International Journal of Informatics, Information System and Computer Engineering

Security Service Monitoring Using Face Recognition, Near Field Communication and Geolocation Technology

Eko Budi Setiawan, Rizky Milan Alpasya Wijaksono*

Department of Informatic Engineering, Universitas Komputer Indonesia, Bandung, Indonesia
*Corresponding Email: eko@email.unikom.ac.id

ABSTRACTS

In a company that provides security services, monitoring, and field control activities are carried out daily to ensure that all designated checkpoints are properly supervised. This research aimed at facilitating the management in summarizing the field control activity reports and enhancing the supervision of the field security personnel conducting field control. The application is developed using Golang, JavaScript, and Kotlin programming languages and utilizes PostgreSQL as its database. The application is web-based for administrative personnel and mobile-based for field security personnel. The technology used in building this application includes face recognition, GPS, and location-based service and NFC reader. Based on the implementation and testing results, it is found that the developed application functions according to the established workflow. The fastest face recognition detection time was 1.22 seconds, and the RFID tag was successfully detected at a distance of less than 4 cm and an average time of 0.378 seconds, and the use of geolocation provides accurate position results.

ARTICLE INFO

Article History:
Received 03 Sept 2024
Revised 01 Nov 2024
Accepted 29 Nov 2024
Available online 08 Dec 2024
Publication date 01 Jun 2025

Keywords:
Field control,
Face recognition,
Geolocation,
NFC,
Monitoring.

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

1. INTRODUCTION

In a company that provides security services, monitoring, and field control activities are carried out daily to ensure that all designated checkpoint locations are continuously supervised. The company's management has the right to expect its employees to adhere to appropriate ethical standards. Employees who act inappropriately or beyond reason can damage the business. Therefore, the company has established rules and procedures aligning with proper working practices to ensure that all activities run smoothly. Work procedures are a series of interrelated work arrangements with a visible sequence of stages and paths that must be followed to complete a task area. Neglecting work becomes a problem for every company or business. This can affect customer trust and decrease the company's credibility (Hasan, 2023).

Employees need supporting tools to carry out work activities according to company management's established work procedures. Technology is the key to achieving this goal (Hayati, 2019). However, based on the real conditions in the field and supported by the interviews, all employees, including administrative staff and security personnel, only use the Whatsapp Messenger chatting application in their work activities, especially in reporting. According to the company's feedback, relying solely on this messaging application makes it quite challenging for management to compile reports, especially monthly and annual reports. This is caused by several factors, such as the increasing number of monitoring photo evidence daily, which quickly fills up the employees' device memory, leading to routine deletions and, consequently, the unintentional deletion of the photo evidence for reporting.

The higher the quality of the company's performance, the greater the satisfaction and trust of the customers. However, the lack of facilities to view reports in real-time or periodically poses a challenge. Currently, administrative staff can only compile reports if there is a specific incident and it is requested by the supervisor, meaning customers can only receive limited report results. Certainly, to enhance service quality and trust, innovation and development are essential to achieve this goal. One security patrol monitoring issue concerns security personnel who often engage in fraudulent activities, such as not performing their patrols and staying only at the security post. This problem is considered highly critical because real-time monitoring of the situation could be improved, so if something goes wrong, security personnel won't observe it during their duty (Irsan & Sulaiman, 2019).

Relying solely on photos sent through a messaging application, the management cannot directly monitor the location or time the photo was taken. Since this company operates in the security services sector, this becomes crucial. If an incident requiring photo evidence occurs, the photo becomes invalid because there is no supporting evidence regarding its authenticity.

This research aims to improve the quality of company services and assist the security monitoring process in real time and avoid fraud committed by security officers when carrying out guard duties so as to make the work results more accurate and reliable.

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

2. METHOD

The research method used in this study is the descriptive method. The descriptive method is one of the methods to solve the problem being studied by illustrating the condition of the subjects or objects in the current research based on the visible facts or existing in the field. Descriptive research aims to discover facts with accurate interpretation. Researchers can be involved in a combination of data from observations, interviews, and documentation to conduct the analysis (Tenhunen et al., 2023). Fig.1. is the research process steps undertaken in this research.

