International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Automated Access Communication System

Ms Deepa Merlin S[1], Mrs M. Angelin Rosy[2], Dr.M. Felix Xavier Muthu[3]

[1]II MCA, Master of Computer Applications Er. Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India.
[2]Assistant Professor, Master of Computer Applications Er. Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India
[3]Associate Professor, Mechanical Engineering, St Xavier's Catholic College of Engineering, Nagercoil, Tamilnadu, India

Abstract
Efficient communication and secure document management are essential for modern organizations. Traditional methods of sharing documents using paper or external storage devices are inefficient and insecure. This project, titled "Automated Access Communication System," presents a web-based solution to enable secure communication and centralized document sharing within organizations. The system provides authenticated access for employees and administrators and stores all documents and user information in a centralized database. It supports multiple departmental modules, such as Administrator, Marketing and Sales, Finance and Accounts, Technical, and HR, to manage department-specific activities. Overall, the system improves data security and communication efficiency and reduces manual effort in organizational process

Keywords: Document Management System, Organizational Communication, Secure Document Sharing, Secure Data Storage

1. INTRODUCTION

1.1 Automation Systems' History

Automation is essential for increasing productivity and security in the digital world. Conventional access systems mainly rely on manual procedures, which are vulnerable to security threats and human error. Automated access systems offer a clever solution by combining control and communication technologies.

1.2 Limitations of Manual Access System

Keys and registers are examples of manual access control mechanisms that are ineffective and unsafe. These can result in data loss, unapproved access, and inadequate monitoring. Additionally, these systems cannot offer centralized control and real-time updates.

1.3 Purpose and Scope of the Study

The goal of this system is to create a communication-based automated access control system that guarantees safe monitoring and authentication. For improved access control, the system can be used in smart settings, offices, and institutions.

1.4 Objective of Project

The goal of this project is to provide a straightforward, user-friendly, yet robust online application for securely sharing, managing, and controlling enterprise documents on the Intranet or Internet within a specific firm. This makes it possible for all the company's departments to communicate online.

2. RESEARCH PROBLEMS

User-support system communication remains primarily manual, ineffective, and time-consuming in many businesses, institutions, and service contexts. Conventional customer service techniques, such as phone calls, emails, or simple IVR systems, frequently result in high operating expenses, variable service quality, delays, and a lack of real-time responses. Additionally, these systems find it difficult to manage several user requests simultaneously and offer tailored interactions.

An intelligent, automated communication system that can deliver accurate, scalable, and real-time responses without continuous human interaction is required to overcome these challenges. The suggested Automated Access Communication System uses Python as the backend and full-stack web development tools to produce an intelligent, interactive platform. To facilitate smooth user-system communication, this system incorporates contemporary technologies such as database administration and online APIs.

The primary issue addressed in this project is the absence of an effective, automated, and intelligent communication system that can manage user inquiries, reduce human labor, speed up response times, and improve user experience. The system's goal is to offer a centralized platform where users can communicate via voice or text, obtain prompt responses, and quickly access the necessary services.

3. LITERATURE REVIEW

3.1 Existing Access Control System

Smart card technologies, radio-frequency identification (RFID)-based systems, and biometric systems are examples of current systems. Although these technologies offer better security, small-scale applications may find them expensive and complicated.

3.2 Manual Vs Automated System

Manual methods rely on human verification, which causes mistakes and delays. Automated systems greatly increase efficiency by offering quicker access, more accuracy, and real-time communication.

3.3 Technologies Used

Python and database management systems are the main software technologies used in the development of the Automated Access Communication System. Python is the primary programming language because of its ease of use, adaptability, and robust automation and communication frameworks. It facilitates quick creation and integration with hardware components like biometric modules and sensors.

MySQL (or SQLite) is the database system used for managing and storing data. System configurations, access logs, and user credentials are safely stored in the database. Python uses connectors like sqlite3 or mysql-connector to communicate with the database, allowing for quick changes and data retrieval.

Additionally, the system may create web-based interfaces for monitoring and user interaction using Python frameworks like Flask or Django. Python-supported network protocols are used to manage communication between system components, enabling real-time data transmission.

4. METHODOLOGY

4.1 System Development Approach

A methodical and modular approach was used to develop the Automated Access Communication System. The system has a client-server architecture in which all processing is performed on the server side using Python, and users interact with the application via a web interface. The goal of the development was to establish an effective, safe, and user-friendly system for document management and communication within the company.

The system was designed with the following layers:

- **Presentation Layer** (User Interface using JavaScript)
- **Application Layer** (Business logic using Python)
- **Database Layer** (Data storage using MySQL)

This layered architecture ensures better performance, maintainability, and scalability of the system.

4.2 Tools and Technologies

The following tools and technologies were used to develop the system:

- **Front-End:** JavaScript
- **Back-End:** Python
- **Database:** MySQL
- **Operating System:** Windows 10

These technologies help build dynamic, secure, and responsive web applications.

