High Protection Bank Locker Security Alert System using Voice Authentication Based on Wireless Sensor Network

Meenakshi Shunmugam[*1,a], Satya Rajesh Kunchaparthy[2,b], Baby Kalpana[3,c]

[1*]*Department of Electronics and Communication Engineering, R.M.K. Engineering college, RSM Nagar, Gummidipoondi, Taluk, Kavaraipettai, 601206, Tamil Nadu, India.*
[2]*Department Of Computer Science, CSTS Govt. Kalasala, Jangareddigudem, WG Dist, Andhra Pradesh,India.*
[3]*Department of CSE, P.A.College of Engineering and Technology, SH 19, Puliyampatti, Pollachi, Tamil Nadu 642002, India.*

Corresponding author: [a]shunmugam.meenakshi@gmail.com
[b]ksatyarajeshcse@gmail.com
[c]drybk.pacet@gmail.com

Abstract.A bank is an organization that provides financial effectiveness and extends financial administration such as giving money, saving things and so on. In the existing method, both bank workers and clients should be given keys to open storage locker. There is a chance of losing the key that makes the insecurity system, and many keys can be duplicated. The system cannot coordinate with the current quick pacing computerized technique. In this method, face identification, Voice recognition, GSM (Global System for Mobile communication), providing a secure, valid and easy to handle. The first step is voice acknowledgment, and the second step is Face recognition, and later by logging based to enter the OTP password via GSM. Therefore, GSM security is more developed and secure than developed personal devices. Machine Learningis the wireless sensor network's interactions as a consenting lock that selects and offers personalized voice recognition access. Wireless Network-based structure includes a high alert of each client's registration and checkout with the required data.
Keywords: Bank Locker Security Alert System, Voice Authentication, Wireless Sensor Network.

1. INTRODUCTION

In a verification system, the person who wants to be identified usually submits a statement of identity to the system by the name of the person's identification. The system rejects or accepts the submitted identity. In the identification system, the system establishes the person's identity, or if the person does not request the identity of the person and does not register the person in the system database, the system fails. The person is a voice recognition verification system, and the term verified identity verification and identification is synonymous in the broadest sense. Accurate automated identification is increasingly important to the functioning of our increasingly electronically interconnected information society.

Traditional automated wireless communication identification technology is used to verify people who use items know (such as personal identification numbers) or identities. Its reliability is not sufficient to meet the security requirements of the communication method. A common problem with these techniques is that they cannot distinguish between unauthorized persons and scammers and those who impose access privileges from authorized people. Voice recognition is a technique that uniquely identifies a person based on physical or behavioral characteristics. The identity for personal identification so can naturally distinguish between unauthorized individuals. However, unlike some traditional techniques, voice module technology cannot establish absolute personal identity. This security alert system is human-oriented and is more accurate than traditional password-based systems.

International Conference on Environmental Engineering and Material Sciences
AIP Conf. Proc. 2655, 020027-1–020027-4; https://doi.org/10.1063/5.0115687
Published by AIP Publishing. 978-0-7354-4475-1/$30.00

2. RELATED WORKS

A security system of safety measurement has been introduced these days for such locations and applications [1]. However, with the wide assortment of security strategies, wireless communication methods also change and expand step-by-step. Accessible can ensure homes and foundations to some extent [2]. Yet, that is not the case with basic facilities such as military workplaces and logical laboratories. These locations require a very secure system at every point on the schedule to ensure significant information and cash [3]. An assortment of security systems is currently accessible. For example, these days' robbers have a ton of current gear, so confidential phrases guarantee to keep resources under the right of protection [4]. As one reference suggests, when a person loses a good opportunity, he loses his opportunity well to be regained; however, if a person loses his vital abundance, it is necessary to invest a little to remember [5]. To protect our asset banks, offer different benefits such as securing storage locations for their customers to store their resources. In this risk perspective, the individual clear check Dave can see registered genuine customers and counterfeits is no longer interested. Passwords, considering everything [6].

Security is the most basic problem in this nomadic world; people find no way to provide physical security for their mysterious resources [7]. In the system's inevitable society, people can access their information anytime and anywhere without any effort. People's situation is also fraught with dangers, and certainly, other people can get comparative information anytime and anywhere [8]. Banks are institutions that improve economic efficiency and expand financial services, such as issuing cash and saving assets [9]. The main thing in a person's life is the savings and safety of the money received concerning its financial visibility. Protection against threats requires security and can ensure security. Today, security has become a key issue in maintaining our data confidentiality in homes, office fees, institutions, laboratories, and other places to prevent unauthorized people from using it. In the past, there have been few security measures to prevent unauthorized access [10].

