IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART ID CARD SYSTEM (LOCATION-BASED ACCESS CONTROL)

[1]Dr. N.V. RAMANA REDDY, [2]CHALLAGULLA JAYA SRI,
[1]Associate Professor, [2]UG STUDENT
[1,2]DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS
[1,2] AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY
Gunthapally(V), Abdullapurmet(M), R.R Dist

Abstract: Project: Smart ID Card System (Location Based Access Control). The project aims to develop a secure and efficient access control system based on smart ID cards and location verification. The system will be able to improve the security of the organization by allowing only the users who are in the authorised geographical areas. It combines employee identity management, real-time location tracking and access validation to prevent unauthorised entry and improve monitoring capabilities.

The proposed system consists of modules such as Employee Management, Location Management, Access Verification and Access Logging. Administrators can track employee records and designate authorised locations with latitude, longitude, and access radius parameters. The system checks the user's current location against the predefined zones and allow or deny access when attempting to access. Each access attempt is logged with timestamp and location information for audit and security purposes.

Application is developed using Java technologies with connectivity to database using JDBC, ODBC concept. The system is designed to be secure, portable, scalable and easy to use. Testing methods such as unit testing, integration testing, functional testing and system testing were performed for reliability and performance assurance. The project shows how smart ID systems combined with location-based services can enhance security in the workplace, automate monitoring processes and reduce risks of unauthorised access.

Keywords— Smart ID Card System, Location-Based Access Control, Access Verification, Employee Management, Real-Time Security Monitoring.

I. INTRODUCTION

In the current digital age, security and access management have become necessary requirements for organisations, institutions and workplaces. Traditional identification and access control systems are mostly based on manual verification methods, passwords or common ID cards, which are prone to misuse, duplication, unauthorised access and human error. With more organisations moving to smart technology and remote work environments, there is an increasing need for a more intelligent, automated and secure access control mechanism. To address these challenges, the Smart ID Card System (Location-Based Access Control) has been developed as an advanced security solution that combines smart identification technology with real-time location verification.

The Smart ID Card System is designed to provide secure authentication and controlled access not only based on the user's identity but also on the user's geographical location. The system will only allow users to access when they are physically present in authorised zones defined by the organization. This helps to greatly improve security by preventing unauthorised access attempts from outside of approved locations. The system integrates location-based services with smart card technology, providing an additional authentication layer to increase reliability, transparency and operational efficiency.

In the proposed system, the employee or user smart ID cards will be associated with the location tracking mechanisms to validate access requests in real time. Administrators can define allowed access zones by setting parameters like latitude, longitude and access radius. When a user attempts to access the system or a protected resource, the application verifies the user's current geographical coordinates against the previously defined authorised locations. If the user is within the allowed range, the request is granted access; if not, the request is denied. The system records all access attempts, whether successful or not, for monitoring and auditing purposes.

One of the biggest advantages of this system is that it can automate the entire access control process, while reducing manual intervention. Traditional systems often require security personnel to verify identities or keep attendance and access records manually, which can be time consuming and prone to errors. But the Smart ID Card System provides instant authentication and verification, which leads to faster operations and better security management. Furthermore, automatic logging of access activities enables organisations to maintain precise records, identify questionable conduct, and produce audit reports when required.

The project is conducted with Java technologies, due to the portability, reliability, object-oriented structure and platform independence. It has good support for networking , database connectivity , security mechanisms , graphical user interfaces , etc . It can be used to build scalable enterprise level applications . Further the system employs database technologies such as JDBC and ODBC for efficient data storage, retrieval and management. These technologies allow the application and the database to communicate smoothly and ensure data consistency and security.

The Smart ID Card System is composed of several functional modules that together ensure efficient operation. The Employee Management Module allows administrators to add, update, and manage employee details such as ID and user roles. The Location Management Module gives administrators the ability to configure authorised locations with geographic coordinates and access boundaries. The Access Verification Module verifies the user's location in real-time before granting access. All access attempts are recorded in the Access Log Module with timestamps, user information and location information for future reference and auditing.