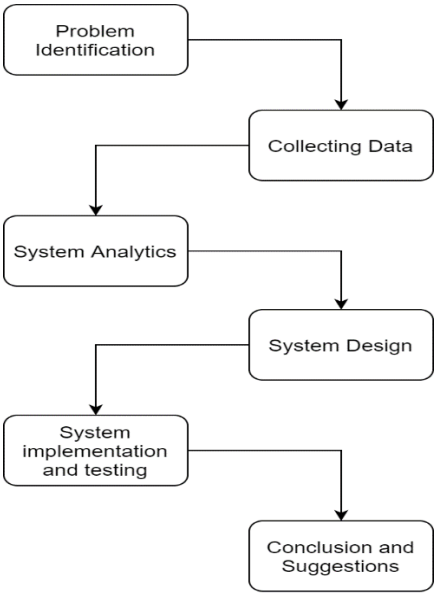

Fig. 1. Research step process

2.1. System analysis and design

The system architecture is a general representation of how the system operates and interacts with each other. The application development utilizes both website and mobile platforms. A system architecture illustrating how this system operates is required to construct a system to address the issues in this research. The following is the website system architecture used in Fig. 2.

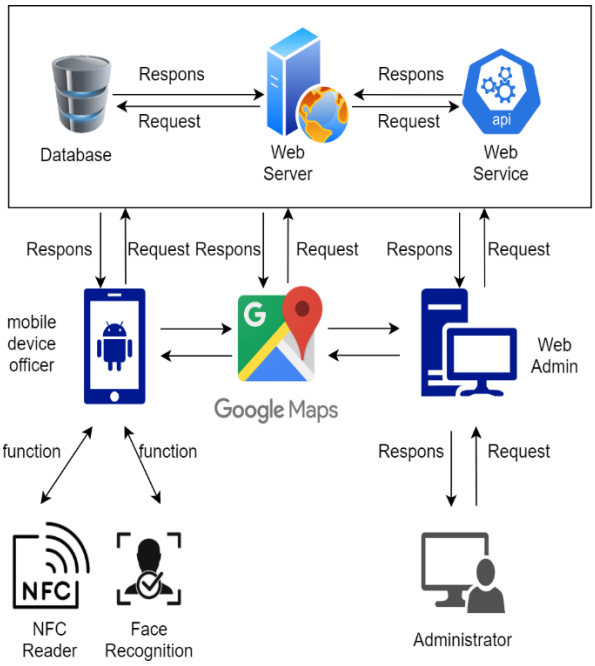

Fig. 2. Architecture System

Information regarding Fig.2 is:

1. The web service acts as the backend tool, containing endpoints that will be used by all users, whether through the website or mobile devices, and serves as a link between the user interface with all its functionalities and the server.
2. Admin uses a gadget or computer device connected to the internet to access the admin website domain address. The admin manages the system directly to ensure smooth operation and generate useful information for the company.
3. The Field Security Officer's page uses a mobile device. It needs to access the system using the internet, allowing users to use the application system according to their roles and duties.

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

4. A web server is a type of software installed on a server that processes requests for web pages through HTTP or HTTPS protocols, sent by clients known as web browsers. It then returns the requested content as HTML documents. In this context, Nginx will be the chosen web server.
5. The database is a place to store a collection of data that will be processed by the application system being developed. The database used in this application development is PostgreSQL (PSQL).
6. Google Maps API in this application development aims to obtain location data from field security officers and display it within the system. It aligns with the concept of Location Based Service, functioning as a service to identify the positions of field officers to determine if they are in the specified area.
7. Android devices request phone coordinates, and GPS satellites provide the coordinates of the smartphone's position.
8. Android devices connect to the internet.
9. The Mobile Application Detects Fake Location Usage.
10. The mobile application detects the user's face.
11. The mobile application can scan RFID cards using the NFC reader feature.

2.2. Location Based Service Detection

In general, location-based services can be defined as services that use the ability to dynamically determine and deliver a person's location in a cellular network through their devices (Orabi et al., 2023). From the perspective of mobile users, location-based services (LBS) are typically services accessed or offered through their mobile devices (Wang et al., 2023).

