IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

Enhancing Organizational Security and Efficiency: A Case Study of IndoAI's Visito - Visitor Management Systems App

Vivek Gujar[1]

Director, IndoAI Technologies P Ltd, Pune, India[1]

Abstract: A digital Visitor Management System(VMS) goes beyond convenience, becoming a strategic necessity for organizations aiming to bolster security, efficiency, and compliance in the digital era. In the age of digital transformation, a robust VMS is crucial for fortifying organizational resilience and ensuring a secure, streamlined environment for stakeholders. IndoAI's Visito, a Visitor Management App, combines Facial Recognition and Aadhar verification for secure entry. With OTP verification, accurate cross-referencing, and a Pass printout, it ensures enhanced security, efficiency, and compliance. The Analytics Dashboard provides administrators with key insights for informed decision-making and optimization. Further, integrating QR code-based VMS with AI Camera and Zero Trust into Aadhar verification ensures continuous scrutiny, minimizing unauthorized access risks and enhancing user experience

Keywords: Access Control, Identity Management, Visitor Management, IndoAI, Facial Recognition Technology, Aadhar

I. INTRODUCTION

Access Control, Identity Management, and Visitor Management collectively constitute a robust framework for safeguarding organizations. Access Control is the first line of defense, regulating entry to physical spaces and digital networks, ensuring only authorized individuals have access. Identity Management complements this by centralizing user identities, facilitating efficient and secure user access across various systems and platforms. Visitor Management extends this security to guests, tracking their presence and activities within the premises, enhancing overall safety and providing data-driven insights. The significance of this integrated approach lies in its ability to fortify organizational security comprehensively. It minimizes risks associated with unauthorized access, streamlines user management processes, and provides real-time visibility into visitor activities. Beyond security, these systems optimize resource allocation, improve operational efficiency, and contribute to a safer and more controlled organizational environment. This proactive security approach aligns with modern organizational needs, where data protection and safety are paramount concerns.

1.1 Synergy: Access Control, VMS and Identity Management

In the intricate web of modern security infrastructure, the seamless integration of Access Control, Visitor Management Systems (VMS), and Identity Management (IDM) is essential for robust and comprehensive security measures.

1.1.1 Access Control

At the core of security, Access Control regulates entry to physical and digital spaces. It encompasses the policies and technologies that dictate who is granted access and to what extent. This includes physical access points, such as doors and gates, as well as digital assets and information. Access Control ensures that only authorized individuals can enter designated areas or use specific resources, safeguarding against unauthorized entry and potential security breaches.

1.1.2 Visitor Management Systems (VMS)

VMS complements Access Control by managing the entry of visitors into a facility. Utilizing technologies like biometrics and digital registration, VMS enhances the accuracy and efficiency of the visitor check-in process. It provides real-time visibility into visitor activity, allowing organizations to monitor who is present on the premises and for what purpose. Integrated with Access Control, VMS ensures that visitors adhere to predefined access policies and do not pose a security risk.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

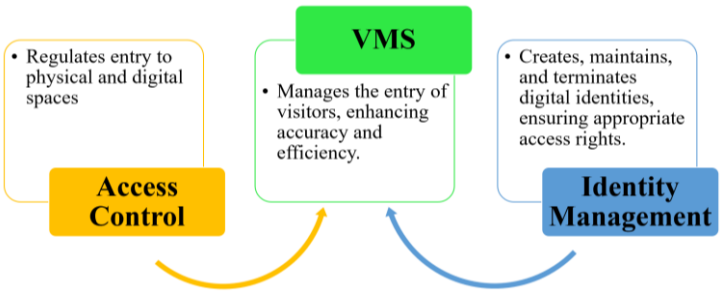
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

1.1.3 Identity Management (IDM)

IDM forms the backbone that ties Access Control and VMS together. It involves the creation, maintenance, and termination of digital identities for individuals within a system. IDM ensures that each user has the appropriate access rights based on their role and responsibilities. This includes verifying the identity of individuals, managing credentials, and enforcing security policies. IDM not only secures digital access but also integrates with Access Control and VMS to extend security measures to physical spaces(see flow diagram below).