Security is a very important feature in the design of the proposed system. Accessing confidential resources and restricted areas without authorisation can lead to data breaches, financial losses and operational risks. Thus, the integration of smart ID authentication with location verification improves security measures and decreases the chances of misuse. The system also enables monitoring and accountability by keeping a full record of user activities. This feature is particularly useful for organisations that have to comply with security policies and regulations.

Another key feature of the system is its ability to adapt to modern workplaces, including remote and hybrid working models. Traditional office-based access systems are no longer sufficient as many organisations now allow employees to work from various locations. The location-based access mechanism ensures that users can securely access organisational resources only from authorised locations, offering flexibility without sacrificing security.

Extensive testing procedures are also used to ensure software quality and reliability. Different testing methods like unit testing, integration testing, functional testing, system testing, white-box testing and black-box testing were done to verify that the application performs accurately and efficiently in different conditions. These testing processes help to identify and eliminate errors, improve system stability, and ensure the final application meets user requirements and expectations.

In conclusion, the Smart ID Card System (Location-Based Access Control) is a novel and effective answer to the challenges of modern security and access management. The system utilises smart identification techniques along with real-time location verification to enhance organisational security, automate monitoring processes and minimise risks of unauthorised access. The project demonstrates how emerging technologies can be integrated to build secure, scalable, and intelligent access control systems suitable for educational institutions, corporate offices, government organisations, and other security-sensitive.

II. RELATED WORK

The domain of access control and smart identification systems have seen a lot of progress with the arrival of digital technologies, wireless communication and location based services. Several researchers and organisations have proposed systems that combine identification technologies with security mechanisms to enhance authentication, monitoring and access management. These previous developments in smart authentication and secure access systems motivate the present work and have laid the foundation of the proposed Smart ID Card System (Location-Based Access Control).

The conventional access control systems mainly relied on manual verification techniques like paper identity cards, passwords, PIN, and attendance registers. But these systems were extensively used, but they had a number of drawbacks like duplication of identities, unauthorised access, human errors and poor record keeping. Manual systems required a high level of supervision by security personnel. Therefore, they were less reliable and also time-consuming in big organisations and institutions.

To overcome these, researchers have proposed RFID based identification system for automated authentication and attendance monitoring. Users might use RFID (Radio Frequency Identification) technology to scan smart cards containing electronic chips to gain access to secure areas. They were faster and more automated but still had poor security because the only check on who could get in was whether they had a card. Stolen or copied cards could still be used by unauthorised people.

Later, identity verification was further enhanced with the introduction of biometric authentication systems including fingerprint recognition, facial recognition and iris scanning. These systems used unique biological features of users to offer more accuracy and security. To check fraud and impersonation, several organisations have setup biometric based attendance and access systems. However, biometric systems often required expensive hardware, high computational resources and frequent maintenance. In addition, their performance and user acceptance were sometimes influenced by privacy issues and environmental conditions.

Due to the rapid development of mobile computing and GPS technologies, researchers have begun to investigate location-based access control systems. These systems introduced the concept of permitting or denying access depending on the user's geographical location. Location-aware security mechanisms grew in importance for remote working environments, military applications and enterprise security systems. Organisations could use GPS-enabled devices to verify that users were accessing services at authorised locations, thus reducing the risk of unauthorised remote access.

A few studies have proposed geo-fencing techniques in secure access control. Geo-fencing is the creation of virtual boundaries around authorised locations using latitude, longitude and predefined values of the radius. The system performs certain functions such as authentication or alerts when a user enters or leaves a specified area. Geo-fencing has been widely applied in logistics, employee tracking and mobile security applications. But many earlier geo-fencing systems didn't have the ability to integrate with smart identity management and centralised monitoring capabilities.

Cloud-based access management systems were also introduced, providing scalable and centralised authentication solutions. These systems enabled administrators to manage users, permissions and security policies remotely via web applications. Cloud-based systems, while improving the flexibility and scalability, also brought along issues of data privacy, reliance on networks and cyber-attacks. Hence the researchers concentrated on blending multiple authentication mechanisms such as smart cards, biometrics and location verification for stronger security.

