Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

ENHANCED SECURITY PROVISION FOR EFFICIENT AND SECURE DYNAMIC ID-BASED AUTHENTICATION KEY AGREEMENT SYSTEM

[#1]NAKATI SUSMITHA, ***Department of MCA,***
[#2]P.SATHISH, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

Abstract: A realistic two factor (2f) authentication is used for smart card password verification. As a result, the two variables are "dynamic ID-based" or "anonymous". To preserve user privacy, smart cards have a tamper-resistant security feature. Reverse engineering and power analysis approaches were used to obtain certain private data from the smart card memory. Rather than relying on a vulnerable database, smart card verification is securely implemented in memory. Daily applications such as e-banking, e-health, and e-governance store password tables on a server. Throughout the login process, the user's identity is sent in clear across public networks. Many non-tamper-resistant OTP solutions have been developed, all with ambitious design processes. A 2f system can ensure that a user with a valid OTP and password will be approved by the server.

IndexTerms:*2fauthentication,EMV,AKE,DA2localsecure*

1. INTRODUCTION

Using cloud computing, files and data may be stored on a scalable network that can be made public or private on the fly. As this technology advanced, the cost of several services, including app hosting, data storage, computation, and content distribution, decreased significantly. Forrester [1] defines cloud computing as an elastic computing model that provides on-demand or subscription-based service to end users. The design of a computer should prioritize bandwidth, data processing, and storage.

2. RELATED WORKS

The security of cloud storage can be managed with an optional two-factor login method. The data is encrypted before being sent from the sender to the recipient via a server in the cloud. The sender must know the recipient's name; all other details are irrelevant. Both the sender and the recipient need to know two things for the message to be deciphered. The first is the lock and key to the storage chest.

A connected gadget that serves to safeguard the machine. You can't find out what's concealed unless you have all the pieces. If you lose your device or it gets stolen, the first thing you should do is disable the security features. Data stored in the cloud is encrypted using the procedures in the security device. The buddy is briefed on the process. Cloud servers are not able to decipher encrypted data. It appears that this strategy will be effective and can be implemented. Accessing data stored in the cloud requires a security device, a secret key, and knowledge of the encrypted data. When the device is turned off, the cloud server immediately and secretly replaces the matching cipher text, making the data even more secure.

The EMV protocol and its implementation were found to have serious flaws by the author. The fundamental issue is that nonces for EMV cards were generated using counters, secret algorithms, and time stamps, which is not secure. There is now public knowledge of a scam "pre-play" attack involving counterfeit cards. Proof-of-concept assaults on automated teller machine and terminal equipment, along with their breadth and potential weak points, are mapped as part of a vulnerability discovery methodology. Issues were discovered in widely deployed ATMs utilized by major corporations. Banks refused to compensate the customer since EMV cards cannot be duplicated and the customer committed a mistake. The card's identification code is vulnerable to attack for the same reasons that protocol failure is possible: each random number is different. The feasibility of evading discovery by exploiting weaknesses in the EMV specification's formal analysis, design, and application was investigated. [2] Two-factor authentication is valuable since it conceals the identities of its users. No previous user-anonymity system had been built using block ciphers, hash functions, and lightweight symmetric key primitives. Two-factor authentication is designed in a way that protects the privacy of its users.

Likewise, the two-factor approach is effective in every scenario. The research is intricate, but it improves our understanding of user privacy. This aids in the development of a more secure two-factor authentication system for our users. They investigated the viability of a privacy-protecting two-factor authentication system in which smart cards are immutable and only simple symmetric cryptographic techniques are employed. It was demonstrated that this concept is applicable to any situation requiring two-factor authentication.

One- and two-factor authentication, as well as users' perceptions of automated telephone banking's security and usability, were all investigated in this study. Sixty-two knowledgeable banking customers utilized a hardware security token in a lab setting to generate a one-time passcode for two-factor authentication. We surveyed users of a current automated telephone banking service to learn what they thought of the program's usability, security, and preference for one- or two-factor authentication. There were noticeable differences between the two authentication techniques, and the results can be used to guide decisions regarding which telephone banking services to choose.

