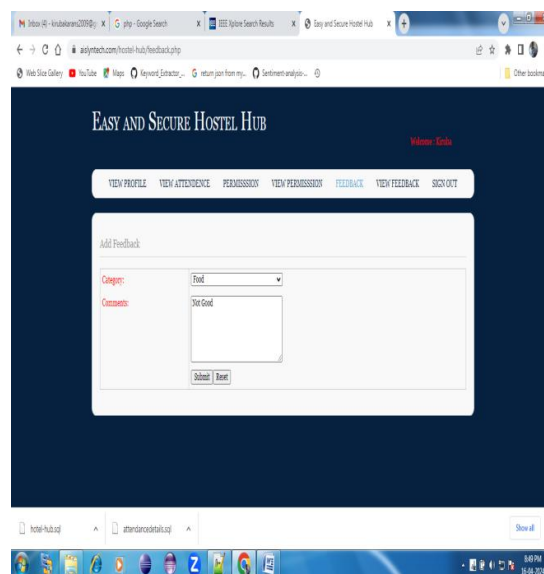


Fig6: Enter Fields Of Feedback

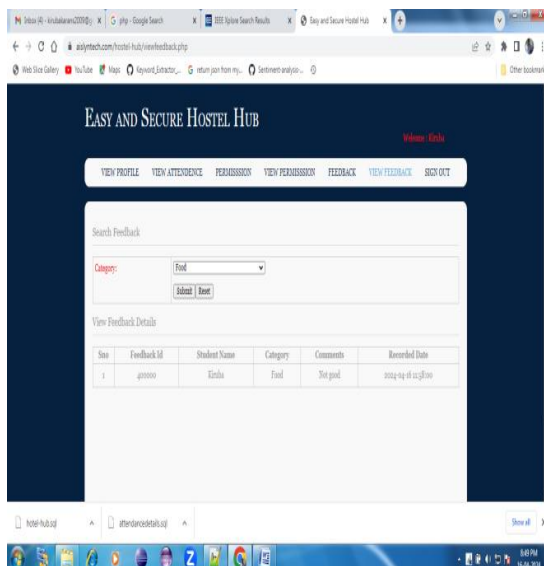


Fig 7: View feedback page

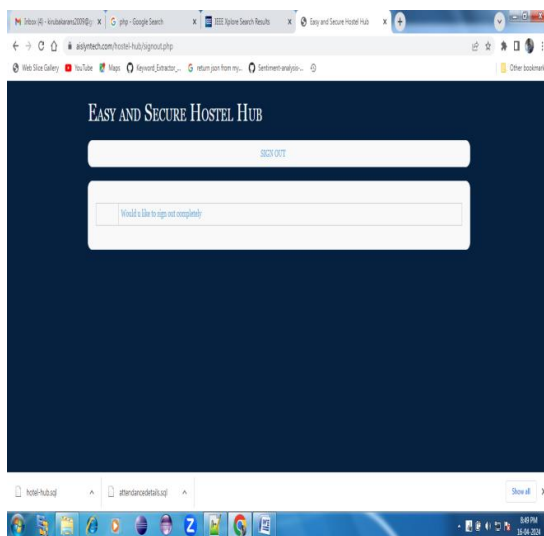


Fig 8: Signout page

IV. CONCLUSION

In this paper, we are going to record the check in and checkout time of hostel student using fingerprint authentication. Our literature survey, confirmed that finger-print authentication is more secure than RFID card authentication, henceforth we used finger-print authentication in our project. In future depending upon the trends and techniques we will be upgrading the “Easy & Secure Hostel Hub”, system. Blockchain technology is given prominence in many applications where security and transparency is very important. Yet, considering the development and application expenses associated with maintenance, it has not been widely adopted by numerous businesses in their management processes.

REFERENCES

- [1]. Holl, K., Elberzhager, F.: Mobile application quality assurance. In: Advances in Computers, vol. 112, pp. 1–77. Elsevier (2019)

- [2]. Roberts, M.L., Zahay, D.: Internet Marketing: Integrating Online and Offline Strategies. Cengage Learning (2012).
- [3]. Varia, J., Mathew, S.: Overview of Amazon Web Services. Amazon Web Services, pp.1–22(2014)
- [4]. George, J.M., Jones, G.R.: Understanding and Managing Organizational behavior (2012)
- [5]. Olatunji, K.A., et al.: Fuzzy—based accommodation allocation system. Int. J. Eng. Sci. Res. Technol. **4**(8) (2015) ISSN: 2277-9655
- [6]. Bolaji, A.L.A., Michael, I., Shola, P.B.: Optimization of office-space allocation problem using artificial bee colony algorithm. In: International Conference on Swarm Intelligence pp. 337–346. Springer, Cham (2017)
- [7]. Wei, Y., Xue, B., Ning, Z., Zhicheng, B.: The research of intelligent storage space allocation for exported containers based on rule base. In: Proceeding of the 2012 International Conference of Modern Computer Science and Applications, pp. 421–425. Springer, Berlin (2013)
- [8]. Rodrigues, E., Gaspar, A.R., Gomes, Á.: An evolutionary strategy enhanced with a local search technique for the space allocation problem in architecture, Part 1:Methodology.Comput.Aided Des. **45**(5), 887–897 (2013)
- [9]. Gajjar, H.K., Adil, G.K.: A dynamic programming heuristic for retail shelf space allocation problem. Asia-Pacific J. Oper. Res. **28**(02), 183–199 (2011)
- [10]. Obit, J.H., Junn, K.Y., Alfred, R., Bolongkikit, J., Sheng, O.Y.: An investigation towards hostel space allocation problem with stochastic algorithms. In: Computational Science and Technology, pp. 227–236. Springer, Singapore (2019)
- [11]. Zeng, M., Cheng, W., Guo, P.: Modelling and metaheuristic for gantry crane scheduling and storage space allocation problem in railway container terminals. Discrete Dyn. Nat. Soc. (2017)
- [12]. Da Silva, G.C., Bahiense, L., Ochi, L.S., Boaventura-Netto, P.O.: The dynamic space allocation problem: applying hybrid GRASP and Tabu search metaheuristics. Comput. Oper. Res. **39**(3), 671–677 (2012)
- [13]. Chang, Y., Zhu, X.: A novel two-stage heuristic for solving storage space allocation problems in rail-water intermodal container terminals. Symmetry **11**(10), 1229 (2019).