3. MATERIALS AND METHOD

The unique voice recognition-based bank locker system improves the traditional bank storage system that uses keys. The Voice recognition confirmed bank storage system is just as easy to use and maintain. Security is an essential concern, and in this occupied, serious world, people cannot find approaches to protect their classified effects physically. Since all things being equal, finds an alternative that can provide undisputed protection in the same way as an atomized one. In a ubiquitous organization society, people can access their data anytime and anywhere without any hassle. Individuals face the maximum risks that other people can access the same data anytime and anywhere without any drag. Because of this fear, personal innovation, which can identify registered real customers and fakes, is currently generating interest. The system uses unique Voice recognition detection and picture capture system examines unique Voice recognitions.

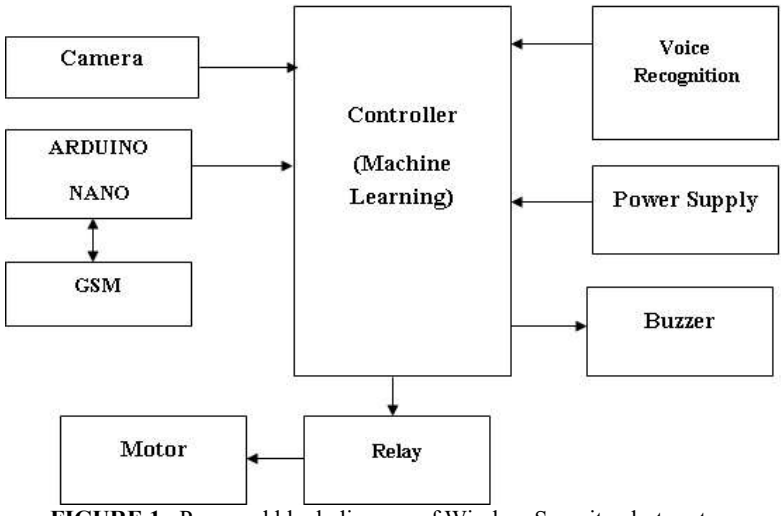

FIGURE 1. Proposed block diagram of Wireless Security alert system

Fig. 1: Additionally, it captures the client's picture and records the client picture case. The client does not match the current picture of a particular client, sending a message to the supervisor and the concerned bank client. Additionally, the ringer is used to make the bank manager think about the person being rejected immediately. The off chance that it matches both the unique icon and the picture, the store opens, and voice acceptance identifies the sound highlights of a discourse seen differently among people.

4. RESULT AND DISCUSSION

The face-based secure access system is becoming increasingly famous for some applications, for example, smartphone opening, internet business and e-banking. The ease of unconstructed imaging using a basic shading camera has led to the acceptance of faces for use in a safe system, operating in various situations. Towards the end of this route, cell phones are asked to capture facial features to confirm subjects with interest. The only factor to note in a smartphone-based biometric system is a single data catch.

TABLE 1. Analysis of Precision (%) F-Measure (%) based on the smart security system

MEASURES	Machine learning	Convolutional neural networks	Alex Net
Precision (%)	75.1	62.1	60.1
Recall (%)	78.5	60.5	61.6
F-Measure (%)	74.1	60.6	58.2

Table 1 gives the:use of a smartphone-based biometric system for verification is exceptionally planned to accommodate the client for unauthorized confirmation from any field and to allow the capture of biometric information non-auxiliary along these lines. The opportunity to capture updated information, especially cell phone-based face recognition, can be abused by unsuspecting customers. The noble accessibility of facial images on various web-based media locales can be used to obtain unauthorized access in such unedited biometric systems operating on cell phones. Any attempt to gain a secure entry by presenting the antiquity of the true subject is presented. Each of the three authors has made equal contributions to this method.