Flow Diagram:



This interconnected approach creates a comprehensive security framework where Access Control, VMS, and IDM work in tandem to fortify both digital and physical security, offering a layered defense against potential threats.

Through biometric authentication, like facial recognition, VMS enhances identity security, aligning with IDM principles. It provides real-time visibility into visitor activity, aiding security and contributing to IDM analytics. VMS enforces access control policies, integrating seamlessly with IDM frameworks, ensuring adherence to rules. In essence, VMS is integral to IDM, offering a holistic approach to identity verification, enhancing security, and providing valuable insights. The integrated approach of Access Control, Visitor Management Systems (VMS), and Identity Management provides a comprehensive security framework tailored to the unique challenges of critical infrastructure and VIP settings which is discussed in the form of case study. It not only prevents unauthorized access and potential security breaches but also establishes a sophisticated system for managing the entry of visitors, which is particularly critical in locations where the stakes are high. Ultimately, the synergy of Access Control, VMS, and IDM forms an indispensable security shield, safeguarding assets, data, and individuals in environments where security is paramount.

II. VISITOR MANAGEMENT SYSTEM(VMS):

In today's landscape, the importance of security and operational efficiency dictates a departure from traditional manual visitor management practices. Outdated methods, such as paper sign-in logbooks and prolonged reception desk lines, no longer meet the standards of customer satisfaction, security & operational efficiency. The transformative solution lies in the evolution of Visitor Management Systems (VMS), representing a critical paradigm shift in how organizations manage and monitor individuals accessing their facilities. Essentially, a VMS serves as a comprehensive solution designed to streamline and enhance the visitor check-in process while fortifying security measures. In an era driven by technological advancements and an increased emphasis on efficiency, security, and compliance, a robust VMS is not just beneficial but imperative.

The term "visitor management system" refers to a system that keeps track of visitors' actions in an organization or public institution. It can quickly offer users with the required output and information, as well as track arriving and outgoing visitors. However, VMS is also capable of streamlining the registration process and providing visitors with accurate and integrated data [8]. A VMS [10] is a digital solution that automates the process of registering, tracking, and managing visitors in an organization. It allows organizations to streamline their entry process and improve security by verifying the identity of visitors and checking for any potential risks before granting access. As per Proxyclick [11] VMS represents all the processes and activities an organization puts in place to manage the flow of visitors, from start to finish, as a part of the bigger picture—the visitor experience. Vpod's [12] VMS is a smart solution that allows organisations to streamline and automate their visitor management process, using technology to monitor, track, and record visitor information.

A Visitor Management System (VMS) transforms guest check-ins with digital solutions like ID scanning and touchscreen registration, ensuring speed, security, and efficiency. This modern approach not only expedites the check-in process but also integrates seamlessly with broader security systems. Traditional manual methods pose security risks and errors, driving the shift to digital VMS. The urgency for digital VMS is heightened by the need for technological alignment,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

especially in the COVID-19 era, emphasizing contactless interactions and integration with broader organizational systems for heightened security and compliance.

Thus, the Visitor Management System, particularly in its digital form, transcends convenience and emerges as a strategic imperative for organizations aspiring to enhance security, efficiency, and compliance in an increasingly digitized world. As businesses embrace the advantages of digital transformation, a robust digital VMS becomes a cornerstone in fortifying organizational resilience, providing a secure and streamlined environment for all stakeholders.

2.1 Objective of VMS

Research objective of Dina et al [8] are the essential objectives of any VMS, which are :

- Track visitors' arrival, presence, and departure, taking swift action.
- Enhance workplace health and safety for employees.
- Facilitate diverse visitor entries with elevated hospitality.
- Personalize visitor treatment based on access levels.
- Improve guidance for secure visitor navigation.
- Promote touchless access solutions.
- Minimize contact between people and surfaces.
- Prepare for unforeseen future circumstances.

