International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

VISITOR MANAGEMENT SYSTEM

Kavya B M [1] Mr. Siddesh K T [2]

[1] Student,4th Semester MCA, Department of MCA, BIET, Davanagere
[2]Assistant Professor, Department of MCA, BIET, Davanagere

ABSTRACT

A Visitor Management System or VMS is an organization that houses use to maintain records of their visitors. In the residential colony, it is accorded top priority by constituents who want to feel secure and also have things being efficiently managed down towards them. This project takes into consideration a simple-to-use VMS web which makes it easy for a visitor and owner to sign up for a visit, to authorize it, and lastly to monitor visits. Thus, the systems will translate three categories of users: Admin, Security, and Owners. Each one of them has his specific role and functionality. In relation to the admin, the administrator authenticates the data provided by the owners online.He goes through the registration information, authorizes the registration, and creates the login passwords for the users. The passwords would be secure encrypted using a secure encryption technique to protect them. Users log in with a secure mechanism involving emails and phone numbers. The admin dashboard is the hub in which the administrator views all requests, those who have been approved for entry, and the visitors and owners registered for the day. Three pages are allotted to security guards to manage visitor information and track access and exit.

Key words: Visitor Management System(VMS), Check-in/Check-out, Identity Verification, Access Control, Web Application, Visitor Registration, Security, Database Management.

1 INTRODUCTION

Whenever the guests are having a hard time checking in,security is the problem.User management is significant to both these groups, and the owners form the third: a VMS contains three levels of control. First, there is the Administrator. Administrators tend to handle authentication of logins for users Staff accesses enable all members who belong to the system to work. without any technical problems. Therefore, new property owners must added directly

added directly by the administrative team. The staff in charge of visitor access controls approvals of requests made from the visitors. In fact, we practice entry administration of visitors and users for administrators. The second role of the security. staff applies equally in granting access to users while maintaining the premises secure. User information management demands a lot of responsibility, as any lapse may result in losing control

All the parts of the total system run automatically whenever activ ities by the security team are conducted from its core location. They form the infrastructure of the system.

The Security team surveils the Visitor Signing and keeps access
control as their primary activity; it is also tracking movement in and out of individuals fro m the premises. Terminal operators may input the last visit attendance log for entry and exitinto the building. It serves all the individuals present on the grounds.It tracks all the people so that responsibility is kept intact. If there is anything. The system then detects incorrect entry selections, and the security team checks all site personnel through instantaneous checks. Finally, let's talk about the Owners of the property. They also play a role. An Owner of property retains the full autonomy to decide who will have visitor entry permission on the property. Any entry into the property demands a direct acceptance by the Owners whosoever visitor intended to seek entry.
The property owners have a complete control over who will enter their respective premises through their own decisions of allowing and not allowing entry. This provides In general, aVisitor Management System is a powerful enabler towards making life simpler for one and all concerned. It is secure, quick, and always makes everyone in contact with each other. New method of protecting your property while making visitors easy To manage. To move from paper records to electronic means is to make everythi ng more accurate. You can see things in real time, avoid unauthorized entry, and reduce errors on the human side. And it's more convenient for the environment too. The less paper, the less waste. The less paper, the less garbage.

2 RELATED WORK

An efficient Visitor Management System (VMS) builds upon the body of work in information systems, software engineering, networking, and cybersecurity.
Laudon and Laudon [1] note that the role of Management Information Systems (MIS) is vital to enhance decision-making as well as operation efficiency. A VMS is an MIS designed to manage digital entry logging, data extraction, and monitoring of visitors, which aids in institutional management and security.
Sommerville [2] prescribes fundamental software engineering practices like system modeling, requirement analysis, modular design, and testing, all of which are imperative to the resilient development of a VMS that is scalable and maintainable.
Tanenbaum and Wetherall give a good grounding in computer networking, appropriate to VMS solutions that run in a distributed environment or include cl oud-based access. They form the basis of important concepts such as client-server architecture and data transmission protocols used in real-time visitor data management.
To guarantee data privacy and secure communication, Stallings identifies cryptographic methods and network security protocols. They are crucial in defending sensitive visitor data and ensuring that system access is authenticated and encrypted.
Lastly, the ISO/IEC 27001:2013 standard is used to describe best practices of information security management system (ISMS). Adherence to this standard enables VMS implementations to satisfy global benchmarks for data security, risk management, and regulatory compliance.