The proposed smart card offers two methods of demonstrating password knowledge. This method of authentication does not involve the usage of a verification table or any modifications to the credentials on distant servers. After the encrypted line has been established, the identities of both parties can be checked. In networks where timings are synchronized, nonce-based techniques can be used to prevent malicious reply attacks. Some have proposed using ID-based gadgets or smart cards to confirm a user's password. Users might select or alter their password in place of presenting an ID.

Authenticated Key Exchange (AKE) is a password-based system that derives its passwords from a database that, in principle, could list every possible password. Many of these procedures were time-consuming. Forward secrecy, session key loss, and guessing attacks are all accounted for in this architecture. The primary objective is AKE. With the aid of a perfect cipher model, the efficacy of the Encrypted Key-Exchange (EKE) protocol for two-flow protocol security is demonstrated. Private channels might be established, even on an unprotected public network, thanks to authenticated key exchange and mutual authentication protocols. A secure protocol must be developed in order to accomplish the aims using cryptographic keys with high entropy.

Protocols' resistance against linguistic attacks can be difficult to demonstrate. AKE employs a D-H key exchange over the course of three rounds to guarantee privacy. The "common reference string" is a publicly accessible property that is hard-coded at the initial setup of a protocol. This eliminates the need for partners in a communication to exchange public keys. A one-of-a-kind protocol, this D-H Key exchange with no authentication takes around four times as long to decipher as a regular one. This solution is simple and secure for password-only authentication since it is based on well accepted security principles.

The recommended approach to password security based on key agreement is reliable and effective. There is no way to know if the same smart card authenticated again in the same session, despite the fact that a traceability feature is added to the communication path to increase security. The first method is also effective against denial-of-service assaults. Symmetric ciphers on smart cards provide for low-cost communications, great productivity, and secure hash functions. Our technologyprevents malicious insiders, DoS attacks, and brute-force password guessing. It safeguards against password sharing, key exchange, mutual authentication, and the prevention of anonymous access.

EXISTING SYSTEM

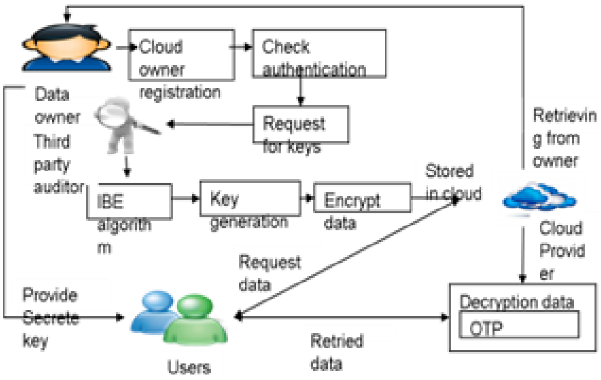
Two types of security flaws are addressed by the standard procedure for smart card authentication in a decentralized system. With a smart card and PIN, the customer's identity may be verified. Unlike with password-only authentication, no private information is stored on the server while using 2FA. In order to use the service, customers must first register. Fingerprints will be used to safeguard sensitive keys. The identity key agreement in the setup protocol is used for this purpose. An adversary can quickly obtain user data and employ it in a direct attack. An adversary can track a user's activities and login times by using the user's static user name. Protecting user privacy and improving the efficiency of password authentication systems can be accomplished with the help of a secure, untraceable smart card. An apparently risk-free method of protecting against assaults on misplaced smart cards was developed as a potential solution.

Disadvantages

- The user details have to be lost.
- The original secret code is not secured.
- The security of the data base is very difficult.
- Login the unauthorized person and modify the user details and security system.

4. PROPOSEDSYSTEM

The proposed system is aims at designing a challenging anonymous two-factor (2f) authentication scheme. The 2f authentication is the most effective password authentication system in distributed systems. A general smart card-based authentication involves a single remote server with a set of users. 2f authentication which does not store any sensitive information on the server than the common password is the key advantage which stores information to the password table on the server.



