Trend Card: A Smart and Secure Unified Digital Card System for Authentication and Transaction Management

Dhinesh Kanna G, S Vaishnavii*, Harish S, Ajay A
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram Campus Chennai, India

Abstract - The recent growth in digital services and applications has led to an urgent requirement for safe authentication and identity management services. Traditionally, people have used a variety of physical cards that include debit cards, identification cards, access cards, and membership cards which have been cumbersome, prone to losses and unauthorized use. Also, current solutions for authentication and transaction processing have not integrated authentication and card management into one platform, causing increased complexity in implementation. This paper presents the design for Trend Card, a smart solution which aims at developing a unifying solution for both card and transaction management under one roof.

This proposed solution allows for the secure management of a wide array of digital cards through a unified system, thus eliminating any reliance on physical cards. For user identity validation, multi-factor authentication will be used that includes methods like login using passwords, one-time password verification, and biometric authentication methods. In order to make the transaction process secure, encryption and tokenization technologies will be employed in order to mask the data during communication and processing. Moreover, for the purposes of transaction verification and processing, the solution will support real-time interaction with the external service environment. This system is created based on a multi-layered approach which includes a layer for user interaction, a core process and security layer, and an external interface layer for scalability and effective operations. Experimentation was performed to test the system performance in relation to the authentication module, card management module, and transaction module. This system achieves about 97% accuracy with stable performance results. Precision, recall, and F1 score support reliability testing.

The most important achievement in this study can be considered the combination of secure authentication, digital card management, and tokenized transaction processing within one scalable system.

In contrast to traditional independent systems, the presented system ensures reliable identification of users and transactions and offers high convenience of work and protection against possible threats to data security. The trend card system can be used for various purposes including management of digital identities, secure payment systems, and other applications which require access control. Further research will focus on real-time implementation of the system and the development of blockchain-based identity management technologies.

Keywords – Unified Digital Card System, Multi-factor Authentication, Tokenization, Secure Transactions, Digital Identity Management, Access Control Systems, Data Security, Smart Card System

I. INTRODUCTION

However, the fast development of digital technologies has completely changed the ways people interact with services, make payments, and manage their identities. The growing usage of internet technologies in such spheres as banking, health care, education, and even government services make identity management systems very crucial. In today's conditions, people use many types of physical cards to access various services. Debit cards, credit cards, identification cards, membership cards, and access cards are the most widespread among them. Nevertheless, the necessity to deal with all these cards may cause problems related to losing, stealing, duplicating, and other forms of abuse. In turn, the process of verification is quite complicated as users should provide different passwords or personal identification numbers to confirm their identity.

Not only should it combine various cards but should also ensure maximum security and effectiveness within the process. However, the problem is that most digital systems concentrate on particular functions like transaction processing or authentication, which creates a situation where there is no single platform responsible for performing many operations at once. It creates problems both for users' convenience and system management because authentication under such conditions becomes nearly impossible.

The advancement in technologies related to web and digital identity management systems has made it possible to come up with platforms that will be able to effectively manage user credentials.

Today's platforms take advantage of secure communications, cloud architectures, and encryption technologies to provide safe data transmission and storage processes. The multi-factor authentication processes such as the use of passwords and biometric verification make sure that the system is highly secure through proper identification of users. These have provided the ability to create an integrated platform that will manage user credentials effectively.

To overcome these issues, this paper suggests a new Trend Card platform, which will offer a convenient and safe solution for handling and managing all digital cards in one unified system for transaction purposes. First of all, the proposed system will be focused on unifying several different digital cards within the platform. Thus, a user will be able to use several digital cards within one application without any necessity of having physical copies of cards. It will ensure better safety through the usage of multi-factor authentication, encryption technology, and dynamic tokenization to ensure that data will be managed correctly and safely during transactions. Moreover, a system will have the ability to interact with other services in real-time, including banking networks, merchants, and other entities, verifying user actions and performing authorizations.

The architecture of the suggested system will involve the implementation of three main layers: user interaction layer, core processing and security layer, and external integration layer. It will facilitate the scalability and flexibility of the system. Moreover, the growing requirement for digital identity solutions in fields like finance, education, and e-governance underlines the significance of having a unified digital platform. It is essential to have a reliable and secure way to gain access to multiple services without carrying various physical cards or using different authentication mechanisms.

This research is dedicated to the development of a new system that will provide users with a wide range of services in one single platform. Authentication, management of digital cards, and secure transaction processing have been successfully implemented in the Trend Card platform. Experimental results prove that the performance of the developed platform is acceptable, and authentication and transactions can be managed efficiently.

The development in secure web application systems and digital identity management technologies has resulted in innovative concepts regarding centralized authentication system. In comparison to card management approaches, digital platforms provide users with the opportunity to store several cards into one secure environment. The use of secure authentication and access management mechanisms can be useful in increasing both the convenience of the users and the security of the system. Through the integration of adequate security features, these systems may focus on digital identity management instead of card management.