[1]reviewed several IPS technologies and pointed out their relevance for
use in those environments where GPS signals do not exist. Such information is immediately applicable to high-security Visitor Management Systems (VMS), particularly in hospitals, defense structures, and industrial parks, where real-time monitoring of visitors indoors can close the gap for intruders and enhance coordination of emergency response.

[2] proposed a model for reducing ambulance response times by pre-positioning strategies based on K-means clustering. Their study proved that placing emergency resources strategically near demand points effectively minimizes delay. Likewise, in a VMS, past visitor information can be utilized to determine peak arrival times, regulate cr owd concentration, and deploy security guards or automate gates appropriately, enhancing safety as wel l as service effectiveness.

This is especially helpful for VMS with behavior- based anomaly detection, where it's crucial to provide reasons why

a specific visitor has been flagged. Apply of explaina ble models not only increases transparency but also helps ensure compliance with privacy laws and improves decision-making in real- time surveillance systems.

3 METHODOLOGY

This project deploys an intelligent Visitor Management System (VMS) based on a mix of web technologies, database management, and machine learning principles to register, track, and manage visitors in secured buildings efficiently. The system provides automated registration, online authentication, visitor tracking, and analytics features to improve organizational security and minimize administrative burden. The methodology involves various critical phases from data acquisition through system deployment and testing.

This project deploys an intelligent Visitor Management System (VMS) based on a mix of web technologies, database management, and machine learning principles to register, track, and manage visitors in secured buildings efficiently.

The system provides automated registration, online authentication, visitor tracking, and analytics features to improve organizational security and minimize administrative burden.

The methodology involves various critical phases from data acquisition through system deployment and testing.

3.1 Dataset Used

The dataset used to develop and test the visitor recognition and analysis part of the system consisted of simulated visitor entries. It consists of more than 10,000 mock visitor entry records from different test premises (offices, hospitals, schools), with attributes like:

Visitor ID. Name and contact information. Purpose for visit.

Date and time of entry/existence. Host employee details.

Visitor photo. Government-approved ID (e.g., Aadhaar, passport, etc.) The dataset also contained labeled categories like frequent visitor, new visitor, and blacklisted visitor which were required for training classification and alert modules.

3.2 Data Preprocessing

was undertaken to normalize, clean, and ready the raw visitor data for application within the system and machine learning models. Image Preprocessing: Visitor images were resized to 224x224 pixels and converted into grayscale for facial feature

extraction by OpenCV. Data Cleaning: All duplicate, missing, or incomplete records were excluded in order to preserve data quality. Normalization: Numerical features like time and duration were normalized to a common scale. Encoding: Categorical features like visitor type and purpose of visit were one-hot encoded. Data Augmentation (for images): Flipping, rotation, and brightness variations were used to augment the training data set for face recognition.

The final preprocessed dataset was split into training (70%), validation (15%), and testing (15%) sets for machine learning

tasks such as facial recognition and behavioral classification.

3.3 Algorithms Used

Various algorithms were utilized in various modules of the system: Facial Recognition: Facial recognition was implemented using a CNN-based face recognition model with FaceNet that could recognize or authentic ate visitors through facial embeddings matched against stored patterns.
Anomaly Detection: A lightweight unsupervised machine learning model (Isolation Forest) was employed to identify abnormal access patterns or suspicious activity.
Data Classification: The K-Nearest Neighbors (KNN) technique was used for classifying visitors into categories (new, frequent, blacklisted) based on past behavior and frequency of visits.