The entire system will get collapsed when the tab le gets leaked. Since no password is stored on the server it prevents security breach of millions of user's identities stored in the server. A new set of design goals is developed for fairevaluation of this type scheme. 2f authentication addresses the threats in security and opens another interesting problem that password-based authentication protocol sexist on secure smart cards and the communication with server is not required for the password change mechanism. The users may have some changes in the prominent phases like password change, registration, authentication and revocation and eviction as supplementary phases.

In the registration phase, a smart card will be issued to the user after submitting some sensitive information to the server that will be used later for the authentication purpose. This process will be repeated only when the user wishes to register again. During the smart card login process the user identity and sensitive information's will be secured.

Advantages

It is difficult to maintain database security when the original secret code is lost, personal details about users must be deleted, and so on.

Permit an unauthorized user to alter their security settings and user information once they have logged in.

Modules

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

Enrolment

The computer is receiving confidential information. Due to the shared nature of the authentication system, it is recommended that each user have their own unique password. A password is used as an instruction manual for the user authentication procedure. Server page access control configuration is required during the registration procedure. Currently, all registered users are successfully logged in..

Factors verification

Verified users are the only ones who can sign in. For starters, the user needs to get the first part ***right. The second item must be submitted before you can access your account. A minimal level of security, including resistance to impersonation attacks and offline password guesses, was achieved using semantic security or AKE security in the absence of tamper resistance. A concise overview of ROM's semantic security proof follows.***

- irst, a model was developed that returns the same answer for identical queries and a random answer for different queries.
- The meaning-based security of the targeted protocol P can be compromised by an attacker A.
- Finally, any of the pre-existing methods for solving cryptographic primitives can be used to break protocol P once it has been broken with A.
- The 3f security proof security strategy is incompatible with any authentication method that uses more than 2f. A risk-free and secure

"black box" cannot be considered secure against sophisticated attacks.

- This is done by ignoring the 2f variant of the problem. One of the five cases below involves a missing smart card. A is able to view and manage all data flows that resulted in the user's card being shown.

Change the factor

The second element can be altered, but only when the individual makes the conscious decision to do so. The new password is texted to the user's registered phone number. The manager will arbitrarily select the variable. The invader, who is likely a snoop, can launch attacks on businesses that rely on the communication route because they have complete access to it. If the conversation between the two entities is handled poorly, the secret could be revealed to A. The principle of advance secrecy and long-term lies were exposed by putting the legal parties in peril. The smart cards' data was stolen using compromised card readers and side channel attacks. Card readers can be readily hacked, allowing for the theft of sensitive user information. It is quite improbable that an attacker will be able to obtain the card with the private information if the user enters the password into malicious card readers and then acts suspiciously. The smart card is tough to hack, and the attack is inexpensive, making it challenging to devise a good strategy. Because a static user identification typically has a predetermined structure and insufficient encryption, guesswork attacks are possible. Second, it is widely disseminated and discussed in open forums and social media. The previous password must be changed and the new one communicated to the phone.

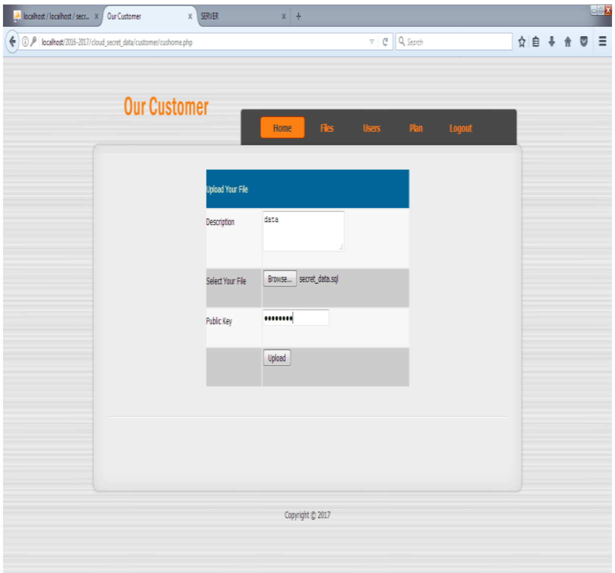
Next verification

A new password and the original first factor are required for account re-access. So, the new password is delivered to the user's smart phone, where it is stored until the next time the user logs in.

