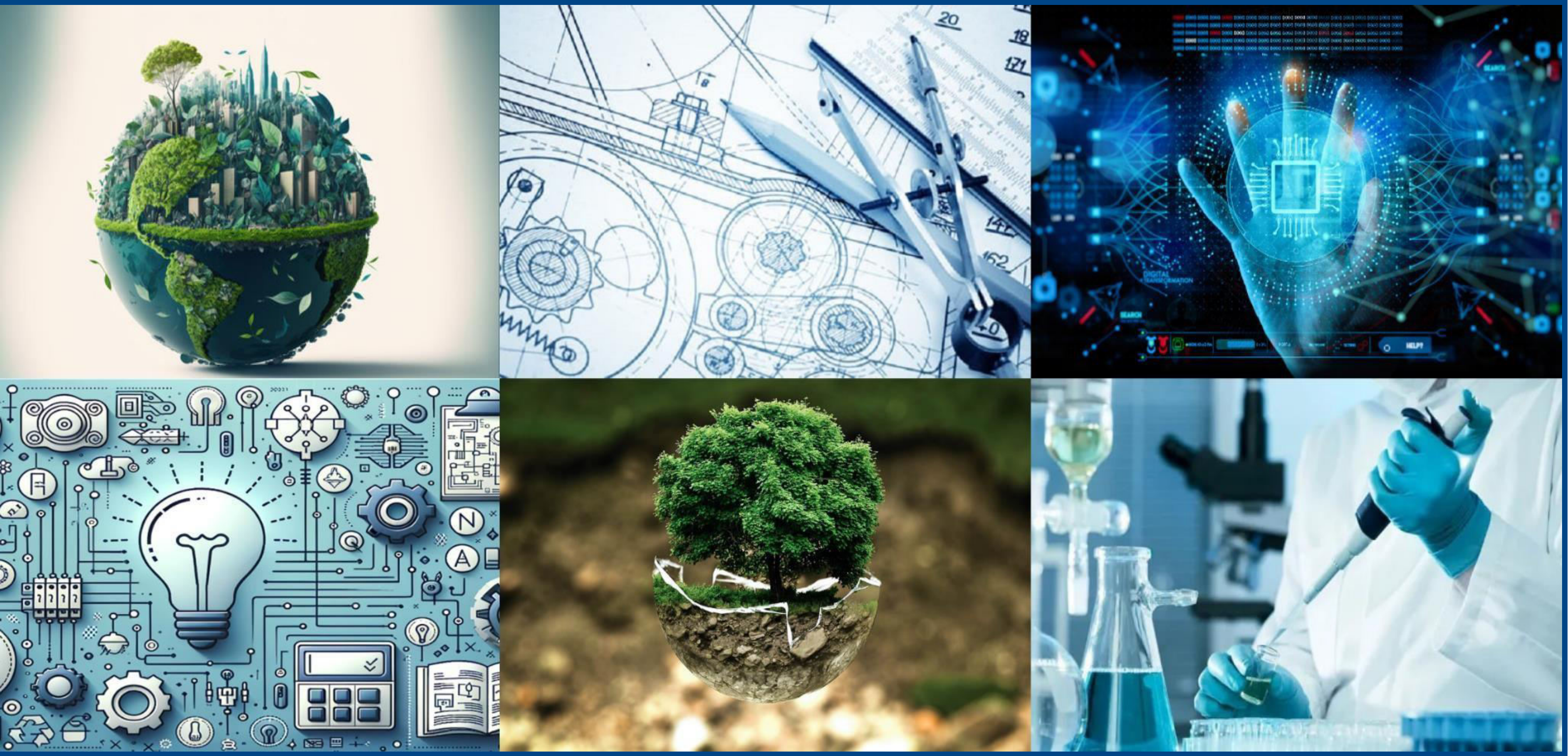
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Special Issue 2, November 2025

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

Unified Smart Card System for Secure Authentication and Access Control

S. Sigappi[1], D.Ramya Cauvery[2], B. Jeyanthi[3], S. Harishka[4]

Assistant Professor, Department of Computer Science and Engineering, Mookambigai College of Engineering, Pudukkottai, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Mookambigai College of Engineering, Pudukkottai, Tamil Nadu, India[2]

Assistant Professor, Department of Computer Science and Engineering, Mookambigai College of Engineering, Pudukkottai, Tamil Nadu, India[3]

Department of Computer Science and Engineering, Mookambigai College of Engineering, Pudukkottai, Tamil Nadu, India[4]

ABSTRACT: The Unified Smart Card System is developed to integrate multiple access functionalities into a single, secure authentication platform. This system eliminates the dependency on multiple identification cards by providing a unified and encrypted authentication mechanism. The proposed model utilizes advanced encryption algorithms, role-based access, and real-time verification to ensure data integrity and system security. Simulation models and conceptual hardware implementations demonstrate that the system is efficient in preventing unauthorized access, enhancing operational convenience, and improving overall security scalability across different institutional environments.