After using GPS technology to detect the location of field security officers, this research also employs Location Based Service (LBS), which encompasses all information services accessible via mobile devices through the network and can display the geographical position of the users' mobile devices (Setiawan & Setiyadi, 2021). It is used when field officers are on patrol. Related to the earlier explanation about GPS, LBS will act as a supporting tool for monitoring. Both admin and field officers can access the travel history and perform tasks at predefined locations using LBS. Thus, utilizing LBS will serve to identify the positions of field officers to determine if they are in the specified area. Below is Fig. 3, depicting the usage of LBS technology.

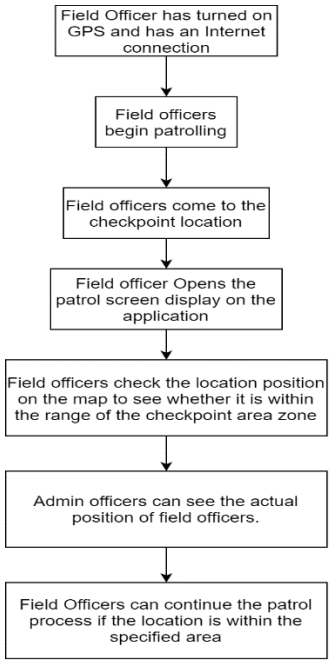

Fig. 3. Utilization of LBS Technology

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

2.3. Fake GPS Detection

Creating an application that utilizes positioning location technology using maps always faces the threat of fraud from Fake GPS (Chang et al., 2018). As the name suggests, fake GPS means a false location, and its main function is determining a false location for the user (Tanış & Erhan Yalçın, 2024).

Typically, fake GPS requires additional applications, or in other words, users need to install a fake GPS application to use it. The main purpose of this fake GPS application is to ensure that the user's position is not accurately known (Altaweel et al., 2023), both by the system and by those tracking them. This is directly related to the application being developed, where the location of the field officers must be accurately detected to perform patrol activities effectively. If the officers use this fake GPS application, it will indicate dishonesty in carrying out their duties. Therefore, in this study, an application for officers will be developed to counter or be an anti-the-fake GPS application. Below is Fig. 4. outlining the process flow to detect the use of a false location in the developed application.

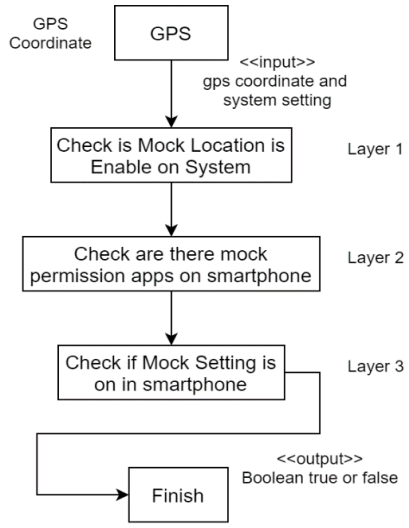

Fig. 4. Fake GPS Detection Process

2.4. Face Recognition Detection

Face recognition is the problem of pattern recognition based on visual facial patterns. A face is a three-dimensional object influenced by lighting, pose, expressions, and other factors (Rusia & Singh, 2023). In the context of technology usage, Face recognition technology is designed to identify human faces by analyzing unique patterns and can re-identify faces under diverse conditions. Presently, face recognition is applied in computer technology as a biometric authentication application and in human-computer interaction surveillance applications (Shivanna & Venkatesiah, 2024).

ace recognition offers several advantages compared to other biometric systems like fingerprint or iris recognition. One of its key benefits is its natural and unobtrusive nature, as it allows detection from a distance and can operate discreetly. As a biometric system, face recognition relies on well-studied facial attributes and functions through two main approaches: face verification (authentication) and face identification (recognition).