4.3 Data Collection and Testing

Sample organizational data, including personnel information, departmental records, and document files were used to test the system. The functionality of modules such as file upload, communication, report generation, and login was checked using various test scenarios.

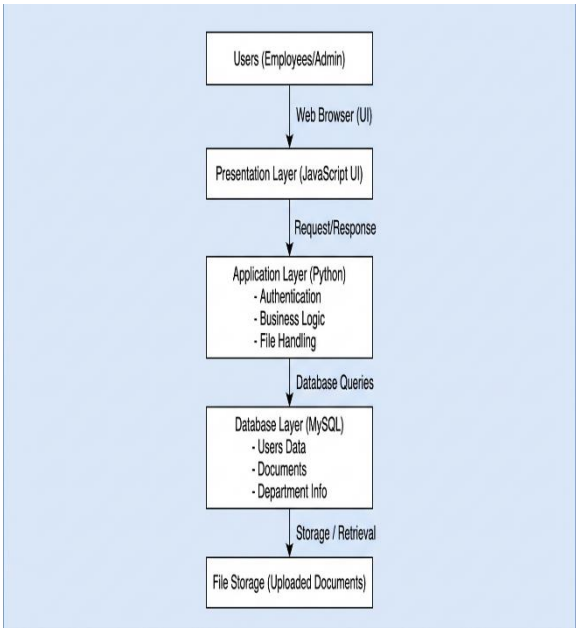
- Unit Testing: Examining separate modules
- Integration testing: Examining how different modules interact
- User Acceptance Testing: Verifying the system satisfies user needs

The outcomes demonstrate the effective operation of the system with precise data processing and safe communication.

5. SYSTEM DESIGN AND ARCHITECTURE

5.1 System Overview

A web-based program, the Automated Access Communication System, was created to control document sharing and communication within the company. The client-server architecture of the system allows users to access the program via a web browser while Python is used on the server for all processing. Through authentication, the system gives staff members from many departments safe access. A centralized database enables users to upload, download, and manage documents. Real-time data access and updates facilitate effective departmental communication



5.2 Modules and Functionalities

The system is separated into multiple modules, each of which is in charge of managing particular organizational functions. Together, these modules guarantee effective data management, safe access, and seamless communication.

Administrator

1. Administrator controls the entire application of this system
2. He enables the user id and password for all the employees with respective departments
3. Admin controls all the activities of the employees
4. Admin could able to produce the reports as per the requirements of the management

Marketing & Sales Department

1. Every employee of the marketing and sales department will be login into this system with user id and password
2. Every employee can able to update their client and customer details, Quotation and invoice preparation, customer tracking about their payment details etc
3. Also the employees can able to apply for their leaves, View salary details etc through this application

Finance & Accounts Department

1. Every employee of the Finance and Accounts department will be login into this system with user id and password
2. Every employee can perform all activities related to their department, such as maintaining cash and bank balances, tax payments, salary payments, and other office expenses. All statutory payments to employees, such as ESI, PT, and PF, are routed through this application.
3. Also the employees can able to apply for their leaves, View salary details etc through this application

Technical Department

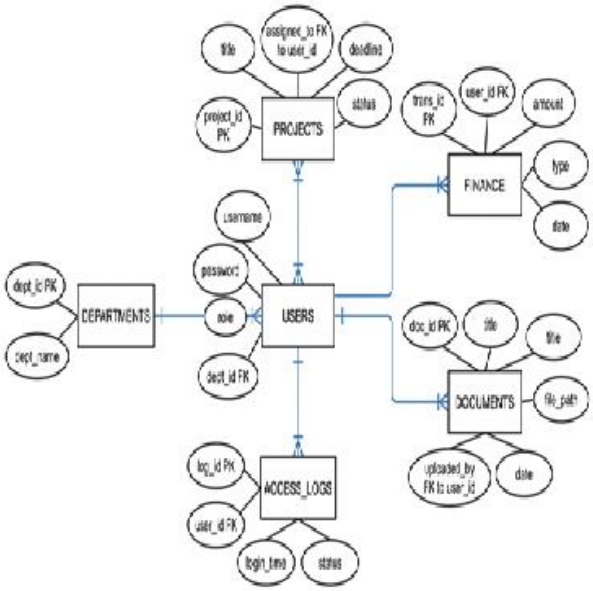
1. Every employee of the Technical (Development Team) department will be login into this system with user id and password

2. After payment confirmation from customers and clients, the respective project work will be allocated to the technical team along with a deadline through this system. Accordingly, the respective teams move towards project completion. After completion of the project the information will be updated so all the other departments and their managers can view the complete data through this system
3. Also the employees can able to apply for their leaves, View salary details etc through this application

HR Department

1. Every employee of the HR Department will be login into this system with user id and password
2. All HR department activities, such as Recruitment, Employee Training, Employee welfare, and reliving formalities, will be taken care of through this system.
3. Also the employees can able to apply for their leaves, View salary details etc through this application

5.3 ER DIAGRAM



5.3.1 RELATIONSHIP

1. USERS ↔ DEPARTMENTS
   - One DEPARTMENTS can have many USERS.
   - One USERS belongs to one DEPARTMENTS.
   - Cardinality: 1:N
   - Implementation: USERS dept_id is a foreign key to DEPARTMENTS. dept _id.
2. DOCUMENTS ↔ USERS
   - One USERS can upload many DOCUMENTS.
   - One DOCUMENTS is uploaded by one USERS.