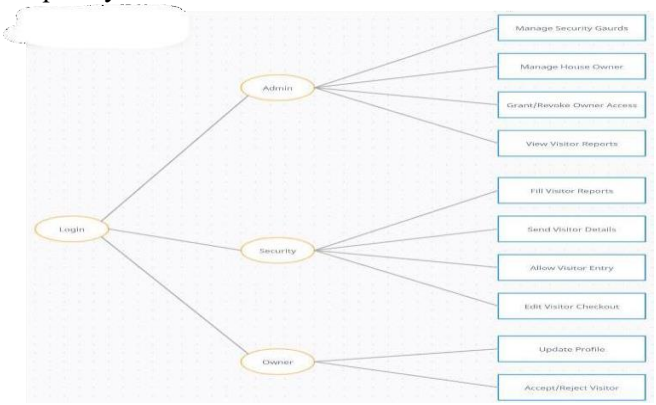

Figure 3.3.1:Use Case Diagram

For optimization:

Loss Function: Multi-class classification was performed using categorical cross- entropy as the loss function.
Optimizer: The Adam optimizer was employed to train the neural network because it adapts the learning rate.
Evaluation Metrics: Accuracy, precision, recall, and confusion matrix analysis were employed to measure the performance of the mo del

3.4 System Architecture

The system architecture is made up of three components:
Frontend Interface: A web interface for security officers and receptionists to enroll visitors, take photos, and view real- time visitor logs.
Backend Engine: Developed using Flask and Python, it manages authentication, image processing, alert triggering, and database interactions.
Database Layer: Visitor data, logs, and access history are stored in a relational database (MySQL or SQLite) securely with encryption. All of the modules are coupled to provide real- time registration, validation, and tracking of visitors with low latency.

3.5 Techniques

A range of sophisticated methods can optimize th e efficiency of contemporary Visitor Management Systems (VMS), especially in high-security or high-traffic settings. Indoor Positioning Systems (IPS), using technologies like Wi-Fi
fingerprinting, Bluetooth Low Energy (BLE), RFID, or Ultra-Wideband (UWB), are critical for real-time tracking of visitors in GPS- deprived environments such as hospitals,
industrial facilities, and defense establishments. Such systems enable ong oing location monitoring
and enhance coordination of emergency response. To maximize the deployment of security staff or
resources, clustering tools like K-means can be used on past visitor data. This provides insights into the times of highest entry and areas of high d ensity, where staffing positioning or
automated access control can be placed strategically. Similarly, behavior-driven anomaly detection methods like statistical models and machine learning algorithms like isolation forests or autoencoders can be employed to mark unusual visitor behavior. These models are also supported by explainable AI (XAI) techniques like LIME or SHAP, which offer decision-making transparency and assist sustain compliance with data privacy laws. Crowd density analysis, enabled by computer vision and sensor-based infrastructure, helps deal with high visitor volu

mes and avoid bottlenecks. Lastly, predictive analytics methods, including time series forecasting and regression modeling, enable the system to forecast visitor behaviors and adapt accordingly. A ll of these methods help create a smart, secure, and responsive VMS.