While above are the basic objective of any VMS, the analytics are the primary requirement of management to get overall output of software which is mentioned in detail in case study section later.

III. LITERATURE REVIEW

The IA VMS of Niharika et al [1] is a web app designed for efficient visitor management in facilities. It features admin and user logins, enabling room creation, booking, and interaction among users. The main feature is creating rooms with specified details, allowing users to browse, book, and engage in community discussions. Admin manages all rooms, approves/rejects bookings, and views a comprehensive list of all bookings. This user-friendly system enhances visitor and room management, fostering user interaction about their bookings.

The paper of Santosha et al [2] introduces an IoT system for smart office visitor management using Raspberry Pi with a camera and an Android mobile phone. Visitors schedule appointments through a client application, receiving a QR code. The consulting person, equipped with a professional application, accesses real-time appointment information by scanning the visitor's QR code with the Raspberry

The special features of the system of Haiya Hamood et al [3] allow users to generate report of visitors, view notification list, generate instant messaging to the visitors, allocate parking and easy payment methods. In future this system will help the management to provide easy accommodation.

The VMS of Indah et al [4] efficiently tracks and provides essential information for both the organization and visitors. Specifically designed for the School of Computing (SOC) at Universiti Utara Malaysia, the SOC Visitor Management System (SOCVMS) replaces the manual visitor process, eliminating data loss and paper wastage. The six-phase development involves requirements, design, development, testing, delivery, and feedback. SOCVMS benefits top management, staff administration, and visitors by enabling easy online applications and providing data analysis and report generation capabilities. The system, evaluated by 13 respondents, received positive feedback for its overall design features.

Chandani et al [5] Smart Visitor Management Systems (SVMS) present innovative solutions for resource optimization and eco-friendly practices in high-rise buildings. This study, through data analysis and expert perspectives, explores the implementation and benefits of SVMS in the context of sustainability. The research highlights positive impacts, including enhanced energy efficiency, reduced carbon emissions, improved waste management, and streamlined visitor experiences. SVMS integration not only aids in achieving sustainability certifications but also aligns with Sri Lanka's environmental goals. The article [5] acknowledges potential challenges such as data security, initial costs, and stakeholder collaboration, providing valuable guidance for stakeholders in sustainable practices for high-rise buildings. Al-Ghaithi and Eaganathan (2016) propose implementing Visitor Management Systems (VMS) by installing tailored, password-protected software on existing computers. This web-based system allows authorized users to pre-register visitors, including additional details like photos and visit information. Kazlauskas (2015) emphasizes the role of VMS in

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

enhancing security and facility management in high-rise buildings. While barriers exist, the integration of Smart VMS (SVMS) is crucial for sustainable economic growth and improved quality of life in urban contexts (Marjaba & Chidiac, 2016).

The proposed solution of Harish et al [6] employs automated facial recognition, addressing security concerns related to the increasing number of visitors. This system benefits apartment residents by allowing them to identify visitors using a dedicated application, enhancing security measures to prevent unauthorized entry.

Rikshit et al [7] introduced a VMS incorporating face recognition for office premises. The biometric security system efficiently identifies individuals within the office, distinguishing between regular personnel and visitors. The system also facilitates the scheduling of appointments for recognized visitors. For unknown face recognition, a token-based authentication method via email is employed.

The VMS of Dina et al [8] is crucial for monitoring visitor numbers, visit objectives, and enforcing security measures, including blocking rule violators. Its overarching goal is to harmonize organizational operations and global visitor interactions. Their synthesis draws from diverse papers, examining similar subjects, to shape the system's foundation. Evaluations of the current system's limitations prompt the need for a new one. Part three delves into project planning, encompassing feasibility studies, Gantt charts, and software methodologies. Functional and non-functional requirements are detailed, along with implementation steps in section four. The conclusion in section five offers clear recommendations and outlines future work for the visitor management system, anticipating refinement after implementation across the organization and affiliated entities.