Face verification involves matching a person's face with the registered face images in the system, enabling the identification of that person's identity. Examples of its applications include immigration permit verification using e-passports or a face recognition application system for student attendance. Face identification involves comparing a face against multiple entries in a database, with the goal of identifying the closest match, such as in-room security application systems where only specific individuals can enter the room. Each person authorized to enter the room

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

is registered in the database, and the application selects individuals by searching for facial similarities based on queries in the database (Qi et al., 2022).

A face recognition system typically involves four main processes: face localization, normalization, feature extraction, and matching. These workflows are illustrated in Fig. 5.

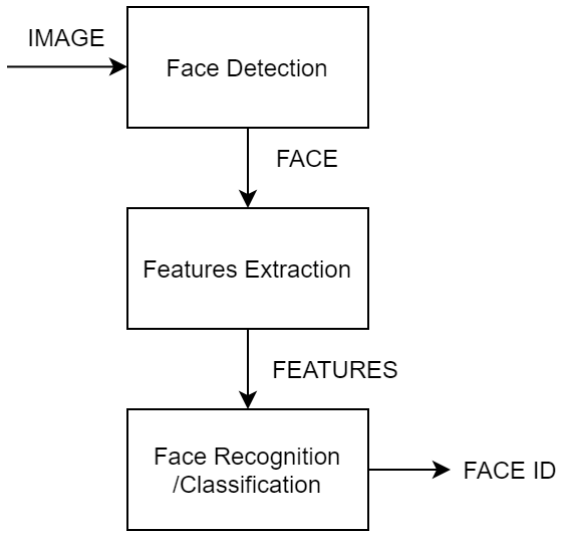

Fig. 5. Face recognition workflow

Face Detection involves separating the face from the background image. In the case of a video, the face will be marked with a frame as a separator between the face and the background. This detection estimates the face's scale and localizes components such as eyes, nose, mouth, etc. Face Normalization is done to geometrically and photometrically normalize the face. In this stage, sophisticated methods are needed to recognize facial images with various poses and lighting. The geometric normalization process transforms the face into a standard frame by cropping the face.

Various face recognition techniques have been introduced in research, with the primary focus on enhancing accuracy. One of the recent advancements in face recognition technology is FaceNet, which utilizes deep convolutional networks and triplet loss for training data. However, the training process is computationally intensive and time-consuming. By integrating TensorFlow machine learning and pre-trained models, the required training time is significantly reduced (William et al., 2019).

Regarding the implementation of face recognition technology, the author has studied several previous researches, including an advanced attendance system using face recognition and android (Susanto et al., 2021), designing an online attendance system with face detection and geofencing based on Deep Learning on the Android platform and research on the performance of face detection and recognition using Baidu AI, which showed twice the speed compared to Face++ in direct detection, with higher recognition accuracy, helping to prevent static image fraud (Chen et al., 2020).

Additionally, research attempts to implement an AI-based Attendance System with computer-based face recognition using surveillance cameras, focusing on speed and face recognition accuracy (Nithya et al., 2022). There is also research on designing an attendance system based on the Internet of Things (IoT) using the IEEE 2413 standard for the IoT architectural framework in face, fingerprint, and QR Code recognition (Abd El-Mawla et al., 2022). Finally, the research aims to design a student daily attendance system that can track real-time attendance using face recognition to eliminate manual input errors (Widjaja et al., 2023).

FaceNet is a high-accuracy face recognition system developed by Google

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

researchers. It uses a Deep Convolutional Neural Network (Deep CNN) to extract facial features and transform them into a vector, known as an Embedding Vector. This vector helps to map the similarities between different faces. FaceNet employs Deep CNN models like ZF-net or Inception. The Face Embedding vector represents the extracted features from a face, which are then compared to vectors from other faces. Vectors that are close to each other may indicate the same person, while those that are farther apart likely represent different individuals. The classification model takes these face embeddings as input and predicts the identity of the face. The FaceNet model generates embeddings for a given facial image, which are used in the classification process. Additionally, it processes the face to create embeddings that can be stored and later used as input for the classification model (Fortuna & Khaeruzzaman, 2022).

