JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

DYNAMIC ID-BASED USER AUTHENTICATION FOR SECURE COMMUNICATION

[#1]Dr. B.RAMESH, *Associate Professor, Department of CSE,*
[#2]Dr. S. NAVEEN ,*Associate Professor, Department of CSE,*
SREE CHAITHANYA COLLEGE OF ENGINEERING, KARIMNAGAR.

ABSTRACT: The smart card password is validated using a real two-factor authentication (2f) system. These two variables are thus "dynamic ID-based" and "anonymous." The privacy of the user is protected by smart cards because of their tamper-resistant security feature. To access certain private data stored on the smart card, methods of power analysis and reverse engineering were used. Smart card verification is carried out securely in memory, as opposed to depending on an exposed database. Commonplace programs keep password tables on servers. These apps include online banking, health care, and government systems. The user's identify is sent over public networks in plain text during the authentication procedure. There are a lot of OTP solutions out there, and while they all have great design techniques, none of them are foolproof. The server can be guaranteed to authorize a user with a valid password and one-time password (OTP) using a 2f scheme.

Keywords:*Dynamic ID, ID-Based Authentication, Secure Communication, User Authentication,Privacy Preservation, Anonymity.*

1. INTRODUCTION

The cloud allows users to store their files and data on a scalable network that may be made public or private if needed. Many services, including application hosting, data storage, processing, and material shipping, saw significant price drops as technology advanced. According to Forrester, cloud computing is a versatile platform that allows users to access services through subscriptions or on-demand. Data processing, storage, and bandwidth should be prioritized while planning a computer system.

2. RELATEDWORKS

The security of your cloud storage can be improved by using an optional two-factor authentication system. Before being sent from one party to another over a cloud server, the data is encrypted. The only piece of information needed by the sender is the name of the recipient; no other details are necessary. There are two main points that need to be grasped in order for the message to be understood by both the sender and the receiver. The first thing is the key and lock for the chest of drawers.

A security device that communicates with the equipment to prevent unauthorized access. Finding the secret requires all the necessary pieces to be in one's possession. Turning off security features should be your first move in the event that your device is stolen or misplaced. Data stored in the cloud is protected by the protocols of the security device. The friend is briefed on how the strategy works. Data encryption prevents cloud servers from deciphering encrypted data. We anticipate success with this approach because it seems to be working. A security device,

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

secret key, and knowledge of the encrypted data are necessary to access data stored in the cloud. Improving data security, the cloud server discreetly and quickly replaces the necessary encryption text when the device is deactivated.

Several flaws in the EMV protocol and its execution were pointed up by the author. Using counters, timestamps, and proprietary algorithms to produce EMV card nonces was unsecure, which is the main concern. More and more people are starting to notice that "pre-play" attacks using fake cards are not legitimate. A key component of the vulnerability assessment process is the demonstration of proof-of-concept attacks against ATMs and terminal equipment, outlining the scope and possible vulnerabilities of these systems.

The widespread use of automated teller machines (ATMs) by major companies led to serious problems. Banks refused to pay out since it was the customer's fault and because EMV cards cannot be copied. Since every random number is distinct, the same circumstances that can cause a protocol to fail could also allow an attacker to compromise the card's identifying code. The primary goal of the research was to determine if there was a way to circumvent detection by taking advantage of loopholes in the EMV standard's formal analysis, design, and implementation. 2 Protecting users' identities is one of the main benefits of two-factor authentication. No one had ever created a user-anonymity system that used block ciphers, lightweight symmetric key primitives, and hash functions previously. Protecting user privacy is the primary goal of two-factor authentication.

The two-factor method works in every situation. Complex as it is, the research deepens our comprehension of user privacy. Our customers may rest easy knowing that two-factor authentication is more secure now. Using immutable smart cards and very basic symmetric cryptographic algorithms, they investigated the possibility of creating a two-factor authentication system that protects user privacy. Any scenario calling for two-factor authentication can be addressed by applying this idea.

Customers' perceptions of automated telephone banking's usability and security, along with one-factor and two-factor authentication, were investigated in this research. In order to implement two-factor authentication, sixty-two knowledgeable bank customers in a controlled environment used a hardware security token to create a unique passcode. We ran a survey to find out how people felt about the safety and ease of use of a modern automated telephone banking service, as well as whether they preferred one-factor or two-factor authentication. You can use the results to help you choose between the two authentication techniques, which showed that they were significantly different.