VMS of Anwar et al [9] was designed and developed in order to monitor visitor movement in an organization. The application can be viewed from local LAN (Intranet) with a standard web browser such as Microsoft Internet Explorer with no additional software or plug-in to load. VMS will be placed at the main guardhouse and will be handled by the corporate security section. Each of the department will be located with at least one front desk officer to monitor the current visitor to visit the department.

IV. CASE STUDY

Advancing Security in Government Offices: The Role of Visito - A VMS by IndoAi

In the landscape of government offices, where security and access control are paramount, the integration of Visitor Management Systems (VMS) becomes a critical imperative. The VMS deployed by IndoAi, aptly named "Visito," stands as a noteworthy of cutting-edge technology, leveraging Facial Recognition Technology and Aadhar verification to fortify security measures within esteemed government entities such as the Chief Minister's Office (CMO) and Minister's Office. Developed for critical infrastructure, including the Chief Minister's Office and Minister's Office, this app leverages advanced technologies to streamline the visitor registration process while upholding stringent security measures.

A) Facial Recognition Technology: A Paradigm Shift in Identity Verification

Facial Recognition Technology represents a significant departure from traditional methods of identity verification. In the context of government offices, where the stakes are high and the need for precision paramount, this technology assumes an indispensable role. Visito's utilization of Facial Recognition Technology of Dutypar's App ensures a swift and accurate means of identifying visitors, mitigating the risks associated with manual identification methods. This advanced technology analyzes facial features with unparalleled precision, adding a sophisticated layer of security that is crucial in government settings.

The significance of Facial Recognition Technology in Visito lies in its ability to provide real-time identification, contributing to the prevention of unauthorized access. The system captures facial data, matches it against Aadhar name, mobile number and photo, and grants access only to those individuals whose identities align with the established criteria. This not only enhances security protocols but also streamlines the visitor check-in process, promoting operational efficiency within government offices.

B) Aadhar Verification: Strengthening Identity Assurance

The integration of Aadhar verification within Visito underscores a commitment to robust identity assurance. Aadhar, a unique identification number linked to biometric and demographic information, serves as a cornerstone in the verification