TensorFlow Lite is a library designed to execute machine learning models on mobile and edge devices. It is optimized to perform machine learning tasks efficiently on devices with limited resources. Currently, the binary size of TensorFlow Lite is approximately 1MB when all supported operators are included in 32-bit ARM builds (Sahin et al., 2022).Furthermore, TensorFlow also aids in creating artificial neural networks that resemble the human brain on a large scale (Sharma et al., 2021). TensorFlow has two main components:

1. Protocol Buffer (.pb) containing the graph and model for running the tested model.

2. Runtime that executes the graph.

In implementing TensorFlow Lite based on Android mobile, the Mobile FaceNet library is utilized for real-time face recognition in the Android application. FaceNet is an efficient CNN model created for real-time, high-precision face verification on mobile devices. It was developed by researchers at Watchdata Inc. in Beijing. Mobile FaceNet delivers impressive speed and accuracy, with a model size of just 4.0 MB. Its accuracy is comparable to that of larger models such as FaceNet (Xiao et al., 2018).

RESULTS AND DISCUSSION

2.5. Application Implementation

Application implementation explains the interface implementation of Android and website applications. The interface implementation of the Android application can be seen in Fig.6.

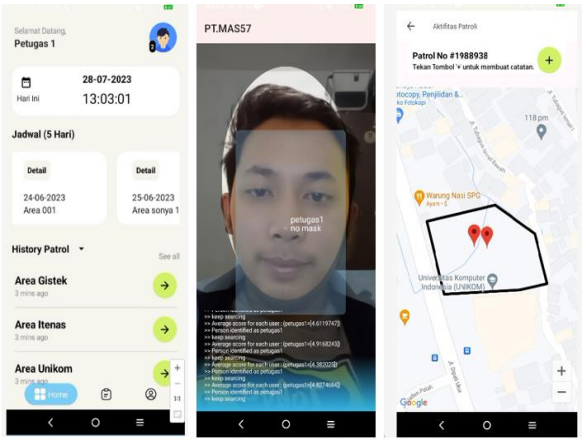

Fig. 6. Mobile interface implementation

Fig. 6. contains the display of the Android application, showcasing the main page, face recognition page, and the main patrol page. Next, below is Fig.7. which represents the implementation of the website application.

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

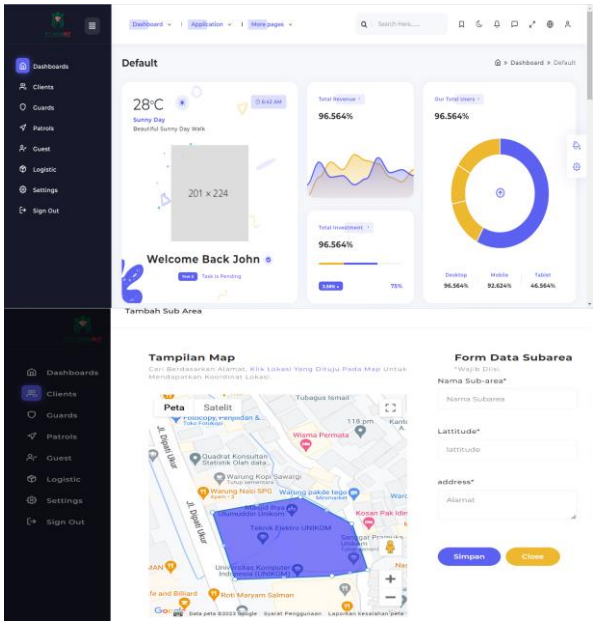

Fig. 7. Website implementation

2.6. Face Recognition Accuracy Result

The performance testing of face recognition was conducted through a series of experiments under specific conditions that could potentially affect the performance of FaceNet, one of the technologies used for the face recognition process. To test the face recognition performance, two aspects were examined: first, the time required for the face recognition process, and second, the effect of the number of faces detected by the camera during the face recognition process. This testing is divided into two phases: the first involves measuring the time taken during the face recognition process, and the second focuses on how the number of faces appearing in the camera frame can affect the face recognition results. Fig. 8. show the face recognition testing process.