Performance evolution

- The authentication of users is protected by this mechanism.
- With today's advanced tools, it is much simpler to check the identities of unwanted guests.
- Passwords can be securely stored and updated locally using the DA2-Local-Secure technique.
- These verifiers evaluated the user's password entry during authentication to see whether they made.
- This method has the potential to simplify the verification process between users.
- No preparation was made for attacks that involve multiple, concurrent sessions, such as reflection, reply, or impersonation of people or websites.

5. RESULT



localhost / localhost / secr...
Our Customer
SERVER
localhost/2016-2017/cloud_secret_data/customer/cushome.php
Search
Our Customer
Home
Files
Users
Plan
Logout
Copyright © 2017

Upload Your File

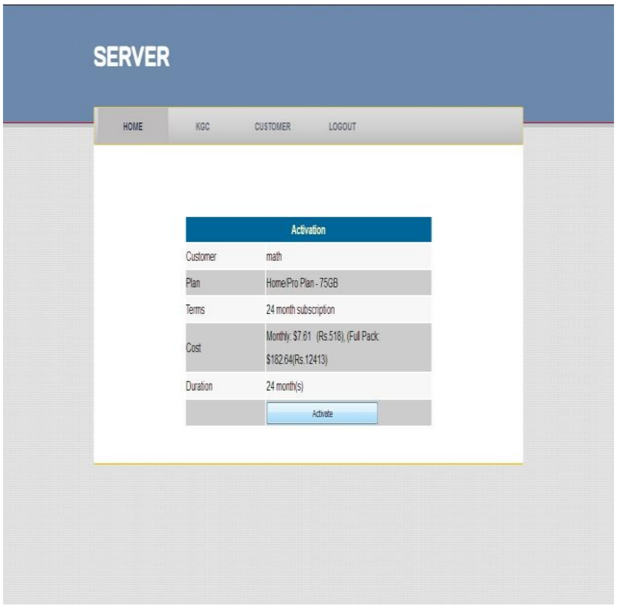
Description: data

Select Your File: Browse... secret_data.sql

Public Key: ••••••••

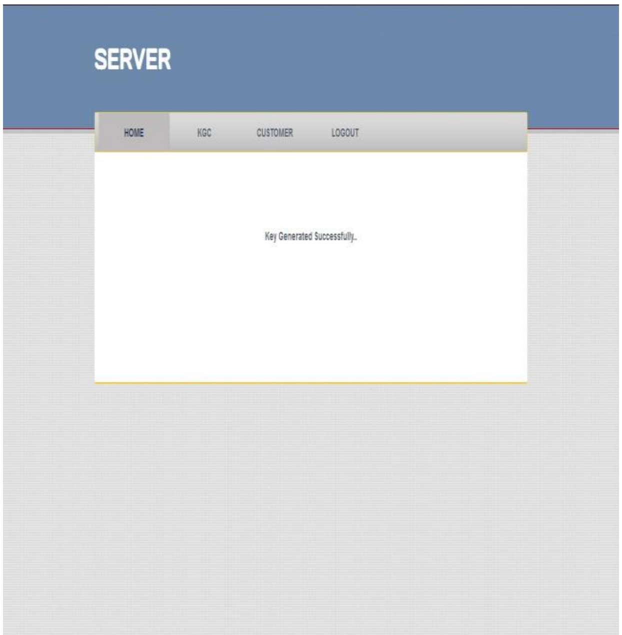
Upload

Fig:1 Plan Selection



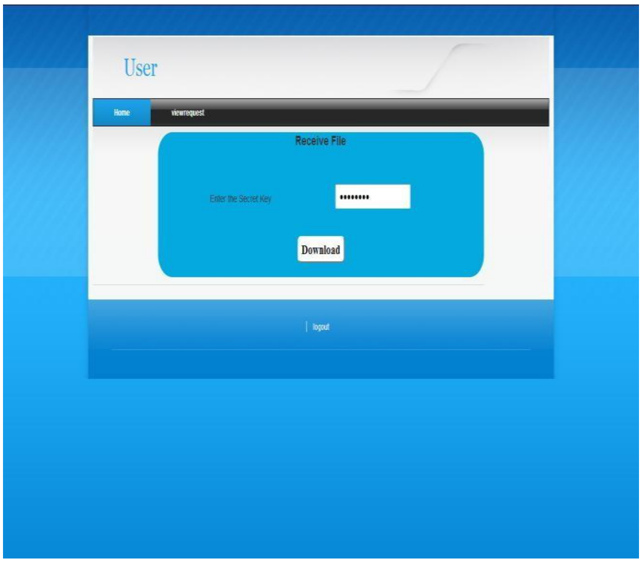
Activation	
Customer	math
Plan	Home/Pro Plan - 75GB
Terms	24 month subscription
Cost	Monthly: $7.61 (Rs.518), (Full Pack: $182.64(Rs.12413)
Duration	24 month(s)

Fig:2 Activation of Plan



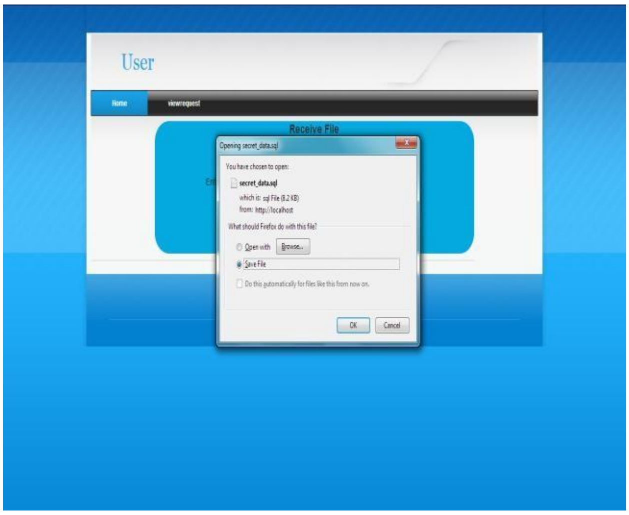
Key Generated Successfully..

Fig:3 File Uploading



Enter the Secret Key ••••••••

Fig:4 Entering the Secret Key



Opening secret_data.sql

You have chosen to open:

secret_data.sql

which is: sql File (8.2 KB)

from: http://localhost

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

Fig: 5 Downloading the File

6. CONCLUSION AND FUTURE ENHANCEMENTS