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

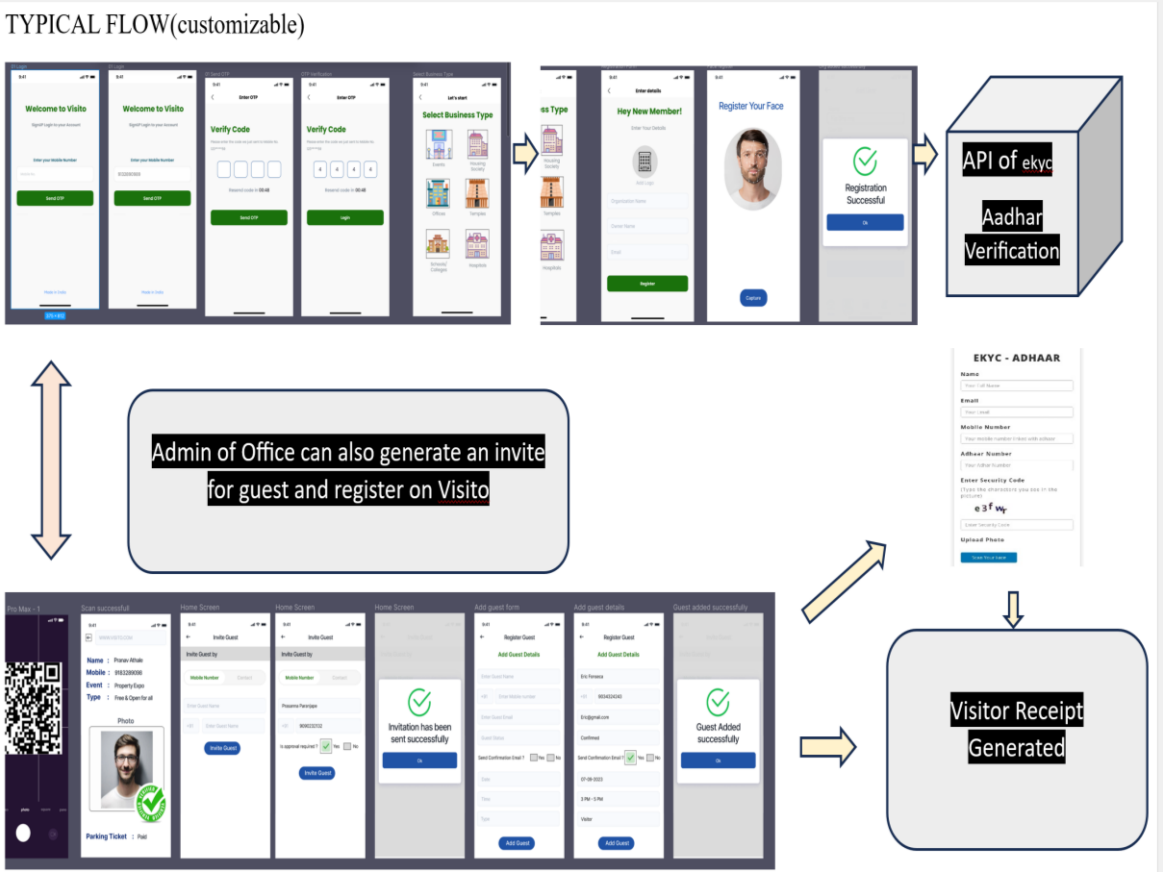
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

process. By validating visitors through Aadhar, Visito ensures that individuals entering government offices are not only visually identified but also cross-verified against a government-issued and widely recognized identification database.

The use of Aadhar verification in Visito is particularly relevant in government settings where adherence to regulatory compliance and the authenticity of visitor credentials are non-negotiable. The integration of Aadhar adds an additional layer of scrutiny, assuring government authorities that visitors are who they claim to be and have undergone thorough verification through a trusted and authoritative system.

C) Overview of the Visitor Management App, Visito



Step 1: User Input
The process begins with the visitor providing essential details – name, contact number, department to be visited, VIP's name, VIP secretary's name, Aadhar number, and a selfie. The app incorporates Dutypar's a) Facial Recognition Technology to capture a precise facial image, enhancing the identification process. b) Verification of Aadhar details by accessing Setu server by Dutypar's ekyc[13] API.

Step 2: OTP Verification
Simultaneously, an OTP is generated and sent to the visitor's provided mobile number. To ensure the integrity of the visitor's details, the OTP must be shared with the personnel responsible for inputting the information. The app awaits verification, ensuring a secure and validated entry process.

Step 3: Information Validation
Upon entering the OTP, the app verifies the visitor's identity, cross-referencing the provided details with the database. This two-step authentication ensures that only legitimate visitors proceed, enhancing security measures.

Step 4: Pass Printout
With successful verification, the visitor is eligible for a Pass printout. This pass includes all relevant information,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

including the visitor's name, department, VIP details, and a prominently displayed facial image captured during registration. This pass serves as the visitor's key to accessing the secured premises.
Step 5: Security Check
Armed with the printed pass, the visitor approaches the entry point, where security personnel can quickly verify the pass's authenticity by matching the facial image on the pass with the visitor. This visual confirmation enhances security and expedites the entry process.

D) Flow of the Visito App:

1. Registration:
The visitor initiates the process by providing personal details, department, and the VIP to be visited. The integration of Dutypar's Facial Recognition Technology ensures accurate and efficient capture of the visitor's facial features & verification of Aadhar by Dutypar's ekyc API.