The Smart ID Card System proposed differs from the previous systems in that it combines smart ID authentication and real-time location-based verification on a single platform. The proposed system differs from traditional RFID or password-based systems by requiring both user identity and physical location validation for access. This two-layer authentication process greatly increases security, and reduces unauthorised access attempts.

Moreover, the proposed system can automatically log and monitor access, so organisations can keep an accurate record of all access attempts. Previous systems were often only concerned with authentication and not with detailed auditing capabilities The proposed system's access log module stores time stamps, user information and geographical data that can be used for security analysis and administrative reporting.

The system is based on Java technologies, JDBC and database integration and conforms to modern software engineering practices. Java based systems are portable, scalable and platform independent and hence are ideal for enterprise applications. The modular architecture facilitates better maintainability and scope for future enhancements like biometric integration, mobile applications, cloud synchronisation and AI based threat detection.

In general, the development of intelligent security solutions has been assisted by past studies and current technologies in RFID systems, biometric authentication, GPS based security, geo-fencing and cloud access management. The proposed Smart ID Card System takes advantage of these technologies and integrates them into a secure, efficient and scalable location-based access control framework that overcomes the shortcomings of traditional systems and meets the modern organisational security requirements.

III.METHODOLOGY

The Smart ID Card System (Location-Based Access Control) methodology is designed to deliver secure, efficient and automated access management by integrating smart identification techniques with real-time location verification. It implements a systematic approach of data collection , user authentication , location authentication , access control and activity monitoring . The primary objective of the methodology is to enable authorised users to gain access to organisational resources only when they are physically present within designated geographical locations.

The system starts with the registration and maintenance of employee or user details through the Employee Management Module. In this phase, the admin enters and manages the user information such as employee ID, name, designation, role and smart ID credentials. Each user is assigned a unique identity and stored securely in the database. This centralised data management facilitates accurate authentication and makes it easy to maintain employee records.

After the user is registered, the Location Management Module is used to define the zones where access is authorised. The administrators will configure geographical parameters such as latitude, longitude and access radius for a particular office location or work area that is permitted. These coordinates form so-called geo-fenced zones, virtual boundaries through which the system verifies users' locations when they make access requests. Also, the possibility of defining multiple authorised locations makes the system suitable for organisations with several branches or remote working environments.

When the user tries to access the system, the Access Verification Module is activated. The module initially authenticates the user's smart ID credentials and then obtains the user's current geographical location by employing the location tracking technologies such as GPS or network-based positioning. The received coordinates are then compared with the authorised zones available in the database . If the user is within the radius of allowed access, access will be granted; if the user is outside the radius of allowed access, access will be denied. The two-tier verification process provides an additional security layer as it simultaneously verifies identity and physical presence.

The methodology includes also continuous monitoring and logging with the Access Log Module. All access attempts , successful or unsuccessful , are automatically stored with details such as user ID , time stamp , access status and geo-location . Those logs are stored in the database for future analysis, auditing and

security monitoring purposes. Administrators can review these logs to identify suspicious activities, track user activity, and create reports as necessary.

The implementation methodology is based on a modular software development approach using Java technologies due to their portability, platform independence and object-oriented architecture. The application is connected to the database using JDBC and related technologies so that they can communicate efficiently. The system architecture is designed to be scalable and maintainable and enable future enhancements such as biometric authentication, mobile integration and cloud-based monitoring.

The system is being put through a number of testing procedures to ensure reliability and accuracy. These include unit testing, integration testing, functional testing, system testing, white-box testing and black-box testing. These testing techniques are used to identify errors, validate functionality, and ensure that the application meets the security and performance requirements. This methodology makes the Smart ID Card System a secure, automated and efficient solution to contemporary access control and security management of an organization.

IV. SYSTEM ARCHITECTURE:

The System Architecture of the Smart ID Card System (Location-Based Access Control) is designed in a modular and layered fashion to ensure security, scalability, reliability and effective communication between system components. The architecture combines user authentication, location checking, database management and access monitoring into a single framework. This system works by verifying the identity and geographical location of users before giving them access to organisational resources or restricted areas.