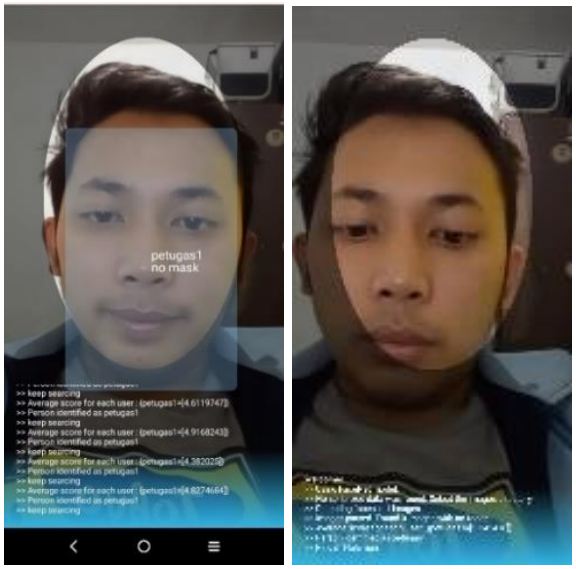

Fig. 8. Face recognition testing

Below are the output data from the face recognition testing based on the two phases discussed. There are tables 1 and 2 for each test result. The accuracy values were obtained from the calculation of the FaceNet model matrix. The Euclidean distance method was used, where the Euclidean distance is always greater than or equal to zero. If the measurement result is zero, then the two vectors are identical. However, if the measurement result is high, the two vectors are not identical.

Table 1. Face recognition time testing results.

Light intensity	Time (seconds)	Accuracy Value
bright	2,41s	10,6548
bright	2,44 s	5,37643
bright	1,49 s	6,38749
bright	1,84 s	4,98735
bright	2,20 s	4,57837
bright	2,49 s	5,67948
bright	1,22 s	5,37643
bright	1,60 s	7,98479
bright	2,60 s	5,23432
bright	2,81 s	8,23423

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

Light intensity	Time (seconds)	Accuracy Value
bright	1,79 s	8,73984
bright	2,68 s	9,92883
bright	2,77 s	11,0920
bright	1,31 s	12,9838
dim	1,33 s	6,88342
dim	2,00 s	9,37422
dim	2,92 s	5,34223
dim	2,99 s	10,8549
dim	1,98 s	5,00231
dim	1,23 s	8,88371
dim	1,32 s	9,28842
dim	2,86 s	5,37182
dim	3,87 s	11,3784
very dim	3,01 s	7,79983
very dim	3,32 s	8,98298
very dim	2,14 s	8,28839
very dim	1,67 s	7,98493
very dim	3,43 s	9,38749
very dim	3,05 s	8,98735
very dim	2,94 s	7,89739

From the table 1 it can be concluded that the face recognition system takes the fastest time, 1.22 seconds, and the longest time, 3.87 seconds, to perform the face recognition process.

Table 2. Results of testing the effect number of detected faces.

Number of Faces in the Camera Frame	Result	Accuracy Value
1 Person	Recognized	6,991075
1 Person	Recognized	6,930216
1 Person	Recognized	6,449585
1 Person	Recognized	6,608981
1 Person	Recognized	5,030202
2 people	Recognized	7,267477
2 people	Recognized	6,233608
2 people	Recognized	5,148525
2 people	Recognized	5,667363
2 people	Recognized	5,79078
3 people	Recognized	6,535877
3 people	Recognized	7,292385
3 people	Recognized	5,444594
3 people	Recognized	7,004122
3 people	Recognized	6,154564
4 people	Recognized	7,592685
4 people	Recognized	5,119465
4 people	Recognized	5,116131
4 people	Recognized	5,302732
4 people	Recognized	7,789023
5 people	Recognized	9,399003
5 people	Recognized	9,593931
5 people	Recognized	8,922676
5 people	Recognized	8,79261
5 people	Recognized	8,085162
6 people	Recognized	8,908319
6 people	Recognized	9,887804
6 people	Recognized	8,699344
6 people	Recognized	7,401134
6 people	Recognized	8,90941

From the Table 2, it can be concluded that the face recognition system can recognize a person's face even when 2-6 other faces are detected in the frame. The system still only recognizes the faces that are registered and correspond to the logged-in user's account within the application.