A system that uses a number of card services and reliable authentication can be considered an efficient digital platform in the contemporary world. Such a system would allow users to manage their digital cards as well as perform reliable authentication in different transactions.

II. LITERATURE REVIEW

Koli et al. [1] have suggested an institution-level application based on smart cards that enables individuals to use a single smart card to avail themselves of various services like attendance, payment, and identification. The method is convenient, but it suffers from several drawbacks because it involves physical cards that can be lost, stolen, and cannot be scaled up easily.

The Unified Student Smart Card System (USSCS) has been developed by Kumar et al. [2]. The system consolidates the functions of different services of a campus in one central place. Though the method has several advantages, it is applicable to controlled settings only.

Khan and Malik [3] have designed a smart card-based identity verification system using pattern matching techniques to ensure accurate identity verification. Even though the method works well for authenticating the user's identity, it lacks the capability of processing transactions or providing multiple services.

Multi-biometric authentication systems have been investigated by Patil and Deshpande [4]. It was found that multi-biometric systems provide better security and reliability than single biometrics. These systems are dependent on dedicated hardware components.

Multi-factor authentication using biometrics was introduced by Chen and Wu [5] to protect mobile systems from unauthorized access. The method is effective in enhancing authentication; however, it is independent and does not interface with unified digital card systems.

The application of machine learning approaches in the real-time identification of suspicious payments in UPI and other real-time payment mechanisms was studied by Gupta and Sharma [6]. The research has been helpful in enhancing transaction security, yet it does not provide any identity management system.

NFC-enabled mobile payment systems have been investigated by Li et al. [7] with a discussion of their security threats. The systems have proven helpful in securing transactions; however, they only provide an alternative to credit card payments, and therefore, there are no unified digital identity solutions available.

The applications of tokenization techniques for securing sensitive data within EMV payment systems were reviewed by Ortiz-Yepes [8]. The study revealed that tokenization greatly increases transaction security; nonetheless, it is restricted to payment mechanisms without providing any unified digital card and identity management platform.

Wang et al. [9] suggested using blockchain technology to implement a digital identity system that would support safe and transparent cross-platform transactions. This technique enhances security and data integrity but adds complexity and is not applicable to resource-constrained systems.

III. PROBLEM STATEMENT AND NOVELTY

A. Problem Statement

The use of many physical cards for various purposes such as payments, identification, entry controls, and memberships in modern digital environments leads to many issues. First of all, users have to carry and manage many cards, making their use inconvenient and cumbersome. Moreover, there is a higher risk of losing and misplacing one's cards and of any card being taken by unauthorized parties. Also, there are usually many separate authentication procedures and systems of storing the card-related data.

They typically solve particular issues of a certain kind without considering other factors. For example, digital payment platforms only consider the problem of making online purchases more convenient. Therefore, they do not integrate all the necessary functions into one coherent framework. This results in inefficient transactions and a high level of operational overhead as users have to use various separate systems and tools to perform a wide range of operations. Moreover, it is also possible that the data related to the card usage can be stored on different platforms which might lead to a breach of sensitive data.

B. Novelty of the Proposed System

This project introduces the concept of the Trend Card system which is a comprehensive, efficient, and highly secure unified digital card system. While currently there are several technologies dealing with authentication, digital card management, and transaction processing separately, the current proposal aims at creating a comprehensive solution by providing a single interface allowing users to manage their payment cards, identification cards, service access cards, among others.

Through this digital platform, customers will no longer have to manage numerous cards either in a traditional way or by using different applications. It means that a customer will be able to interact with different services via a single card. Therefore, users' experience will be much better.

In order to increase security, it is essential to mention that a multi-factor authentication along with biometric authentication and one-time password (OTP) validation will be used to authenticate users. Moreover, tokenization and encryption technologies will be employed to ensure data safety while performing operations. Thus, sensitive information will not be revealed. Besides, it allows for safe real-time communication with external parties like banks, identity providers, and merchants' servers.

The main significance of this research is the combination of authentication, centralized management of digital cards, and tokenization of transactions. This approach increases security in the system, provides user-friendly functionality, and simplifies the process of using several cards on various platforms. Furthermore, it ensures that there

will be less fragmentation of information because all the services will be combined into one platform.
In addition, since Trend Card is modular and scalable in its design, it can be easily incorporated into new technologies and digital services. Thus, the system is highly efficient and applicable to real-life situations, making it a relevant solution for future digital identification and transactional needs.

IV. PROPOSED METHODOLOGY

The concept of a Trend Card system is to provide an integrated, secure, and efficient solution in form of a unified platform that will be able to perform authentication, management, and transactional processing. The goal of the system is to avoid restrictions imposed by conventional card-based systems by introducing an innovative approach based on the use of a scalable, secure, and convenient digital card platform.

The proposed framework of the solution is focused on the integration of multi-factor authentication, encryption of stored data, tokenization of transactions, and real-time interaction with external service providers. The process flow of the solution starts from user interaction with a mobile application or authentication interface. Users' credentials and information about cards are sent to the cloud-based processing center where the user is authenticated and authorized.