The architecture is composed of four main layers: User Interface Layer, Application Processing Layer, Database Layer and Location Verification Layer. These layers together provide secure and seamless access control functionality.

The User Interface Layer is the front-end part of the system that allows administrators and users to interact with it. Administrators can add and manage employees details, set up authorised locations, review access logs and create reports using graphical interfaces. Users use their smart ID credentials to request access to the system. This layer is supposed to be user-friendly and responsive for ease of system operations.

The application processing layer is the central functional element of the system. It comprises of all the important modules like Employee Management Module, Location Management Module, Access Verification Module and Access Log Module. This layer is responsible for handling user requests, validating smart ID information, comparing locations and controlling access permission. The application logic is developed using java technologies which provide the platform independence, object orientated design and secure application development.

The Location Verification Layer is used to obtain and verify the geographical position of the user. This layer uses GPS or network based location services to obtain the current co-ordinates of the user in real-time. The obtained latitude and longitude values are compared with pre-defined authorised locations configured by administrator. if the user's location is within the radius of allowed access the system will continue with authentication else access is denied. This layer is the main security feature in the proposed system implementing geo-fencing and location aware authentication.

The Database Layer stores information about the organization and the system such as employee information, smart ID information, locations, permissions, and access history. The Java application connects to the database using JDBC. The database allows secure storage, efficient retrieval and proper handling of data. All access attempts are logged with timestamp, user ID, access status, location coordinates, etc., for monitoring and auditing purposes.

When a user makes an access request with a smart ID card or login credentials, the system workflow starts. The application first authenticates the user's identity and then obtains the current geographical location. The live coordinates are compared to the authorised location database by the location verification module.

If both identity verification and location validation are successful, the system allows access. Otherwise the request is denied and logged in the system database.

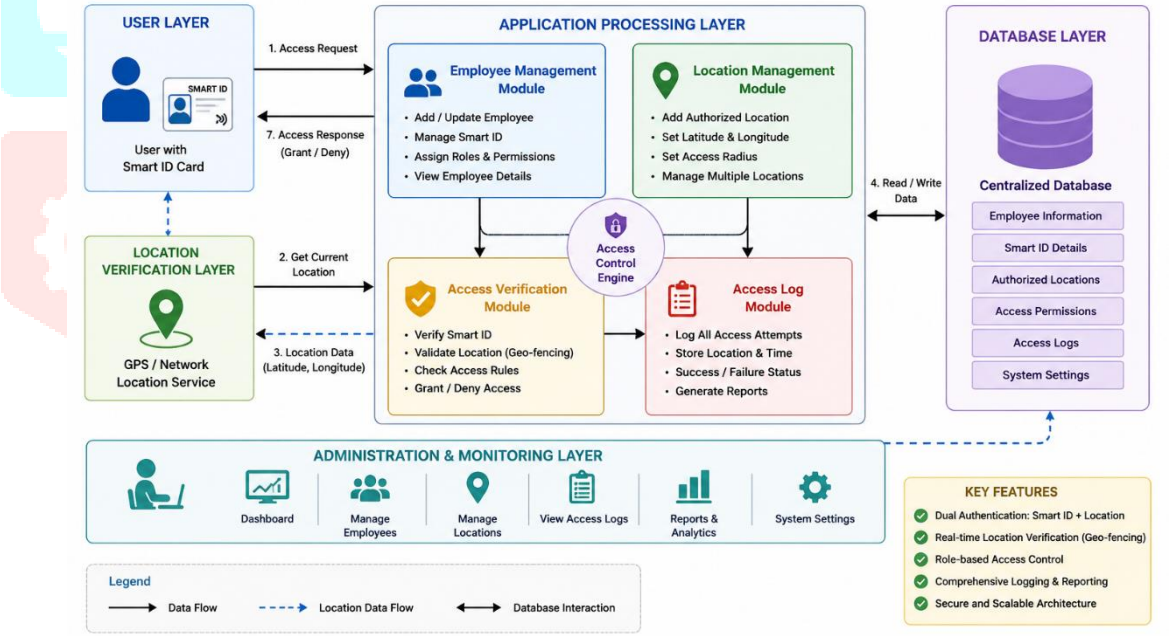
The architecture also enables centralised monitoring and management. The management interface allows an administrator to add or delete users, create new access zones, update security policies and check access history. In future upgrades, easy upgrades and integration of additional features like biometric authentication, mobile applications, cloud storage and AI based threat analysis are possible due to the modular architecture design.