- Cardinality: 1:N
- Implementation: DOCUMENTS.uploaded_by is a foreign key to USERS.user_id.

3. ACCESS_LOGS ↔ USERS
   - One USERS can have many ACCESS_LOGS (login/audit records).
   - One ACCESS_LOGS entry belongs to one USERS.
   - Cardinality: 1:N
   - Implementation: ACCESS_LOGS.user_id is a foreign key to USERS.user_id.

4. PROJECTS ↔ USERS
   - One USERS can be assigned to many PROJECTS.
   - One PROJECTS is assigned to one USERS.
   - Cardinality: 1:N
   - Implementation: PROJECTS.assigned_to is a foreign key to USERS. user _id.
5. FINANCE ↔ USERS
   - One USERS can have many FINANCE transactions.
   - One FINANCE transaction is associated with one USERS.
   - Cardinality: 1:N
   - FINANCE.user_id is a foreign key to USERS.user_id.

5.4 DATABASE DESIGN

5.4.1 CORE TABLES

- users(user_id, username, password, role, department)
- employees(emp_id, name, department, salary)
- documents(doc_id, title, file_path, uploaded_by, date)
- departments(dept_id, dept_name)
- transactions(trans_id, type, details, date)

6. IMPLEMENTATION

6.1 System Workflow

The system workflow describes the sequence of operations performed when a user interacts with the Automated Access Communication System. This ensures smooth communication and secure data handling.

- User Authentication:The user logs into the system using a valid username and password. The system verifies the credentials using a database.
- Access Request Processing:After successful login, the user sends requests, such as viewing data, uploading documents, or accessing modules, based on their role.
- Communication with the Database:The application communicates with the MySQL database to retrieve or store data, such as user details, documents, and transaction records.
- Access Decision and Logging:Based on user roles and permissions, access is granted or denied. All user activities are recorded in the system logs for monitoring and auditing.

6.2 User Roles

The system defines different user roles to ensure proper access and security.

- Administrator: The administrator has full control over the system. They manage users, assign roles, monitor activities, and generate the reports.
- User (Employee): Users have limited access based on their departments. They can perform operations such as uploading and downloading documents and updating relevant data.
- Viewer: Viewers have read-only access. They can only view reports and data but cannot make any changes to the system.

6.3 Security Features

The system incorporates various security measures to protect the data and ensure safe communication.

- Password Encryption:User passwords are stored in an encrypted form to prevent unauthorized access.
- Secure Communication Protocols:Data transmission between the client and server is secured to avoid data breaches.
- Role-Based Access Control (RBAC):Access to system modules is restricted based on user roles to ensure data confidentiality.
- Activity Logging:All user actions, such as logins, data access, and modifications, are recorded for auditing and tracking purposes.

7. RESULTS AND EVALUATION

7.1 Performance Metrics

The performance of the Automated Access Communication System was evaluated by comparing it with that a of traditional manual system. The results show significant improvements in efficiency, accuracy, and security.

Metric	Manual System	Automated System	Improvement
Access Time	Slow	Instant	Faster

Error Rate	High	Low	Reduced
Security Level	Low	High	Improved

The automated system reduces the processing time and minimizes human error. It also enhances data security by implementing authentication and access control mechanisms.

7.2 User Feedback

The system was tested by users from different departments, and the feedback collected highlighted its effectiveness and usability.

- The system is easy to use with a simple and user-friendly interface
- It provides high security through authentication and access control
- It significantly improves efficiency in communication and document handling
- Reduces manual workload and saves time
- Ensures accurate and reliable data management

8. CONCLUSION AND FUTURE ENHANCEMENTS

The Automated Access Communication system provides a secure, reliable, and efficient solution for managing communication and document sharing within an organization. This reduces manual effort, minimizes errors, and improves overall system performance. The use of a centralized database management and role-based access control ensures data security and easy accessibility. The system enhances communication between departments and increases their productivity.

FUTURE ENHANCEMENTS

The system can be further improved by incorporating advanced technologies such as:

- Integration with mobile applications for easy access anytime and anywhere
- Cloud-based access control for scalability and remote data management
- AI-based security analysis for detecting unauthorized activities
- Face recognition technology for enhanced authentication and security

REFERENCES

1. Web-based Access Control System Journals, Google Scholar. Available: https://scholar.google.com/scholar?q=web+based+access+control+system
2. MySQL Documentation, Oracle. Available: https://dev.mysql.com/doc/
3. Automation and Security Research Papers, Google Scholar. Available: https://scholar.google.com/scholar?q=automation+and+security+systems
4. MDN Web Docs, Mozilla Foundation. Available: https://developer.mozilla.org