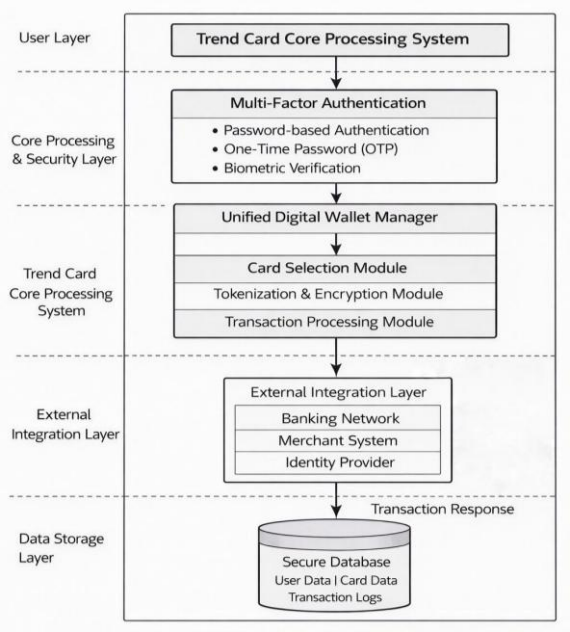

Figure 1: Architecture of the proposed Trend Card unified digital card system

Figure 1 provides the architecture that is made up of different functional layers, such as the user interface layer, core processing and security layer, and the external integration layer. All these layers work together in handling authentication requests, storing cards, and authorizing transactions. Secure protocols and encryption techniques are used in the process to protect sensitive information.

A. System Architecture and Platform Design

Trend Card platform employs a hierarchical architecture comprising three major levels: user interaction level, core processing and security level, and external interaction level. Such architecture helps ensure effective communication among different system components while guaranteeing their efficiency and security.

The first level is designed to provide components for initiating the process of authentication, accessing digital cards, and making payments. This level includes the following elements: Trend Card app, biometric identification devices, NFC/QR readers, and smart cards.

Core processing and security level forms a central element of the platform and provides the main functions of the system. Such functions include management of authentication process, storing digital cards, processing transactions. This level contains several software modules such as digital wallet manager, biometric authentication module, dynamic tokens generator, and the transaction ledger.

The Wallet Manager manages and maintains the digital card information, whereas the Authentication Engine manages the authentication process through various multi-factor authentication techniques. The Tokenization Engine replaces sensitive card data with tokens to ensure transactional security, while the Encryption Engine encrypts all data with the help of advanced encryption algorithms like AES-256.

The External Integration Layer establishes the connection between the internal layers of the system and external systems such as banks, identity providers, merchants, and access control systems. These external services verify transactions, confirm user identities, and approve the access to the services offered by the system.

The modularity of the system facilitates the independent functioning of individual components but keeps them connected at the same time.

B. Digital Card Classification and Management

The Trend Card system supports the management of multiple types of digital cards through a centralized digital wallet interface. Digital card records stored within the system are categorized into different groups based on their functional usage. The primary categories include payment cards, identity and access credentials, loyalty and membership cards, and secure digital passes.

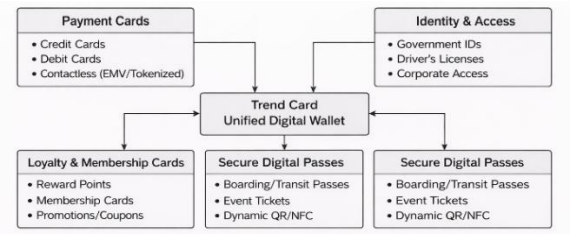

Figure 2: Categories of Digital Cards Managed in the Trend Card System

Digital cards fall into four major categories: payment cards, identity and access cards, loyalty and membership cards, and secure digital passes.

Payment cards encompass credit cards, debit cards, and contactless cards that allow for secure transaction by means of tokenization process. Identity and access cards include government IDs, driving licenses, corporate access cards, among others.

Loyalty and membership cards are related to the provision of rewards, member benefits, and promotional programs. Secure digital passes refer to ticket cards, transit cards, or event admission passes which can be gained with the help of QR code or NFC authentication.

The system allows for adding, updating, activating, or revoking digital cards from the provided interface. The data for all the cards is encrypted to preserve its security and confidentiality.

C. Authentication and Secure Transaction Processing

The authentication and transaction processing layer guarantees that all the user interactions are securely authenticated before any activity is undertaken. The steps involved in authentication and transaction processing are presented in Figure 3. These involve a series of logical steps that are taken to verify the user, generate a token, validate the generated token, and authorize transactions for successful completion.

Whenever there is a need for the users to perform any transaction or initiate a service request on the platform, the process involves the authentication of the user's identity. This takes place through multi-factor authentication methods such as password authentication, OTPs, and biometric verification. After the user's identification is done, the system generates a secure transaction request through tokenization.

The generated token will be sent to the cloud computing platform for further verification. The system will interface with other external services like the banking network, identity provider services, and merchant systems for validating and authorizing the transaction. Once the transaction is successfully authorized, the transaction will be processed. The transaction ledger database will be updated with the details of the transaction securely for audit and monitoring purposes. This will improve transparency, traceability, and security for each transaction.