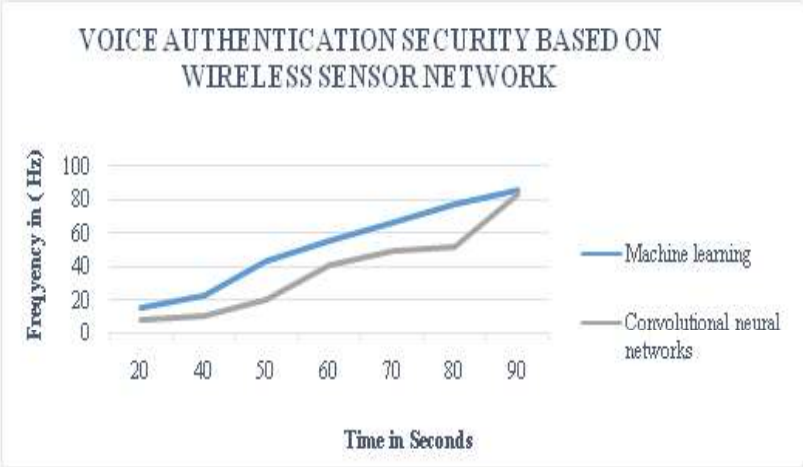

FIGURE 2. Analysis of Wireless security system based on Machine learning

Fig. 2 gives the:face picture on an electronic screen to access a face picture and a biometric structure aimed at the smartphone. On the other hand, the picture can be printed on method, and the smartphone information can be presented back in the catch system. The inability to differentiate such attacks on face-based biometric structures invalidates the issue of security in terms of confrontation-based recognition. Such attacks can be triggered by the introduction of Assault Discovery (PAD) calculations attached to the biometric system. Several methods have been suggested to combat such attacks on face-based biometric structures that influence live effort and introduction attacks' structural features.

5. CONCLUSION

Individual abilities are performing security alerts appropriately for wireless communication. After using the tests, the results check the functions of the individual function. Bank locker security system with the goal that they could try to break the system and use their fingerprints in the system. Ourvoice recantation-based lock system has a high accuracy rate and Precisionto understand fingerprints, strengthening continuous integration with clients and providing more stringent security. By replacing and putting insecure detail extraction, the wireless sensors are more accurate and faster than our past highlight extraction. The sure to check in our proposed system to see if the unique fingerprint is a significant client. Large-scale evolving financial innovation has streamlined the way banking practices are handled security efforts at banks will contribute fundamentally to attacks on consumers in the wild. The Machine learning systems are most important considering the vulnerabilities and causality in general claims, and banks should meet some models to ensure a reliable and safe financial environment for their customers.

REFERENCES

1. Karakaya and S. Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-4, doi: 10.1109/ISDFS.2018.8355381.
2. Y. Lin and J. Chang, "Improving Wireless Network Security Based On Radio Voice recognition," 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Sofia, Bulgaria, 2019, pp. 375-379, doi: 10.1109/QRS-C.2019.00076.
3. X. Wu, W. Fu, D. Mu, D. Mao, H. Zhang and W. Zheng, "Improving the Security of Wireless Network Through Cross-project Security Issue Prediction," 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 2020, pp. 1179-1184, doi: 10.1109/ICCC49849.2020.9238816.
4. N. Siasi, A. Aldalbahi and M. A. Jasim, "Reliable Transmission Scheme Against Security Attacks in Wireless Sensor Networks," 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 2019, pp. 1-6, doi: 10.1109/ISNCC.2019.8909123.
5. Y. Kong, B. Lyu, F. Chen and Z. Yang, "The Security Network Coding System With Physical Layer Key Generation in Two-Way Relay Networks," in IEEE Access, vol. 6, pp. 40673-40681, 2018, doi: 10.1109/ACCESS.2018.2858282.
6. R. M. H, Shrinivasa, C. R, D. R. M, A. N. J and K. R. N. S, "Biometric Authentication for Safety Lockers Using Cardiac Vectors," 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICPECTS49113.2020.9336976.
7. V. K. Kolur and P. Reshmi, "IoT based Security System for Organization," 2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC), Vijiyapur, India, 2020, pp. 1-4, doi: 10.1109/B-HTC50970.2020.9298007.
8. S. Hossain, M. I. Ahmed and M. Niaz Mostakim, "A Prototype of Automated Vault Locker Solution for Industrial Application," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 2019, pp. 1-6, doi: 10.1109/ICASERT.2019.8934754.
9. A. Chikara, P. Choudekar, Ruchira and D. Asija, "Smart Bank Locker Using Voice recognition Scanning and Image Processing," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 725-728, doi: 10.1109/ICACCS48705.2020.9074482.
10. A. Kumar, P. Sood and U. Gupta, "Internet of Things (IoT) for Bank Locker Security System," 2020 6th International Conference on Signal Processing and Communication (ICSC), Noida, India, 2020, pp. 315-318, doi: 10.1109/ICSC48311.2020.9182713.