2.7. NFC Accuracy Result

The performance testing of this Near Field Communication (NFC) implementation was conducted through experiments to observe how distance

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

could affect the speed and accuracy of data reading from the RFID cards.

Below is Table 3, which presents the results of testing the distance required for the sensor to read RFID tags.

Table 1. Results of sensor and RFID tag distance testing.

NFC Distance	Description
1 cm	Success
1,5 cm	Success
2 cm	Success
2,5 cm	Success
3 cm	Success
3,5 cm	Success
4 cm	Success
4,5 cm	Failed
5 cm	Failed
5,5 cm	Failed

Based on the table 3, it can be concluded that the effective reading distance that the NFC sensor from the security officer's mobile device can be used is < 4 cm.

Table 4 showing the results of testing the time required for the sensor to read RFID tags from distances of 1 - 4 cm.

Table 2. Results of reading time based on distance.

Distance (cm)	Time (seconds)	Description
1	0,3	Success
1,5	0,52	Success
2	0,2	Success
2,5	0,09	Success
3	0,12	Success
3,5	0,68	Success
4	0,62	Success
4,5	0,5	Success

Fig. 9 show reading time testing NFC tags.

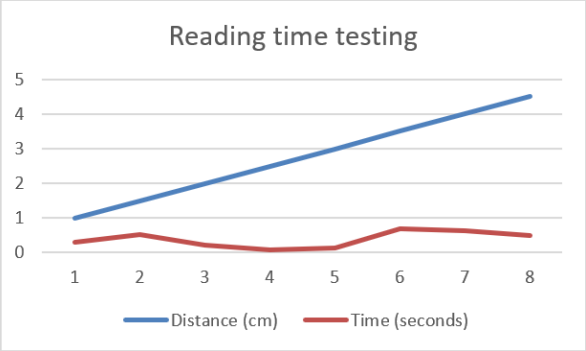

Fig. 9. NFC Reading time testing

From the graph in Figure 12, it can be concluded that the proximity of the tapping distance does not affect the reading time. For this test, the average time obtained was 0.37875 seconds.

From the two experiments above, it can be concluded that the influence of the distance on the speed of RFID data reading time is significant but not too significant.

4. CONCLUSION

Based on the results of program implementation and testing conducted on the security service monitoring application, it can be concluded that the development of the field monitoring and control application using face recognition, NFC and geolocation has been completed and can helped the company's operational activities. This application has facilitated the administrative officers in recording the field control data.

ACKNOWLEDGMENTS

Author would like to thank the Universitas Komputer Indonesia for its assistance in publishing the results of this research.

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

REFERENCES

Abd El-Mawla, N., Ismaiel, M., & Team, A. (2022). Smart Attendance System Using QR-Code, Finger Print and Face Recognition. *Nile Journal of Communication and Computer Science*, *2*(1), pp. 1–16.

Altaweel, A., Mukkath, H., & Kamel, I. (2023). GPS Spoofing Attacks in FANETs: A Systematic Literature Review. In *IEEE Access* vol. 11, pp. 55233–55280.

Chang, Y.-H., Hu, C.-L., Hwang, Y.-L., Ou, C.-W., & Hsu, F.-H. (2018). Fake GPS Defender: A Server-side Solution to Detect Fake GPS. *Proceedings of the 3rd International Conference on Advances in Computation, Communications and Services*, pp. 38–41.

Chen, P., Geng, X., Zou, M., Xu, Q., & Tan, D. (2020). Development and Optimization of Check-in System Based on Face Recognition Technology. *IOP Conference Series: Materials Science and Engineering*, *782*(5), pp. 1–9.

Fortuna, I., & Khaeruzzaman, Y. (2022). Implementation of OCR and Face Recognition on Mobile Based Voting System Application in Indonesia. *IJNMT (International Journal of New Media Technology)*, *9*(1), pp. 20–27.

Hasan, S. (2023). Utilitas Etika Profesi Konsultan IT Terhadap Optimisme Kepercayaan Perusahaan. *Jurnal Teknologi Terapan and Sains 4.0*, *4*(1), pp. 917–922.