2. OTP Generation:
Simultaneously, an OTP is generated and sent to the visitor's mobile number. This serves as an additional layer of security, preventing unauthorized access.

3. OTP Verification:
To proceed, the visitor shares the OTP with the person entering the details. The app verifies the OTP, ensuring that the information input aligns with the visitor's identity.

4. Database Cross-Verification:
The app cross-references the provided details with the database, ensuring accuracy and legitimacy. This step reinforces the security of the entry process.

5. Pass Printout:
Upon successful verification, the visitor receives a Pass printout containing crucial information and a prominently displayed facial image. This pass serves as the entry ticket.

6. Security Check:
Approaching the entry point, the visitor presents the printed pass. Security personnel verify the pass by matching the facial image with the visitor, ensuring a visual confirmation of identity.

E) Benefits of the Visito App:

Enhanced Security: The integration of Facial Recognition Technology and OTP verification ensures a multi-layered security approach, mitigating the risk of unauthorized access.
Efficiency and Speed: The streamlined process minimizes delays, allowing legitimate visitors swift access to the premises.
Accurate Records: The app maintains a comprehensive database of visitor details, aiding in record-keeping and future reference.
Visual Confirmation: The inclusion of a facial image on the pass facilitates quick visual confirmation, reducing the likelihood of human error during security checks.
User-Friendly: The app's intuitive interface ensures a smooth and user-friendly experience for both visitors and personnel inputting the details.
Compliance: The app aligns with data protection regulations and compliance standards, ensuring the secure handling of sensitive visitor information.
Thus Visito App represents a significant leap forward in ensuring the security and efficiency of high-profile government offices. By leveraging advanced technologies and implementing a meticulous registration and verification process, the app stands as a beacon of innovation in the domain of visitor management for critical infrastructure.

F) VMS Analytics

The Visitor Management App Analytics and Dashboard provide a comprehensive overview of the system's performance, security efficacy, and user interactions. By leveraging these key metrics and visualizations, administrators can make informed decisions, optimize processes, and ensure the continued effectiveness of the app in safeguarding critical infrastructure and high-profile government offices.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

Metric	Key Metric	Dashboard Visualization
Total Visitors	Number of visitors processed	Line chart depicting daily, weekly, and monthly trends in visitor numbers. Total visitor count displayed prominently for quick reference.
OTP Verification Success Rate:	Percentage of successful OTP verifications.	Pie chart illustrating the OTP verification success rate. Comparative analysis over different time periods.
Facial Recognition Accuracy	Percentage accuracy of facial recognition technology	Bar chart showcasing the accuracy rate of facial recognition. Trends and variations in facial recognition performance.
Pass Issuance Rate	Percentage of visitors issued a pass after successful verification.	Gauge chart displaying the pass issuance rate. Color-coded indicators for quick identification of pass issuance status.
Security Check Efficiency	Average time taken for security personnel to verify a visitor	Histogram displaying the distribution of time taken for security checks. Metrics on the efficiency of security checks during different time slots.
Visitor Categories	Categorization of visitors based on departments and VIP visits	Stacked bar chart showcasing the distribution of visitors across different categories. Dynamic filters for exploring specific visitor categories.
System Utilization	Percentage of time the system is actively processing visitor data.	Heatmap representing the system's active hours and periods of peak utilization. Historical analysis of system utilization trends.
Error and Exception Rates	Percentage of errors or exceptions encountered during the visitor registration process	Radar chart highlighting the types and frequency of errors. Drill-down capability for a detailed analysis of specific error types.
Pass Utilization Trends	Frequency of pass usage by visitors for access	Trendline depicting the usage patterns of issued passes over time. Visitor feedback integration for pass effectiveness analysis
System Health and Performance	Overall health and performance of the Visitor Management System	Health score gauge reflecting the system's operational status. Real-time monitoring of system performance metrics.