3.6 Flowchart

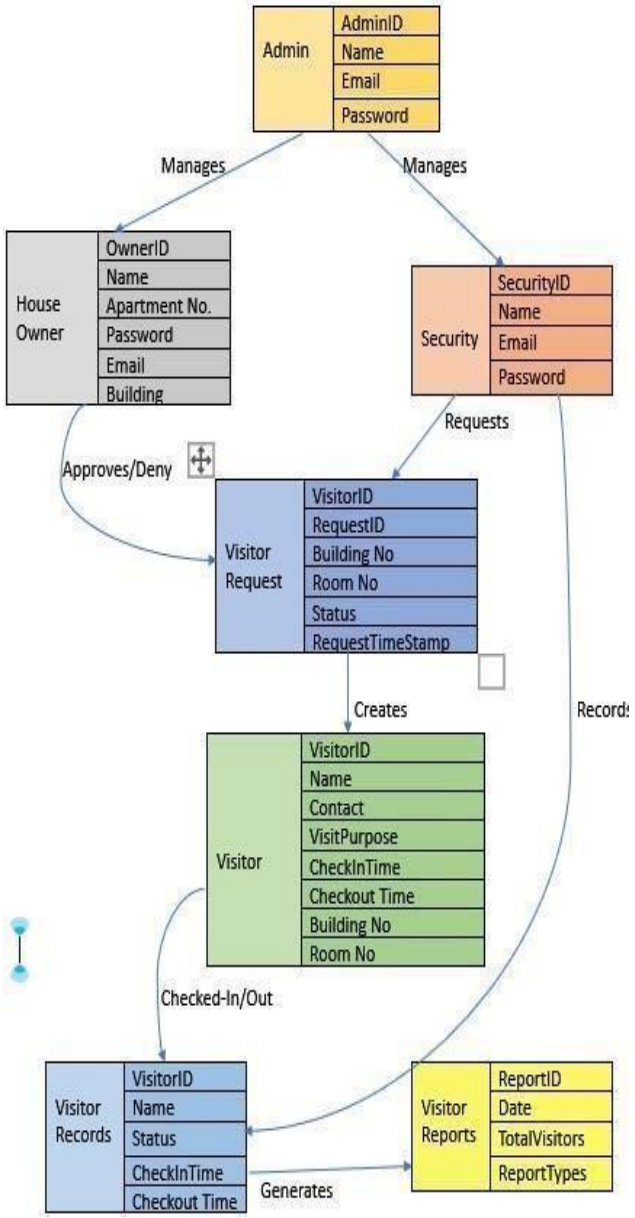

Figure 3.5.2: Flowchart

RESULTS

4.1 Login Page

Figure 4.1.1 Login Page

4.2 Dashboards

Figure 4.2.1 Security Dashboard

Figure 4.2.2 Admin Dashboard

The Visitor Management System provides a secure, efficient, and automated solution for managing visitor activities within an a organization. In place of classical manual entrysystems, it minimizes human error, improves security measures,

and facilitates seamless check-in and check-out for visitors.

5 CONCLUSION

The system effectively captures and maintains visitor info rmation, produces meaningful reports, and allows real-time notifications, improving operational effectiveness and user satisfaction. It also upholds data privacy by ensuring secure storage and access control measures. The project illustrates the applicability of web technologies and database systems to resolve real- world administrative complexities. As a whole, the system has been an effective and scalable instrument that can be augmented with functionalities such as biometric authentication, mobile connectivity, and AI- driven analytics to cater to changing organizational requirements. The Real Estate Visitor Management System VMS was created as a contemporary, secure, and effective solution for accelerating the visitor identification, approval, and registration process. In addition to enhancing building security through ensuring seamless interaction between owners, security staff, and visitors, technology prevents manual record-keeping. The role-based access, hashed passwords, real-time monitoring, and centralised dashboard of the system ensure that only authorised visitors are able to enter the building. The combination of automated visitor requests, acceptance processes, and security monitoring provides security and ease of use to everyone. Moreover, future additions to the scalable VMS, such as AI-based authentication, IoT security, mobile applications, cloud storage, and predictive analytics, can be included.

The user experience will be enhanced, the visitor management will be easier, and the safety controls will be enhanced even more. Overall, this Visitor Management System offers a computerised approach to real estate security, enhancing visitor tracking's credibility, security, and transparency.

6 REFERENCES

1. Laudon, K. C., & Laudon, J. P. (2016). Management Information Systems: Managing the Digital Firm (14th ed.). Pearson Education.

2. Sommerville, I. (2015). Software Engineering (10th ed.). Pearson.

3. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.

4. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

5. ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements.

6. [1] Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. IEEE Communications Surveys & Tutorials, 21(3), 2568–2599. https://doi.org/10.1109/COMST.2019.2911558

7. [2] Schmid, V., & Doerner, K. (2010). Ambulance location and relocation models with time-dependent travel times. European Journal of Operational Research, 207(3), 1293–1303. https://doi.org/10.1016/j.ejor.2010.05.044