Hayati, L. N. (2019). Sistem Monitoring Karyawan Dengan Metode Lbs (Location Based Service) Berbasis Android. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *2*(1), pp. 61–66.

Irsan, M., & Sulaiman, H. (2019). Pemanfaatan Teknologi Near Field Communication(Nfc) Dan Face Recognition Sebagai Media Monitoring Keamanan (Patroli) Anggota Security. *Faktor Exacta*, *12*(3), pp. 167–179.

Nithya, J., Vignesh, S. R., Devadarsan, A., & Venkatesh, S. (2022). AI based contactless attendance monitoring and management system. *International Journal of Health Sciences*, *6*(3), pp. 10600–10614.

Orabi, M., Al Aghbari, Z., & Kamel, I. (2023). FogLBS: Utilizing fog computing for providing mobile Location-Based Services to mobile customers. *Pervasive and Mobile Computing*, *94*, pp. 101832.

Qi, S., Zuo, X., Feng, W., & Naveen, I. G. (2022). Face Recognition Model Based on MTCNN and Facenet. *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications, ICMNWC 2022*. https://doi.org/10.1109/ICMNWC56175.2022.10031806

Rusia, M. K., & Singh, D. K. (2023). A comprehensive survey on techniques to handle face identity threats: challenges and opportunities. *Multimedia Tools and Applications*, *82*(2), pp. 1669–1748.

Sahin, V. H., Oztel, I., & Yolcu Oztel, G. (2022). Human Monkeypox Classification from Skin Lesion Images with Deep Pre-trained Network using Mobile

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584

Application. *Journal of Medical Systems*, *46*(11), pp. 46–79.

Setiawan, E. B., & Setiyadi, A. (2021). Mapping application for Greater Bandung Area using Web Technology. *Journal of Engineering Research (Kuwait)*, *9*, pp. 1–15.

Sharma, H., Sewani, H., Garg, R., & Kashef, R. (2021). Face Mask Detection: A Real-Time Android Application Based on Deep Learning Modeling. *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2021*, pp. 106–112.

Shivanna, P., & Venkatesiah, S. S. (2024). Biometric Identification for a Secured Environment Using AI-Based Facial Recognition. *International Journal of Safety and Security Engineering*, *14*(1), pp. 185–190.

Susanto, F., Fauziah, F., & Andrianingsih, A. (2021). Lecturer Attendance System using Face Recognition Application an Android-Based. *Journal of Computer Networks, Architecture and High Performance Computing*, *3*(2), pp. 167–173.

Tanış, M., & Erhan Yalçın, M. (2024). A statistical method of GPS spoofing detection using power spectral density for hardware. *International Journal of Circuit Theory and Applications*, *52*(5), pp. 2560–2573.

Tenhunen, S., Männistö, T., Luukkainen, M., & Ihantola, P. (2023). A systematic literature review of capstone courses in software engineering. In *Information and Software Technology* Vol. 159, p. 107191.

Wang, B., Li, H., Ren, X., & Guo, Y. (2023). An Efficient Differential Privacy-Based Method for Location Privacy Protection in Location-Based Services. *Sensors*, *23*(11), pp. 1–18.

Widjaja, A. E., Harjono, N. J., Hery, Mitra, A. R., & Haryani, C. A. (2023). Automated Class Attendance Management System using Face Recognition: an Application of Viola-Jones Method. *Journal of Applied Data Sciences*, *4*(4), pp. 431–440.

William, I., Ignatius Moses Setiadi, D. R., Rachmawanto, E. H., Santoso, H. A., & Sari, C. A. (2019). Face Recognition using FaceNet (Survey, Performance Test, and Comparison). *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*.

Xiao, J., Jiang, G., & Liu, H. (2018). A Lightweight Face Recognition Model based on MobileFaceNet for Limited Computation Environment. *EAI Endorsed Transactions on Internet of Things*, *7*(27), pp.1–9.

DOI: https://doi.org/10.34010/injiiscom.v6i1.13976
p-ISSN 2810-0670 e-ISSN 2775-5584