G) Unlocking the Potential of QR Codes in Visitor Experience

In addition to things found in the literature,[5] most experts emphasise that VMS can assist in waste reduction efforts by promoting digital communication and documentation. Instead of printing visitor badges or passes, the system can generate digital credentials or QR codes that visitors can store on their mobile devices. This reduces the production of physical waste associated with traditional badge printing

QR code technology extends beyond enhancing workforce visibility and security, offering valuable advantages for visitors. Integrating QR codes into a visitor management system brings several benefits:

Increased Automation: A QR-integrated platform facilitates pre-appointment communication, including parking directions, and enables touchless sign-in upon arrival. Visitors gain access to advance information, enhancing their experience by providing details on locating destinations or discovering additional on-site resources.

Simplified Processes: Automation improves customer satisfaction by streamlining workflows. Staff intervention remains available when needed, or visitors can navigate uninterrupted through automated checkpoints, following custom paths tailored to their specific needs.

Enhanced Security: QR codes streamline the completion of non-disclosure agreements (NDAs) or waivers before appointments, saving time and increasing productivity. ID verification portals using QR codes ensure quick and reliable validation of government-issued IDs.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

Touchless Authentication: QR codes facilitate health-related screenings for visitors and employees, contributing to on-premises safety. Implementing a touchless Visitor Management System (VMS) fosters a sense of security among staff and visitors.

Real-time Watchlists and Alerts: A QR-enabled VMS enables screening visitors against watchlists, triggering alerts to security personnel in case of a potential threat. This system ensures timely notifications of visitor or appointment arrivals to the relevant staff.

H. Strengthening Security: Integrating Zero Trust Technology into Visito

Zero Trust is a cybersecurity concept based on the principle of "never trust, always verify." In a traditional security model, once inside the network, users are often given broad access. Zero Trust, on the other hand, assumes that threats may come from both outside and inside the network. It requires verification from anyone trying to access resources, even if they are inside the network. No one is given automatic trust.

How Zero Trust works:

Verification of Every User: In a Zero Trust model, every user, whether inside or outside the network, is treated as untrusted. Verification is required before granting access.
Continuous Monitoring: Access permissions are not static; they are dynamically adjusted based on the user's behavior, device health, location, and other contextual factors. Continuous monitoring ensures that access is appropriate at all times.
Micro-Segmentation: Networks are segmented into small, isolated zones, and access is restricted based on the principle of least privilege. Users only have access to the specific resources they need for their job.
Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of identification, such as a password and a temporary code sent to their mobile device.

Integrating Zero Trust into the Aadhar verification in a Visito: Process

Visitor Input: The visitor provides details including name, contact number, department to be visited, VIP's name, VIP secretary's name, Aadhar number, and a selfie.
Zero Trust Verification: Each piece of information provided by the visitor is treated as untrusted. The system requires continuous verification through multiple factors, such as Aadhar biometrics, facial recognition, and mobile OTP.
Continuous Monitoring: Throughout the visitor's interaction with the system, their behavior is continuously monitored. Any deviation from normal patterns triggers additional verification steps.
Micro-Segmentation: Access to different areas within the facility is segmented based on the visitor's purpose. For example, a visitor going to the Minister's office will have restricted access compared to someone going to a general department.
Multi-Factor Authentication (MFA): The visitor might need to authenticate multiple times during their visit, ensuring a high level of security.

V. CONCLUSION

The integration of Facial Recognition Technology and Aadhar verification within Visito reflects a comprehensive approach to security in government offices. The advanced capabilities of Facial Recognition Technology elevate the precision of identity verification, while Aadhar verification adds a layer of authenticity and compliance adherence. Together, these technologies not only fortify security measures but also contribute to the seamless functioning of government offices, building trust and the commitment of IndoAi to advancing technological solutions tailored for the unique demands of government entities. Visito, in this context, emerges as a beacon of innovation, aligning seamlessly with the imperative of securing sensitive government spaces in an era where precision and efficiency are paramount. Further this system can use QR code-based VMS integrated with AI Camera which will enhance user experience. By integrating Zero Trust into Aadhar verification in Visito, the VMS ensures that every step of the visitor's interaction is subject to continuous scrutiny and verification, minimizing the risk of unauthorized access and enhancing overall security.