The paper concludes that the system architecture of Smart ID Card System provides secure, reliable and efficient location-based access control via the integration of smart identification, real-time location verification, database integration and automated monitoring in a unified framework.

A. Overview:

The figure shows a Smart ID Card System for location based access control. It is a layered architecture where a user with a smart ID card sends an access request that is verified using identity and real time location data (GPS/network). The system comprises of access control engine, employee management module, location management (geo-fencing and access radius) and access verification and access logging modules. A central database stores employee details, permissions, authorised locations and logs. There's an admin/monitoring layer which provides dashboards, reporting and system management. This means that access decisions can be monitored and controlled in real time based on role and location rules.

B. Architecture Diagram:



V. EXPERIMENTAL SETUP:

The experimental setup of project "Smart ID Card System (Location Based Access Control)" has been designed to implement and evaluate a secure authentication system that allows or denies access to users as per their geographical location. The system was designed using Java technology, JDBC connectivity, Spring Boot framework and MS Access database for storing employee records, authorised locations and access logs. The development environment was set up using Java SE 17, Maven build tools and Eclipse IDE to ensure smooth development, deployment and testing of the application.

The system consists of four main functional modules that cooperate to provide secure location-based access control. The first module is the Employee Management Module. This module is used to maintain the employee's information such as employee id, profile details and role assignments. This module facilitates the administrator to add, update and delete employee records easily. The second module is the Location Management Module. It allows the administrator to define authorised locations by entering the latitude and longitude and the allowable radius of access. These coordinates are stored in the database and used for access validation. The Access Verification Module is the core component of the system and is the third module. It constantly checks the present location of the user against the defined allowed zones and grants or denies access to them in real time . The fourth module is the Access Log Module that logs every access attempt with details such as timestamp, employee ID, access status, and location information for future auditing and monitoring.

The system architecture is designed using java network concepts and database connectivity technologies. JDBC was the standard interface for connecting Java applications with relational databases, and ODBC support was provided for database interoperability. The data transfer between the server and client components was performed using TCP/IP communication protocols. The support of the Java Virtual Machine ensured that the application was portable across different operating systems. The project also relied on Maven configuration files and Java runtime environments to efficiently manage dependencies and execution processes.

Various testing methodologies were employed in the experimental validation to confirm the reliability and performance of the system. Unit testing was carried out to verify the individual software components and to ensure that each module produces the correct outputs for valid inputs. Integration testing was performed to ensure the integrated modules such as employee management, location verification and database connectivity worked seamlessly. Functional testing was carried out to verify that all business requirements and functionalities were correctly implemented including access granting, denial responses and log generation. The complete integrated system was then subjected to system testing to verify that it met user requirements and operated reliably in a wide variety of situations. Also, the application was tested using white box testing and black box testing techniques to test the internal logic and external functionality of the application.

The experimental setup also included validation of different operational scenarios such as verification of valid and invalid user inputs, checking duplicate entry prevention, testing page navigation, validating real time location tracking and ensuring accurate database updates. The functional test cases were done and the field testing was done manually to verify if the system responded appropriately with no delays and secure authentication procedures were maintained. The last test results indicate that all modules are functioning successfully without any major defects, and the system successfully achieved secure location-based access control with reliable performance and accurate access logging.

VI. RESULT AND DISCUSSION:

The results of the project "Smart ID Card System (Location-Based Access Control)" show that the developed system can provide secure and efficient access control based on the geographical location of users. The system could correctly verify the real-time location of the employees and allow them access or deny access depending on the predefined authorised zones saved in the database. All modules of the application including Employee Management, Location Management, Access Verification and Access Log Management were working correctly and interacting smoothly without major errors during execution.