KEYWORDS: Unified Smart Card, Encryption, Authentication, Access Control, Security System.

I. INTRODUCTION

In recent years, organizations have increasingly relied on digital identification and smart card systems to manage access control and authentication. Traditional systems require separate cards for each service, creating inefficiencies and potential vulnerabilities. The Unified Smart Card System addresses these issues by combining multiple access points under one secure authentication mechanism. By incorporating encryption techniques and centralized validation, the system ensures that each user interaction is verified through a robust and secure channel.

II. PROPOSED SYSTEM

The proposed system comprises several interconnected components that work together to achieve secure authentication and data protection. The core elements include an authentication server, encryption/decryption module, smart card interface, user database, and alert mechanism. Upon scanning a smart card, the system retrieves encrypted credentials, validates them against the database, and grants access accordingly. Figure 1 illustrates the block diagram of the proposed Unified Smart Card System.

| DOI: 10.15680/IJMRSET.2025.0811626 |

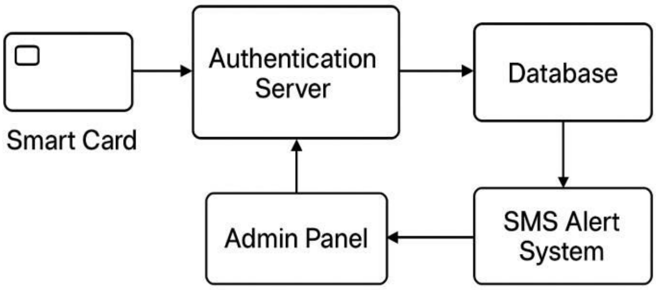


Fig. 1 – Block Diagram of Unified Smart Card System

III. MATHEMATICAL MODELLING

The authentication and encryption mechanisms can be mathematically represented as follows:

Let U = {u1, u2, ..., un} represent the set of users, and C = {c1, c2, ..., cn} represent the corresponding credentials.
Authentication function: A(u, c) → {0,1}, where 1 indicates valid access and 0 indicates denial.
Encryption: E = Enc(K, c), where K is the encryption key.
Decryption: D = Dec(K, E), where D(c) = stored(c) ⇒ Access Granted, else ⇒ Access Denied.

IV. FORMATTING OF TABLE

Table 1 - Performance comparison of system metrics.

Parameter	Value A	Value B
Authentication Time (ms)	0.8	1.2
Encryption Delay (ms)	1.5	2.0
Accuracy (%)	99.2	98.7

V. SIMULINK MODELLING AND RESULT

A Simulink model was developed to simulate the logical workflow of the authentication mechanism. The model represents input signals as user credentials, while the processing blocks execute encryption and verification. Results indicated that legitimate users were authenticated within milliseconds, while unauthorized users were denied access immediately.

VI. HARDWARE AND RESULT

The conceptual hardware design integrates an RFID reader, microcontroller, and LCD interface. When the smart card is scanned, the microcontroller communicates with the authentication server via a secure channel. Verification results are displayed in real-time, and unauthorized attempts trigger an alert message. This hardware prototype validates the system's reliability and speed under simulated environments.

VII. CONCLUSION

The Unified Smart Card System provides a comprehensive and secure solution for multi-level authentication and access control. By combining encryption algorithms and centralized data management, the system ensures improved security and operational efficiency. This model can be further extended to large-scale organizations, educational institutions, and government applications to enhance data protection.

VIII. ACKNOWLEDGEMENTS

The author expresses sincere gratitude to the Department of Computer Science and Engineering, Mookambigai College of Engineering, for providing guidance and resources for the successful completion of this research work.

REFERENCES

1. von Busch, O., & Palmas, K. (2016). Designing consent: Can design thinking manufacture democratic capitalism? Organizational Aesthetics, 5(2), 10–24.
2. Brader, T. (2006). Campaigning for hearts and minds: How emotional appeals in political ads work. University of Chicago Press.
3. Jang, S. (2019, August 8–11). Deconstructing the opposition of natural/arbitrary in Coleridge's theory of language [Paper presentation]. NASSR 2019: Romantic Elements, Chicago, IL, United States.
4. Saini, N., & Kumar, R. (2023). Smart card-based secure access control systems using encryption. IEEE Access, 11, 55421–55430.
5. Ahmed, M., & Khan, A. (2022). Multi-level authentication framework for secure IoT access. International Journal of Computer Applications, 182(35), 10–15.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com