REFERENCES

[1] M. Niharika, Rachankonda Saisr, Jilla Vaishnavi, Volam Meenakshi, Voruganti Navaneetha, Divya Gudibandla, “Company Visitor Management System”, International Journal for Research in Applied Science & Engineering Technology Volume 11, Issue VI, June 2023

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 10, Issue 11, November 2023

DOI: 10.17148/IARJSET.2023.101114

[2] Santhosha Rao, Casbona Jonathan, "QR code based Visitor Management System for Smart Offices", International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue-4, November 2019

[3] HaiyaHamood Al Ghaithi, Umapathy Eaganathan, "A Brief Study And Implementation Of Visitor Management System For Asia Pacific University, Malaysia", International Journal of Advance Research in Science & Engineering (IJARSE), Vol 5, Issue 4, Apr 2016

[4] Indah Saqinah Naharanuar, Cik Fazilah Hibadullah, Ali Yusny Daud, "Design and Development of Web-Based System: Visitor Management System", International Journal of Research in Engineering and Science (IJRES), Volume 11, Issue 4 , April 2023 , PP. 337-346

[5] Chandani, G.G.N. , Asmone, A.S., "Utilising smart visitor management system to enhance sustainable practices in high-rise buildings in Sri Lanka" In: Sandanayake, Y.G., Waidyasekara, K.G.A.S., Ramachandra, T. and Ranadewa, K.A.T.O. (eds). Proceedings of the 11th World Construction Symposium, 21-22 July 2023, Sri Lanka. pp. 1116-1128. DOI: https://doi.org/10.31705/WCS.2023.89.

[6] Harish B.G, Bhavana R B, "Visitor's Management System for Apartments", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Volume 11, Issue 6, June 2022, DOI:10.15662/IJAREEIE.2022.1106011

[7] Rikshit Makwana, Romil Nandwana, Jayshil Jain, Tejas Laxmeshwar, Shirish Sabnis, "VISITX: Face Recognition Visitor Management System", International Research Journal of Engineering and Technology (IRJET), Volume 06, Issue: 03, Mar 2019

[8] Dina Alkhodary, Ibrahim A. Abu-AlSondos1, Basel J. A. Ali , Maha Shehade, Hanadi A. Salhab, "Visitor Management System Design and Implementation during the Covid-19 Pandemic", Inf. Sci. Lett. 11, No. 4, 1059-106 2022, http://dx.doi.org/10.18576/isl/110406

[9] Anwar N, M. N. Masrek , Y. R. Rambli, "Visitor Management system by applying the model of UTAUT", 2012 IEEE Symposium on Business, Engineering and Industrial Applications, Bandung, Indonesia, 2012, pp. 223-228, doi: 10.1109/ISBEIA.2012.6422874.

[10] https://timesofindia.indiatimes.com/blogs/voices/how-a-visitor-management-system-can-help-in-transforming-the-workplace-experience-of-employees-guests/

[11] https://www.proxyclick.com/visitor-management-system

[12] https://medium.com/vpodsolutions/tagged/visitor-management-system

[13] Vivek Gujar, "Integrating Facial Recognition Technology in IndoAI App with eKYC Case Study & Future of AI Cameras in Banking", International Journal of Science and Research (IJSR), Volume 12 Issue 11, November 2023, pp 711-718, DOI: https://dx.doi.org/10.21275/SR231108193207

BIOGRAPHY

Vivek Gujar, PhD, MBA BTech, an ex IT security auditor, presently Director, IndoAI has interests in Facial Recognition Tech, AI, AI Camera, Blockchain, Process Improvement, Innovation: writing on these through blogs, research articles and case studies.