The suggested smart card has two ways to prove you know the password. You won't require a verification table or to change credentials on remote servers to use this authentication method. Once the encrypted channel is set up, it becomes possible to verify the identities of both parties. Networks with synchronized timings can be protected from malicious replay attacks using nonce-based approaches. Some have suggested that

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

users' identifying devices or smart cards be used to validate their passwords. Instead of entering their name, users have the option to select or change their password.

Authenticated Key Exchange (AKE) relies on passwords and gets them from a database that has every possible password. A lot of time was needed for many steps. Attacks based on guessing, forward secrecy, and session key compromise are all taken into account in this design. The first order of business is to complete the AKE. The effectiveness of the Encrypted Key-Exchange (EKE) protocol in guaranteeing security for two-flow protocols is illustrated using an ideal cipher scenario. By implementing methods for authenticated key exchange and mutual authentication, private channels can be established across an unsecured public network. The goals can only be attained with the establishment of a secure protocol that makes use of high-entropy cryptographic keys.

Proving that protocols are resilient to linguistic attacks is not always easy. To ensure user privacy, AKE uses a three-stage D-H key exchange. When a protocol is first set up, there is a predefined attribute called the "common reference string" that anyone can access. This means that sharing public keys is optional for all parties involved in a communication. Decryption takes almost four times as long as it would with a regular protocol since the D-H key exchange protocol is distinct and does not use authentication. Because it is based on tried-and-true security principles, this technique is both easy to use and safe for password-only authentication.

Password security based on key agreements is a reliable and effective solution. Although tracing functions improve security in communication pathways, it is still not feasible to tell if the same smart card has re-authenticated inside the same session. When it comes to DOS attacks, the first tactic works. For safe hashing, more efficiency, and less expensive communication, smart card symmetric ciphers are the way to go. Attacks like as denial of service, brute-force password attempts, and malevolent insiders are all prevented by our solution. Secured against key exchange, unauthorized access, and password sharing, it verifies identities and prohibits unauthorized access.

3. EXISTINGSYSTEM

The conventional approach to smart card authentication in a decentralized system handles two types of security flaws. A customer's identify can be verified using a smart card and PIN. Unlike when using a simple password, the server does not save any sensitive information while using two-factor authentication. Before they may use the service, customers need to sign up. Important keys will be protected by fingerprints. This is accomplished by utilizing the setup protocol's identity key agreement.

Data belonging to users can be easily accessed by an adversary, who can then use this information to conduct an attack. It is possible for a person with malicious intent to use a user's static username in order to monitor the user's every action while they are checking in. Through the utilization of a safe and untraceable smart card, it is possible to improve the level of

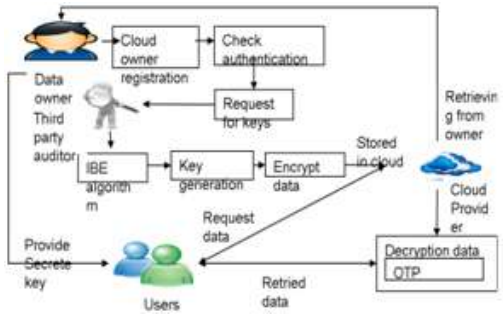
JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

privacy and security of password authentication methods for users. Smart cards that have been misplaced can now be protected against attacks using a secure mechanism that has been created.

Disadvantages

- Data pertaining to the user needs to be erased.
- The first secret code is not secure.
- The database's security is difficult to maintain.
- The security system and user data are accessed and altered by an unauthorized person.

4. PROPOSEDSYSTEM



A two-factor (2F) authentication technique that is both anonymous and cumbersome is the goal of the suggested approach. Password security in distributed systems is best achieved with two-factor authentication (2FA). A group of users and a remote server make up a standard smart card authentication system. In contrast to two-factor authentication, which does not save any private information on the server, the regular password does maintain information in the server's password database. A breach in the table will cause the whole system to collapse. Because the server does not save any passwords, the identities of millions of users are safe from any potential security breaches. In order to evaluate this program type fairly, new design objectives have been created.

Also, changing your password does not require contact with the server. Changes to the main processes, including changing a password, creating an account, verifying a user's identity, and removing an account, are visible to users.

Once the user registers and provides the server with some sensitive information, they will be sent a smart card. We will need this card for identity verification later on. This step is only required if the user plans to re-register. The user's private information and identity will be kept safe during the whole smart card authentication process.

Advantages

Protecting the database becomes more difficult after the initial secret code is compromised and user personal information needs to be erased.

The unauthorized user should be able to change their own data and security settings after logging in.