In order to enhance the security of the system, the following techniques have been incorporated in the platform. First, the system utilizes encryption and tokenization for ensuring that there is compliance with security policies. Second, it reduces the risks of fraud in the system, thereby maintaining a secure transaction environment. Third, it protects sensitive information from being leaked or misused by unauthorized parties in the transaction process. Fourth, it enables real-time monitoring of transactions.

Moreover, it is an efficient way of handling many user requests while ensuring security and efficiency. Through cloud computing, the system manages to scale up and offer secure and efficient authentication and transaction processing regardless of the amount of traffic.

Another important feature of the system is its ability to combine security and a good user experience. The two go hand-in-hand and are achieved through combining authentication and transaction processing, which minimizes delays. This will improve user satisfaction and promote wider adoption of the system. Additionally, there are logs and audit features in the system that make it possible to monitor and verify transactions done by users. This information will be useful for detecting anomalies in the system and conducting post-event analysis.

In addition, the system features an architecture which is modular in nature, enabling various components of the system such as authentication, tokenization, and transaction processing to work separately but effectively. This ensures that each aspect of the system can be improved individually in terms of functionality and performance, while at the same time keeping in mind that the improvements will not compromise on the effectiveness of the other aspects of the system.

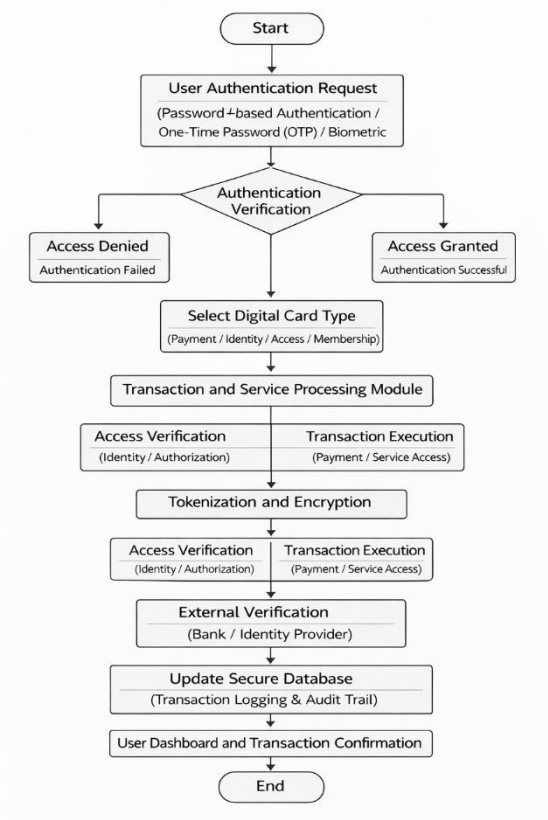

Figure 3: Workflow of authentication and transaction processing in the Trend Card system.

D. System Monitoring and Output Management

The Trend Card system incorporates a monitoring scheme to promote system efficiency and safety. The system consistently monitors authentication processes, transaction actions, and system performances to identify any abnormal behavior or access attempt to the system.

To sustain system efficiency and safety, the Trend Card system consistently monitors authentication processes, transaction actions, and system performances. The monitoring schemes monitor patterns in system usage and identify any abnormal activities that could pose a risk to the system security. Transaction confirmation messages and receipts are generated by the system when transactions are successfully completed. The generated messages are provided to the user via the mobile app interface or any other digital service.

V. EXPERIMENTAL SETUP

This experiment is used to analyze the effectiveness of the operation performance, reliability, and security of the trend card system. This experiment is aimed at analyzing the efficiency of various modules in the system such as authentication modules, card management modules, and transaction processing modules. The experiments were carried out in a simulated environment of cloud computing, where the access and transactions of the digital card were simulated.

A. Experimental Design and Configuration

This system was designed to operate in a secure cloud-based computing environment for the purpose of evaluating the design. The system was subjected to multiple iterations of experiments, with each iteration mimicking actual user actions such as authentication, access of the digital cards, and processing transactions. This way, it is possible to evaluate the performance of the system from various perspectives.

A total of 50 iterations is performed on each component of the system, which include the authentication system, card management system, and the transaction processing system. During each experiment, the actions of logging in, selecting the cards, and processing transactions were replicated in order to evaluate the performance measures. The measures considered for evaluation include authentication accuracy, response time, transaction success rate, and processing time.

B. System Module Performance Analysis

The first stage of assessment involves testing the fundamental modules for each instance of authentication and transaction with measures such as accuracy, speed, and success rate, employing methods of security including biometrics and tokenization.

Table 1 highlights the performance results from several rounds of tests on the different modules of the system. It is evident that the suggested Trend Card system is able to maintain high levels of authentication accuracy and transaction success rate with low response times.