Many concerns and issues arose during the process of developing the secret two-factor procedures. The technique also reveals the interconnected nature of the variables. No approach is expected to offer "timely typo detection," a "DA10" feature, and no method gives "true local password updates" that enable "SR6" lost smart card support. Stricter evaluation criteria, protocol designers and security specialists, a feasible plan, and better choices between usefulness and usability would all be helpful for anonymous 2f systems.

REFERENCES

1. Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and YangXiang “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, StevenJ. Murdoch, Sergei Skorobogatov, Ross Anderson “Chip and Skim: cloning EMV cards with the pre-play attack ”IEEE Symposium on Security and Privacy, SanJose, CA,PP 18–21May2014.
3. Ding Wang, Ping Wang, “On the an on ymity of two factor authentication schemes for wireless sensor networks: Attacks, principle and solutions” computer networks, Elsevier, August2014.
4. 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. 5.Wen-Her Yang and Shiuh-Pyng Shieh, “Password Authentication Schemes with Smart Cards” Computers & Security Vol.18, No.8,pp.727-733,1999
6. Mihir Bellare, David Pointcheval, and Phillip Roga way “Authenticated Key Exchange Secure against Dictionary Attacks

”Springer,2000

7. JONATHANKATZ, RAFAILOSTROVSKY AND MOTIYUNG “Efficient and Secure Authenticated Key Exchange Using Weak Passwords”, ACM 2009
8. Xiangxue Li, Weidong Qiu, Dong Zheng, Kefei Chen, and Jianhua Li“ Anonymity Enhancement on Robust and Efficient Password Authenticated Key Agreement Using Smart Cards”