Implementation and Testing The system showed a reliable performance in terms of managing employee data, validating location coordinates and ensuring secure authentication processes. The Access Verification Module successfully compared the current location of the user with the configured latitude and longitude values and successfully restricted unauthorised access attempts. The Access Log Module recorded every access attempt with details such as employee ID, timestamp, and location information, improving the system monitoring and auditing capabilities.

Different types of testing methods like unit testing, integration testing, functional testing, system testing, white box testing and black box testing were performed to evaluate the overall performance of the application. Test cases validated user inputs (both valid and invalid), prevention of duplicate entries, proper navigation of pages and proper interaction of modules of the system. Results showed that all the pages and links worked correctly, database operations were successful and no major defect was found during testing.

The system also showed good portability and stability due to the use of Java technology and JDBC connectivity. The application was capable to maintain an efficient communication between the software modules and the database ensuring secure data processing. The experimental evaluation proved the effectiveness of the proposed system to implement location-based authentication and can be used in organisations to improve security, monitor employees' access and prevent unauthorised entry to restricted areas. Overall the project was successfully implemented and delivered reliable, accurate and secure results.

VII. CONCLUSION:

The project “Smart ID Card System (Location-Based Access Control)” was designed and successfully implemented providing a secure and efficient access management system based on location-based authentication techniques. The system uses Java technology, database connectivity and real time location verification to effectively ensure that only authorised users can access restricted areas. The project implemented modules such as Employee Management, Location Management, Access Verification and Access Log Management to ensure accurate monitoring and secure control of user access activities.

The developed system increases security in the organization by minimising the probability of unauthorised access and recording all the access attempts in detail. Using latitude, longitude and access radius for location verification adds another layer of security over traditional ID card systems. The portability, reliability and efficient communication between the application and the database was achieved by using Java, JDBC, ODBC and networking technologies.

The application has been extensively tested using a range of testing techniques such as unit testing, integration testing, functional testing, system testing, white box testing and black box testing and found to perform accurately and consistently under different conditions. The system successfully validated user inputs, avoided double entries and kept up with navigation and security access logs without any major defects.

In summary, the project was successful in achieving its objectives through the development of a robust, scalable and user-friendly smart ID card system that can improve access security to organisations. The proposed system can be further enhanced in the future by incorporating advanced technologies such as biometric authentication, cloud-based monitoring, mobile applications, and AI-based security analysis to offer more intelligent and automated access control solutions.

VIII.REFERENCES:

- James Gosling, Bill Joy, Guy Steele, and Gilad Bracha, The Java Language Specification, Addison-Wesley, 2005.
- Herbert Schildt, Java: The Complete Reference, 11th Edition, McGraw-Hill Education, 2018.

- Kathy Sierra and Bert Bates, Head First Java, 2nd Edition, O'Reilly Media, 2005.
- Deitel & Deitel, Java How to Program, 10th Edition, Pearson Education, 2015.
- Sun Microsystems, Java Database Connectivity (JDBC) API Specification, Oracle Corporation.
- George Reese, Database Programming with JDBC and Java, 2nd Edition, O'Reilly Media, 2000.
- E. Balagurusamy, Programming with Java, 6th Edition, McGraw-Hill Education, 2019.
- William Stallings, Data and Computer Communications, 10th Edition, Pearson Education, 2013.
- Behrouz A. Forouzan, TCP/IP Protocol Suite, 4th Edition, McGraw-Hill Education, 2010.
- Ian Sommerville, Software Engineering, 10th Edition, Pearson Education, 2017.
- Roger S. Pressman, Software Engineering: A Practitioner's Approach, 8th Edition, McGraw-Hill Education, 2015.
- Bruce Eckel, Thinking in Java, 4th Edition, Prentice Hall, 2006.
- Oracle Corporation, Java Platform Standard Edition Documentation.
- Martin Fowler, Patterns of Enterprise Application Architecture, Addison-Wesley, 2002.
- Cay S. Horstmann, Core Java Volume I – Fundamentals, 11th Edition, Pearson Education, 2018.