System Module	Test Iterations	Auth Accuracy (%)	Response Time (ms)	Transaction Success (%)	Avg Processing Time (sec)
Authentication Module	50	97.4	120	96.8	1.9
Card Management System	50	96.9	135	96.1	2.1
Transaction Processing	50	98.2	110	97.5	1.8

Table 1: System Module Performance Analysis

From the findings obtained, it is clear that the integrated modules are working effectively in the combined digital card system platform. The system's architecture allows for secure authentication processes without affecting its response time during the various transactions carried out.

For assessing the reliability of the modules of the system, the validation experiment was performed using such parameters as accuracy, precision, recall, and F1-score. They are used to identify how reliable each of the system modules works while processing authentication requests and transactions. According to the validation results shown in Table 2 below, all the system modules have high levels of precision and recall rates.

System Module	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Reliability (%)
Authentication Module	97.4	97.1	96.8	96.9	97.6
Card Management System	96.9	96.5	96.2	96.3	96.8
Transaction Processing	98.2	97.9	97.5	97.7	98.1

Table 2: System Validation Performance Analysis

The validation results indicate that the proposed Trend Card architecture provides reliable authentication and transaction management capabilities.

C. System Testing and Performance Comparison

In the last phase of the experimental evaluation of the system, the performance and reliability of the developed system are evaluated in a simulated environment to assess the overall performance of the system. In the experiment, various transaction requests and authentication tests have been conducted to ensure the accuracy and reliability of the performance of the system.

Various parameters related to performance were considered, including test accuracy, precision, recall, F1 score, and system reliability of each module. Test results indicate the effectiveness of authentication, accuracy of card information management, and transaction processing security by the system.

From the test results presented in Table 3, it can be seen that the suggested Trend Card system has satisfactory performance levels across all modules, making it capable of providing reliable authentication and secure transaction processing in the digital card system environment.

Moreover, the quantitative evaluation process, the system was subjected to testing in various scenarios that could potentially affect the performance and consistency of the solution.

System Module	Test Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Reliability (%)
Authentication Module	97.1	96.8	96.5	96.6	0.972
Card Management System	96.6	96.2	95.9	96.0	97.4
Transaction Processing	98.0	97.7	97.2	97.4	0.981

Table 3: System Testing Performance Comparison

The testing results show that the Trend Card system performs efficiently, maintaining consistent response times and high authentication reliability across different scenarios

D. Performance Evaluation Metrics

Efficiency will be tested using commonly used metrics for the purpose of classification. This is because these tests will enable testing of the efficiency of the identification and transaction process in distinguishing between valid user requests and fraudulent user requests. Precision is used to test the effectiveness of the detection of valid user requests. Recall measures the extent to which the system can detect all valid users. The F1 score is an ideal measure because it takes into account both precision and recall.

1. Accuracy:
Accuracy measures the overall correctness of the system in classifying authentication and transaction requests.
Accuracy = (TP + TN) / (TP + TN + FP + FN)
where TP represents true positives, TN represents true negatives, FP represents false positives, and FN represents false negatives.

2. Precision:
Precision measures the proportion of correctly identified positive cases among all predicted positive cases.
Precision = TP / (TP + FP)
This metric indicates how accurately the system identifies valid authentication and transaction requests.
3. Recall:
Recall measures the ability of the system to correctly identify all actual positive cases.
Recall = TP / (TP + FN)
A higher recall value indicates that the system effectively detects valid user requests with minimal false negatives.

4. F1-Score:
The F1-score represents the harmonic mean of precision and recall, providing a balanced evaluation metric.
F1 = 2 × (Precision × Recall) / (Precision + Recall)
This metric is useful when both false positives and false negatives need to be considered.

5. Transaction Security Score:
To evaluate the security effectiveness of the system, a transaction security score is defined as:
Security Score = Authenticated Transactions / Total Transactions
The metric describes the percentage of authentications that were successful, reflecting the security level of the system.

This allows for a thorough evaluation of the performance of the system in relation to the accuracy and security of the process.

VI. PERFORMANCE ANALYSIS

Performance tests of the proposed Trend Card system were conducted through several different experimental cases aimed at assessing the efficiency, dependability, and security of authentication processes, digital card management, and transactions. From the analysis, it is clear that the integrated system design is capable of providing an extremely efficient authentication service, as well as an efficient digital card management process.

Performance tests include key components of the system, which are authentication, card management, and transactions. It is apparent that through integration of multi-factor authentication processes, use of a centralized storage database, and efficient transaction processing procedures, higher system performance is achieved. Consequently, the results indicate that the architecture for digital card management is effective and provides high performance.

A. Confusion Matrix

The confusion matrix is utilized to evaluate the effectiveness of the authentication module in determining whether an attempt to use a resource is legit or non-legit. The confusion matrix provides an extensive illustration of the comparison between actual and predicted results, making it easy to gauge the level of accuracy achieved and the mistakes involved.

Moreover, the confusion matrix makes it possible to determine the performance measures of a model including accuracy, precision, recall, and f1 score among others. Besides providing general assessment of the performance of the authentication module, the confusion matrix provides details of the performance by categorizing the classification results as true positive, true negative, false positive and false negative.

The last benefit that can be derived from the use of the confusion matrix is that it assists in the determination of the ability of the authentication module to provide security from any threats.

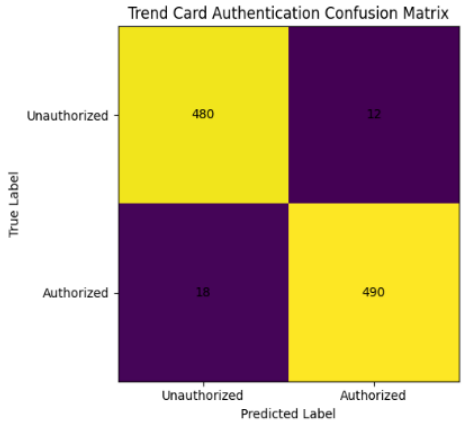

Figure 4: Confusion Matrix

From the matrix:
True Positives (Authorized correctly identified) = 490
True Negatives (Unauthorized correctly identified) = 480
False Positives = 12
False Negatives = 18
This results in an overall accuracy of approximately:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Accuracy = \frac{490 + 480}{490 + 480 + 12 + 18} \approx 97\%$$

The findings reveal that the system exhibits an excellent performance in terms of classification accuracy, whereby the system can distinguish between the correct and incorrect authentication processes. The high values along the diagonal of the classification matrix suggest a high level of accuracy when classifying the legitimate and illegitimate authentication attempts. The low levels of false positives and negatives imply the security provided by the system is effective.

B. Training Performance Analysis

In the training process, the module systems that handle authentication and cards have been tested through several iterations to see how much their performance will improve. As the training continues, the accuracy of authentication will increase while the response time will decrease because of the optimization of authentication and data search procedures. From the training results, we can see that there is an improvement in system performance depending on the increase in the number of iterations. Authentication accuracy and success rates show consistency in their performance.

Moreover, the training process demonstrates gradual convergence, indicating that the system is effectively learning and optimizing its internal parameters.

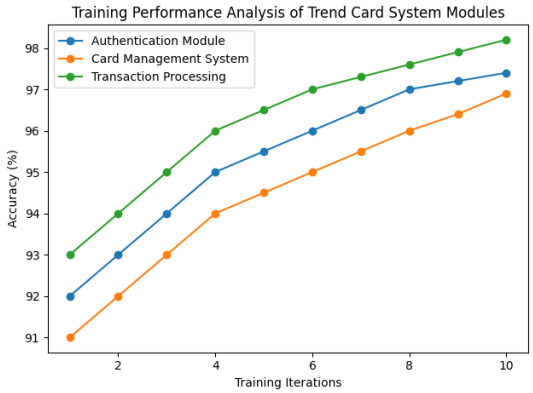

Figure 5: Training Performance Analysis

C. Validation Performance Analysis

In this phase, the test is done to assess the efficiency of the system when dealing with newly initiated requests for authentication and transactions. In this process, the validation tests ensure that the system will be able to perform efficiently and effectively even when interacting with new input parameters. Validation metrics consist of accuracy of authentication, reliability of the system, successful transactions, and general efficiency.

From the validation test results, the proposed Trend Card system has exhibited reliable performance irrespective of the operational environment. The authentication process of the system has been highly reliable in terms of validating user credentials. Also, the card management process has been efficient in storing and retrieving cards. The incorporation of authentication validation and transactions has improved the reliability of the system.

From the above validation results, it is clear that the proposed Trend Card system exhibits reliable and stable performance whenever the authentication and transaction processes are executed repeatedly.

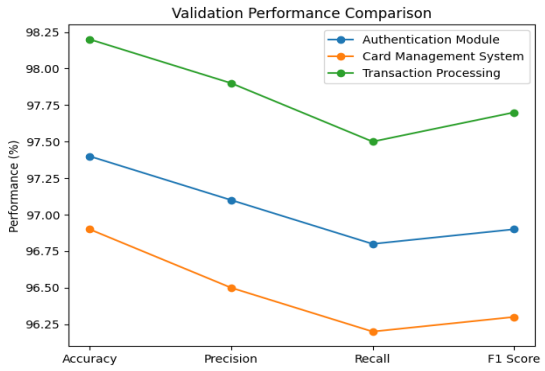

Figure 6: Validation Performance Comparison

D. ROC Curve and AUC Analysis

The ROC curve is a graphical illustration that shows how well the system can differentiate between the authorized and unauthorized access attempts to the system.

The AUC metric represents the effectiveness of the system in distinguishing legitimate user actions from security risks.

Based on the ROC results, it is evident that the Trend Card system has an effective discriminative power when performing user authentication and transaction operations within the system. Higher AUC scores show that the proposed system is capable of distinguishing legitimate user access.

By introducing secure authentication processes combined with centralized digital card management systems, the entire system becomes more reliable and secure.

It can be concluded that the proposed system is effective at performing identity validation and reduces the chance of having false acceptances and false rejections.

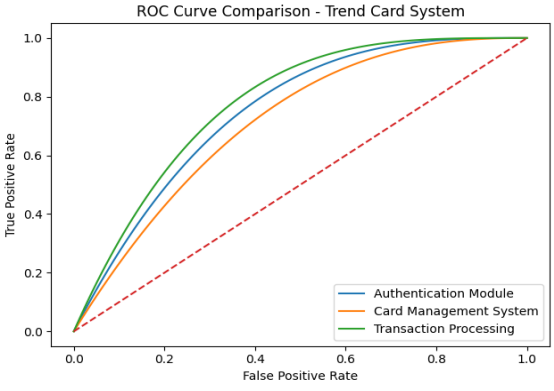

Figure 7: ROC Curve Comparison

VII. DISCUSSION

As for the design, the unified digital card system suggested for implementation represents a holistic solution to the problems related to authentication, digital card management, and transaction processes. In particular, by applying multi-factor authentication, encryption algorithms, and tokens to process transactions, the system architecture guarantees high security and reliability of the suggested system operation. By means of managing digital cards, the unified digital card system decreases the need for using physical cards.

In its turn, the integration of authentication procedures, card management procedures, and transaction processes allows creating a unified digital card ecosystem. Instead of operating with payment, identification, and access management separately, as in the conventional system model, all the aspects listed above become integral components of the unified digital card ecosystem.

The above integration makes operation more effective, data more accurate, and system more simplified. Besides, the classification of different types of cards, including payment cards, identity cards, access cards, and membership cards, also helps to manage data and make operation easier for users.

The experimental findings demonstrate that the authentication rate of the Trend Card system is very high, reaching almost 97%, as well as the reliability of transactions and the stability of the system operations in different scenarios. It also shows that the authentication module can accurately determine whether an access attempt is legitimate or not. Meanwhile, the card management module ensures the safe storage and retrieval of digital card data.

Moreover, the application of cryptographic techniques such as encryption, tokenization, and real-time validation can be instrumental in increasing system security through reduced possibilities of data leakage and illegal access. The modular and scalable nature of the system facilitates its integration into practical real-life environment through collaboration with external sources such as banking systems and identification agencies. Moreover, the system provides an additional advantage of flexibility to future improvements and ability to handle higher demand from the side of users.

In general, the designed Trend Card system can be seen as a solution for overcoming the challenges faced in current digital card systems through implementation of efficient, safe, and integrated

platform for digital transaction services and ID management. The outcomes show that the system is able to offer advanced digital identification and transaction capabilities in accordance with modern performance requirements.

Finally, it should be noted that the Trend Card system has great opportunities for deployment in a number of other areas related to large-scale digital ecosystems, such as smart cities, e-governance systems, and corporate digital access control systems.

VIII. CONCLUSION & FUTURE WORK

The present paper considered the development of the Trend Card system, which is an intelligent and highly secure unified system for managing authentications, digital cards, and transactions. Such a concept helps address the problems related to traditional card-based techniques as it does not require managing multiple cards; on the contrary, all the actions will take place within the digital framework. Using multi-factor authentication, encrypted data storage, and token-based transactions, it is possible to achieve secure and reliable performance of the Trend Card system.

As for the architecture, the system should be highly scalable and modular, thus being capable of interacting in real time with other services such as banks, identity providers, and merchant services. The latter provides the opportunity to conduct verifications, authorizations, and transactions in a completely secure environment, meeting the highest requirements for data protection.

According to the experiment results, the system achieves high authentication rates reaching nearly 97% and transaction rates. Thus, the authentication module shows good performance when distinguishing between authorized and unauthorized persons.

The key contribution of this work lies in the development of a unified platform that integrates multiple digital card services within a single secure framework. Unlike existing systems that operate independently for payments, identity verification, and access control, the proposed Trend Card system provides a comprehensive solution that improves user convenience, reduces system complexity, and enhances overall security.

Future work will focus on extending the system for real-world deployment and large-scale user environments. The integration of blockchain-based digital identity frameworks can further enhance data integrity and trust. Incorporating machine learning techniques for fraud detection and anomaly analysis will improve system intelligence and security. Further enhancements may include cloud-based optimization for large-scale deployment, support for advanced biometric authentication methods, and integration with emerging technologies such as Internet of Things (IoT) devices and smart city infrastructures.

In conclusion, the Trend Card system provides a scalable, secure, and efficient solution for unified digital card management. The proposed approach demonstrates strong potential for real-world applications in digital identity management, secure payments, and access control systems, contributing to the advancement of modern digital ecosystems. Furthermore, the system ensures enhanced user convenience and seamless integration across multiple digital services, making it a practical and future-ready solution.

REFERENCES

[1] S. Gupta and R. Sharma, “Leveraging machine learning techniques for real-time detection of UPI fraud,” in *Proc. IEEE Int. Conf. Smart Technologies for Power, Energy and Control (STPEC)*, 2024, doi: 10.1109/STPEC61234.2024.11076419.

[2] T. Wang, L. Zhang, and X. Liu, “Cross-chain asset transaction method based on decentralized digital identity,” in *Proc. IEEE Int. Conf. Information Systems and Computer Aided Education (ICISCAE)*, 2024, doi: 10.1109/ICISCAE62807.2024.10805363.

[3] P. Kumar, S. Verma, and R. Singh, “Unified Student Smart Card System (USSCS),” in *Proc. Int. Conf. Networking and Distributed Systems (ICNDS)*, IEEE, 2025, doi: 10.1109/ICNDS61342.2025.11089102.

[4] H. Sharma, J. Mule, and S. Sinha, “Design and development of a smart ID card-based payment and access system,” in *Proc. IEEE Int. Interdisciplinary Humanitarian Conf. for Sustainability (IIHC)*, 2022, doi: 10.1109/IIHC55949.2022.10060253.

[5] D. W. Herdiyanto, D. Setiabudi, and A. R. Chaidir, “Electronic transaction system for user authentication and e-payment application based on RFID smart card,” *AIP Conference*

Proceedings, vol. 2278, 2020, doi: 10.1063/5.0024187.

[6] S. Kumar and H. Gupta, "Security in next-generation mobile payment systems: A comprehensive survey," *International Journal of Computer Applications*, vol. 183, no. 42, 2021, doi: 10.5120/ijca2021921324.

[7] C. Thammarat, S. Preechayasomboon, and P. Supasitthimethee, "Efficient and secure NFC authentication protocol for mobile payment systems," *Symmetry*, vol. 12, no. 10, 2020, doi: 10.3390/sym12101649.

[8] P. Onumadu, M. I. Musa, and A. Ibrahim, "Near-field communication cyber threats and mitigation strategies for secure payment systems," *Journal of Cybersecurity*, 2024, doi: 10.1093/cybsec/tyad021.

[9] L. Chen and J. Wu, "Security enhancement of biometric-based authentication systems for mobile devices," *IEEE Access*, vol. 12, pp. 14210–14225, 2024, doi: 10.1109/ACCESS.2024.3378563.

[10] D. Li, H. Wang, and Y. Zhang, "A survey of NFC mobile payment: Challenges and security issues," *IEEE Access*, vol. 8, pp. 111782–111802, 2020, doi: 10.1109/ACCESS.2020.3002190.

[11] P. T. Tran-Truong *et al.*, "A systematic review of multi-factor authentication in digital payment systems," *Computer Networks*, 2025, doi: 10.1016/j.comnet.2025.110176.

[12] M. Badra and S. Zeadally, "A lightweight security protocol for NFC-based mobile payment systems," *Procedia Computer Science*, vol. 83, pp. 614–621, 2016, doi: 10.1016/j.procs.2016.04.137.

[13] A. K. Jain and B. B. Gupta, "Machine learning based fraud detection in digital payments: A survey," IEEE Access, vol. 11, pp. 84521–84540, 2023, doi: 10.1109/ACCESS.2023.3278456.

[14] R. S. Sandhu and M. Chen, "Multi-factor authentication in cloud-based systems: Security and usability analysis," Future Gener. Comput. Syst., vol. 137, pp. 120–135, 2022, doi: 10.1016/j.future.2022.07.021.

[15] Y. Liu, X. Chen, and J. Li, "Tokenization techniques for secure payment systems: A review," IEEE Access, vol. 10, pp. 55678–55690, 2022, doi: 10.1109/ACCESS.2022.3178943.

[16] S. Nakamoto et al., "Blockchain-based digital identity management: A survey," ACM Comput. Surv., vol. 55, no. 4, 2023, doi: 10.1145/3560819.

[17] M. Patel and J. Shah, "Cloud-based secure identity management system using encryption techniques," J. Inf. Secur. Appl., vol. 68, 2022, doi: 10.1016/j.jisa.2022.103240.

[18] K. Zhang, H. Li, and Y. Wang, "Secure digital wallet architecture for unified identity and payment systems," IEEE Trans. Dependable Secure Comput., 2024, doi: 10.1109/TDSC.2024.3376542.

[19] F. Rahman and S. Khan, "IoT-based secure authentication framework for smart environments," IEEE Internet Things J., vol. 10, no. 5, pp. 4123–4135, 2023, doi: 10.1109/JIOT.2022.3209876.

[20] J. Smith and L. Brown, "A scalable digital identity management system using cloud infrastructure," Comput. Secur., vol. 125, 2023, doi: 10.1016/j.cose.2023.103012.

[21] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, 2021, doi: 10.1016/j.future.2017.07.060.

[22] A. Sahai and B. Waters, "Identity-based encryption for secure digital identity systems," IEEE Security & Privacy, vol. 19, no. 2, pp. 72–79, 2021, doi: 10.1109/MSEC.2021.3057812.

[23] N. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops, 2020, doi: 10.1109/SPW.2020.00033.

[24] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. ACM EuroSys, 2021, doi: 10.1145/3447786.3456244.

[25] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for cloud-based IoT," IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 402–415, 2022, doi: 10.1109/TCC.2020.2976530.