Modules

- Enrolment
- Factors verification
- Change the factor
- Next verification
- Performance evolution

Enrolment

Secret data is being accessed by the computer. Having a distinct password for every user is crucial due to the shared authentication approach. A user's identify can be more easily verified with the help of the password. During registration, it is essential to set up access control for server sites. It appears that all users who have registered have been able to access their accounts.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

Factors verification

Verified users are the only ones who may access. The first step must be executed correctly by the user. Prerequisite to gaining access to your account is the submission of the second item. The absence of tamper resistance necessitated the implementation of semantic security, also known as AKE security, to provide a baseline degree of protection against offline password guessing and impersonation attacks. Following is a concise description of the ROM semantic security proof.

- A model was first created with the intention of providing random answers to specific questions and the same answers for subsequent queries.
- The targeted protocol P's semantic security could be compromised by an attacker A.
- Protocol P can be eventually compromised using A, and then any of the current methods for addressing cryptographic primitives can be used to undermine it.
- Any authentication system that uses more than 2f cannot be used with the 3f security proof methodology. Even a highly protected "black box" can be breached by determined cybercriminals.
- The 2f version of the problem is ignored in order to do this. A misplaced smart card is one of the five scenarios. A has the ability to monitor and control all data streams leading up to the user's card being shown.

Change the factor

The second component is completely up to the person making the change. The user's registered cellphone number receives a text message with the changed password. A manager's random selection of the variable is in order. Because of their unfettered access, the intruder—probably an espionage agent—may target businesses that depend on the communication network. If none of them handles the transaction well, A might find out what's going on. The ideas of preemptive secrecy and protracted deceit were put to the test by putting the legal parties at risk. In order to steal information from the smart cards, they used infected card readers and side-channel attacks.

Hackers can easily gain access to sensitive user information through card readers. If someone enters their password into a malicious card reader and then acts strangely, it's quite improbable that the criminal will be able to get their hands on the card with the sensitive data.

The low assault cost and difficulties in compromising the smart card make it tricky to formulate a successful strategy. Because static user identity is predictable and there aren't enough encryption protections, guesswork attacks can happen. The second thing is that a lot of people talk about it and spread the word about it online. Notify the phone of the new password and update the old one.

Next verification

A new password in addition to the original authentication factor is necessary to restore account access. The user's new password is sent to their smartphone and is stored there until they log in again.

Performance evolution

- User authentication is protected by this method.
- The use of modern technological

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

instruments greatly streamlines the process of confirming the identity of unwanted guests.

- Passwords can be safely stored and updated on your personal computer using the DA2-Local-Secure approach.
- Checkers checked the user's input of the password during authentication to make sure it was correct.
- The usage of this method could make user authentication easier.
- Attacks that required several simultaneous sessions, such thinking, reacting, or impersonating people or websites, caught us off guard.

5. RESULTS

Fig:1 PlanSelection

Fig:2Activation of Plan

Fig:3 FileUploading

Fig:4 EnteringtheSecretKey

Fig: 5 DownloadingtheFile

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/23
DOI: https://doi.org/10.5281/zenodo.19091854

6.CONCLUSION AND FUTURE ENHANCEMENTS

The creation of the covert two-factor approaches was fraught with problems and difficulties. The methodology also shows how all the different aspects are related to each other. For the purpose of managing "SR6" lost smart cards, no solution is expected to offer "timely typo detection," a "DA10" capability, or "genuine local password updates." An effective strategy, competent protocol designers and security specialists, better evaluation criteria, and better decisions on usability and utility would all contribute to anonymous 2f systems' success.

REFERENCES

1. Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang – "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, Vol. 65, No. 6, June 2016
2. Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson – "Chip and Skim: Cloning EMV Cards with the Pre-Play Attack", IEEE Symposium on Security and Privacy, San Jose, CA, pp. 18–21, May 2014
3. Ding Wang, Ping Wang – "On the Anonymity of Two-Factor Authentication Schemes for Wireless Sensor Networks: Attacks, Principle and Solutions", Computer Networks, Elsevier, August 2014
4. Nancie Gunson, Diarmid Marshall, Hazel Morton, Mervyn Jack – "User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking", Computers & Security, pp. 208–220, 2011
5. Wen-Her Yang, Shiuh-Pyng Shieh – "Password Authentication Schemes with Smart Cards", Computers & Security, Vol. 18, No. 8, pp. 727–733, 1999
6. Mihir Bellare, David Pointcheval, Phillip Rogaway – "Authenticated Key Exchange Secure Against Dictionary Attacks", Springer, 2000
7. Jonathan Katz, Rafail Ostrovsky, Moti Yung – "Efficient and Secure Authenticated Key Exchange Using Weak Passwords", ACM, 2009
8. Xiangxue Li, Weidong Qiu, Dong Zheng, Kefei Chen, Jianhua Li – "Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards"