International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Bi-Crypto: An Efficient System with Enhanced Security

Mohemmed Yousuf R, Karthick Myilvahanan J, Sindhanaiselvan K, Mannar Mannan J

Abstract: ***A convenient two factor (2f) authentication is used in smart card password verification. Thus, the two factors are "dynamic ID-based" or "anonymous". To preserve user privacy, a tamper resistant security feature used in smart cards. Reverse engineering and power analysis techniques were used to reveal some sensitive information from the smart card memory. The smart card verification is securely implemented in memory than in the database that can be easily attacked by any person. A day to day application such as e-banking, e-health and e-governance maintains password tables on server. During login process user identity is transmitted as clear over public networks. Various non-tamper resistant schemes on OTP put forward but claim to be ambitious in design process. Truly a 2f scheme can make sure that the user whoever possess a valid OTP and password can be authorized by the server.***

Index Terms: 2f authentication, EMV, AKE, DA2 local secure.

I. INTRODUCTION

Cloud computing is a dynamically scalable infrastructure of a public or a private network for applications involving file and data storage. With emergence of this technology App-hosting, data storage, cost computation and content delivery got reduced significantly. Forrester [1] expresses cloud computing as a massively scalable computing infrastructure capable enough of provisioning resources to end users based on subscriptions. An efficient computing infrastructure is created by storage consolidation, bandwidth and data processing.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

Mr. Mohemmed Yousuf R, Assistant professor, Department of computer science and engineering at MVJ College of engineering, Bangalore, India.

Mr. Karthick Myilvahanan J, Assistant professor, Department of computer science and engineering at MVJ college of engineering, Bangalore, India.

K. Sindhanaiselvan, Bachelor of Technology in Information Technology, Master of Engineering Degree in Computer Science from the Anna University, Chennai, India.

Dr. Mannar Mannan J, Associate Professor, Department of information science and engineering, MVJ College of Engineering, Bangalore, India.

I. RELATED WORKS

A two-factor revocability mechanism is designed to handle security in cloud storage system. The encrypted data is sent to the receiver from the sender via cloud storage server. The identity of the receiver must be known by sender other information's were irrelevant. In order to decrypt a message, sender and receiver must process two things. The first thing is the key contained in the storage.

A device with unique personal security connected to the computer. The cipher text can't be decrypted without either of the pieces. The most important task is the revocation of security, if the device is lost or stolen. To make the cipher text un decryptable, cloud server uses algorithms from the security device. The process is made clear to the sender. The cipher text cannot be decrypted by the cloud server at any time. The system not only seems to be efficient but also practical. The receiver should possess security device, a secret key and knowledge about the encrypted data to gain access data in the novel 2f data security mechanism for cloud storage system. Not only the confidentiality of the data is enhanced, when the device is revoked corresponding cipher text will be auto updated by cloud server without any notice to the data owner. [1] A widespread implementation flaw and more difficult EMV protocol flaw is discovered by the author. Counters, home grown algorithms and timestamps were used by EMV manufacturers to generate nonce is the main flaw. A very type of fraud "pre-play" attack on cloned cards that is supposed to prevent is exposed. A survey methodology on how to detect vulnerability charts the evidence, scope and weakness from ATM and terminal equipment's the proof of concept of attacks. Flaws were found from widely used ATM from largest manufacturers. The banks refused to refund the amount to the customers by stating that the EMV cards cannot be cloned and the customer have mistaken. The other problem exposed were protocol failure, uniqueness of random number generation attacker can replace the authentication code from card. The exploration of design and implementation the shortcomings of the EMV specification, formal analysis, design and implementations were explored from the flaws to evade detection. [2] One of the important properties in two-factor authentication is to preserve the privacy of the users known as anonymity. None had succeeded so far in designing a user anonymity scheme by using block ciphers and hash functions in light weight symmetric key primitives. A two-factor authentication scheme intrinsically supports user anonymity.

For universal environments also two-factor scheme works remarkably. The work lead to inherent complexity and provides a better understanding of user privacy which establishes groundwork for more efficient privacy preserving two-factor authentication scheme. In this work, they have focused on whether it is possible to construct a privacy preserving two-factor authentication system under tamper resistance assumption of smart cards only by using light weight symmetric cryptographic techniques. This principle can be applicable in two-factor authentication schemes for universal environment is shown. [3] An experiment on automated telephone banking was investigated with perceptions from user on one-factor and two-factor with security and usability. Under controlled environment of 62 banking customers knowledge along in financial industries used single one factor authentication and a two-factor approach by using a hardware security token generates a onetime passcode. The user attitudes were explored on one-factor and two-factor authentication with security and usability on already established automated telephone banking service. Between two authentications approaches some interesting differences together with participants were expressed and decisions can be taken on telephony context specifically telephone banking service with two-factor authentication involving physical tokens. [4] A smart card with two password authentication schemes was proposed. In this scheme, password changes no need to be updated on remote servers and verification table is not required to authenticate users. Once the secure channel is setup, both communicating parties can authenticate themselves. Networks with a sync clocks, malicious reply attacks can be prevented using nonce based mechanisms. ID-based schemes and smart cards were the two practical password authentication schemes were proposed. Users were freely allowed to choose or change their password unlike in other ID-based authentication schemes. [5] Authenticated Key Exchange (AKE) a Password-based protocols uses passwords retrieved from a space that might well enumerate, all possible passwords. Several such protocols had suggested a lagging. A model has been designed to address this problem to deal with session key loss, forward secrecy and guessing attacks. AKE has been taken as the basic goal. The correctness of the Encrypted Key-Exchange (EKE) protocol using an ideal cipher model of two flow protocol security is proved. [6] Secure channels were enabled by Mutual authentication and authenticated key exchange techniques in an unsecured public network. To achieve the goals with high entropy cryptographic keys a secured protocol to be designed. A difficult problem is that one must be clear that the protocols are not prone to dictionary attacks. A 3-round protocol AKE provides proof of security by using a decisional D-H key exchange. “common reference string”, a public parameter is hard coded during protocol implementation which does not need to pre-share a public key between communicating parties. A remarkably efficient protocol, approximately 4 times greater computation than a classical D-H Key exchange which provides no authentication. This is the practical and provably secure protocol for password-only authentication using standard cryptographic assumptions. [7] An efficient and robust password authentication key agreement scheme is presented. A traceability property is addressed to strengthen the security of the communication channel and cannot say whether the same smart card authenticated twice in the same session. The original scheme prevents denial of service attacks also. Low communication costs, efficiency, effective and secure cryptographic hash functions is inherently viable on smart cards environment with symmetric cipher. Our solution preserves key agreement, mutual authentication password change, prevents anonymous users but also prevents insider attacks, Dos attacks and Password guessing attack. [8]

II. EXISTING SYSTEM

The current system focuses on two specific security threats on authentication on distributed system smart cards. The identity of the client is verified by the password-based authentication on smart cards. 2f authentication which does not store any sensitive information on the server than the common password only scheme is the key advantage. The users have to first register the details into the server. By using biometric finger print, secret key security will be provided. Authentication is provided with Authentication key agreement with establishment protocol. An attacker may easily recover the user information and makes active attacks. Static user identity is exploited by an attacker to facilitate access to user’s login history and current location for tracing. A non-tamper resistance secure smart cards used to preserve user anonymity to improve resistance to attacks and performance by password authentication protocols. An enhanced scheme was developed to evade the weaknesses and claimed to be secure against attacks on lost smart cards.

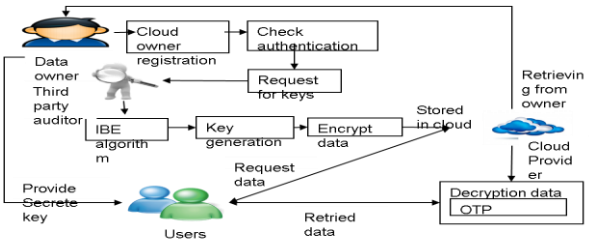
A. Disadvantages

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

III. PROPOSED SYSTEM

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 table 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 fair evaluation of this type scheme. 2f authentication addresses the threats in security and opens another interesting problem that password-based authentication protocols exist 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.

A. Advantages

- ✓ Server maintains a sensitive password table.
- ✓ Password authenticated key exchange process for securing the secret key value.
- ✓ Detect the malicious card reader problem.

B. *Modules*

i. Enrolment
ii. Factors verification
iii. Change the factor
iv. Next verification
v. Performance evolution

C. *Enrolment*

Thus, the phase can be registering the user along with sensitive information to the server. More users are accessing the same login phase so create the password on unique for each member. Thus, the password is using to identify the user certification process. The registration process has to be allocating the access control of the server page. All the registered users have been login to the page.

D. Factors verification

Authenticated person is allowed to login to the system. The user must be entering the first factor correctly. And enter the second factor then login to the account. A basic level of security such as impersonation attack resistance and offline password guessing attacks were achieved under semantic security or AKE security under non-tamper resistance been breached and lost. Proof of semantic security in ROM is a general rationale is:

(1) A model which outputs same value for identical query and a random value for unique queries were modelled.

(2) Target protocol P's semantic security can be broken by an attacker A.

(3) A is exploited to build cryptographic algorithms such that protocol P is broken by A then any of the algorithms solves the cryptographic primitives.

The security model for 3f security proof is only suitable for 2f authentication. sophisticated attacks will never be deemed as a secure "black box" which is free from threats. To accomplish this task 2f version is left unanalysed. Smart card lose case is one of the second five cases. A is equipped with ability and controls the communication channel that has breached the user's card.

E. Change the factor

First the user should login to their account and then permitted to modify the second factor. The updated password is communicated to the user via registered mobile number. The admin generates the factor in a random manner. The intruder who is assumed to be the eavesdropper who is having full control over the communication channel may perform the active attacks between communicating entities. The secret may be leaked to A by improper handling of messages exchanged between communicating entities. The legitimate parties were corrupted to capture the notion of forward secrecy and to learn long term secrets. To extract the information stored in the smart cards, malicious card readers and side channel attacks were used. Malicious card readers easily intercept the user inputted data. The card which contains the secret information is unlikely extracted by the attacker when the user inputting the password through malicious card readers by side channel attacks and perform abnormal operations. Since the smart card is highly tamper resistant it is difficult to design an ideal scheme and the attack is cost effective. Firstly, static user's identity generally has a predefined structure and little cryptographic strength very vulnerable to guessing attacks. Secondly, it can be easily reaped from open sources and public forums. The old password has to be modified and transmitted to a user smart phone.

F. Next verification

The user login in to the account second time has to use their first factor and the modified password as the second factor. Thus, the modified password must be referred from the user smart phone and that could be used for the subsequent login process.

G. Performance evolution

The user account login process is secured by this method. Compared to the previous technology's security is improved to prevent the unauthorized entity authentication. A password table which stores user's password related information on a table which is stored on the server; scheme is used by the DA2- Local-Secure for storing and updating the password locally. Those verifiers were used for verifying the user inputted password during typological errors happened accidentally during login. A mutual authentication is supported by this scheme. The possibility of parallel session attack, reflection attack, replay attack and impersonation attack to a user or server were excluded.

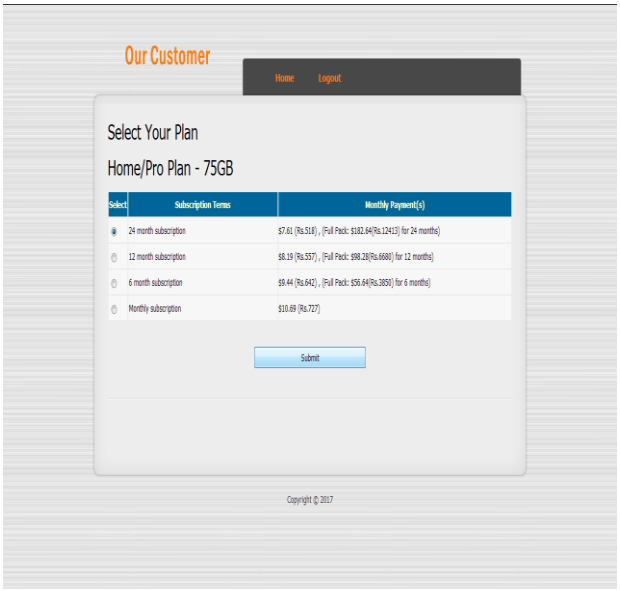


Fig: 1 Plan Selection

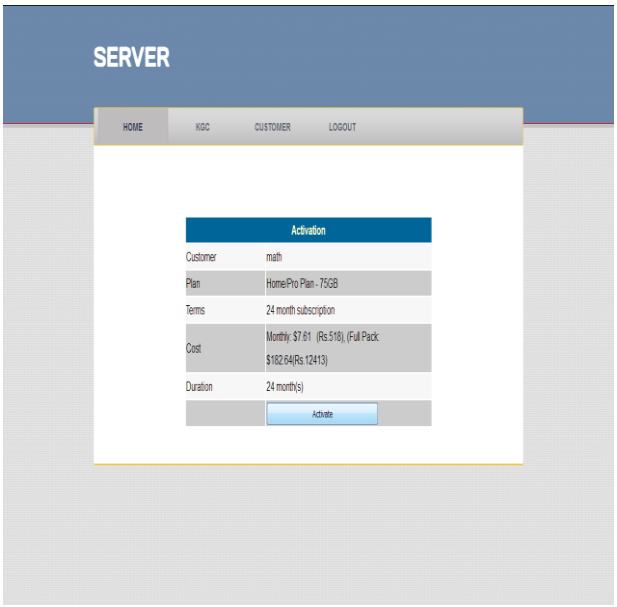


Fig: 2 Activation of Plan

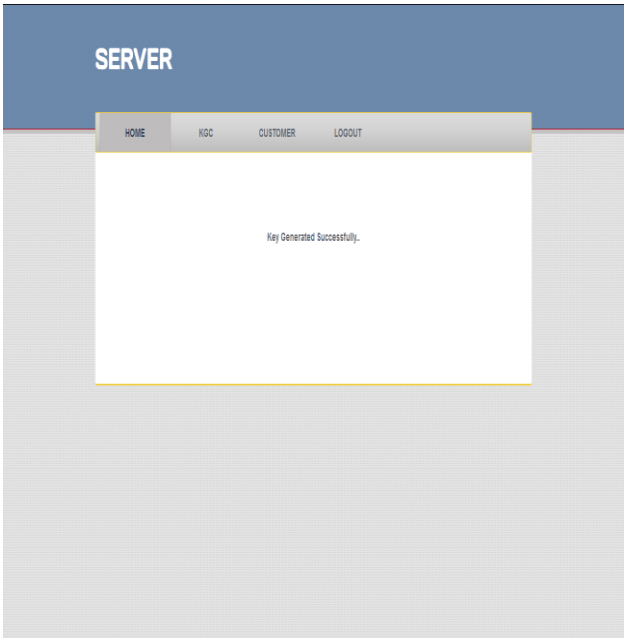


Fig: 3 Key Generation

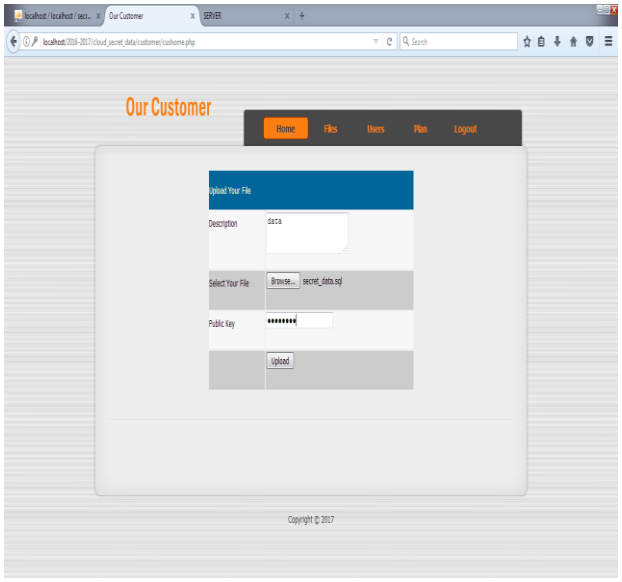


Fig: 4 File Uploading

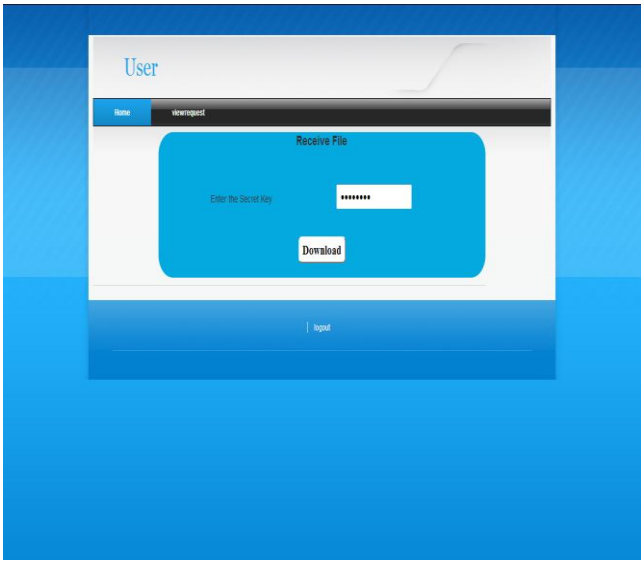


Fig: 5 Entering the Secret Key

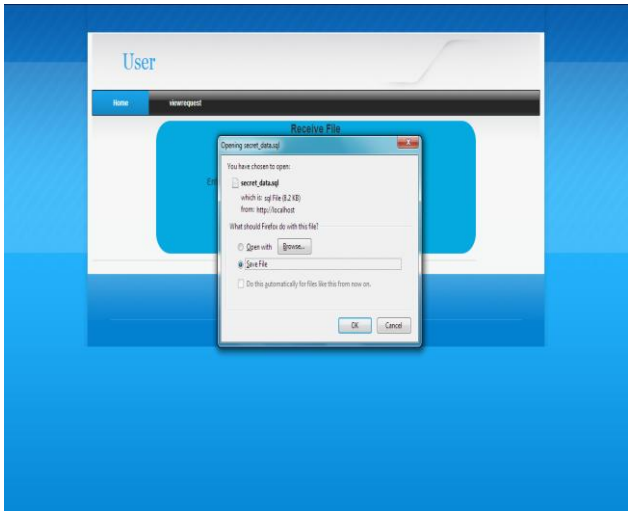


Fig: 6 Downloading the File

IV. CONCLUSION AND FUTURE ENHANCEMENTS

The anonymous two-factor schemes; several difficulties and challenges were uncovered while designing this scheme and reveals the relationships among the criteria. Most essentially, no scheme supports password changes locally that achieves lost smart card assistance “SR6” that unlikely provide “timely typo detection”, a property of “DA10. For anonymous 2f schemes, a better evaluation metric with appropriate protocol designers and security engineers with a with a practical scheme and better usability tradeoffs.

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. 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”,compute rs & security , PP 2 0 8 -2 2 0,2011
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 Rogaway “Authenticated Key Exchange Secure against Dictionary Attacks”Springer,2000
7. JONATHAN KATZ,RAFAIL OSTROVSKY AND MOTI YUNG “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”1

AUTHORS PROFILE

Mr. Mohemmed Yousuf R, received the Bachelor of Engineering Degree in Computer Science from Anna University, Chennai in 2010 and his Master of Engineering Degree in Computer Science from the Anna University, Chennai in 2013. He is working as an Assistant professor in the Department of computer science and engineering at MVJ College of engineering, Bangalore. He is a member of MIAENGG and CSTA. His current area of research interest is Cryptography and Network Security, Data Analytics in security and having 5 years of teaching experience in engineering colleges and Industry.

Mr. Karthick Myilvahanan J, completed his B.Tech (Information Technology) in 2006 from Anna University, Chennai,. M.Tech. (Information Technology) in 2010 from Anna University, Coimbatore. He is working as an Assistant professor in the Department of computer science and engineering at MVJ college of engineering, Bangalore. He is a member of ISTE. His research areas include Cryptography and Network Security, Data Analytics in security and having 12 years of teaching experience in engineering colleges and Industry.

K.Sindhanaiselvan, received the Bachelor of Technology in Information Technology from Anna University, Chennai in 2005 and his Master of Engineering Degree in Computer Science from the Anna University, Chennai in 2007and his Doctor of Philosophy in Information and Communication Engineering from the Anna University, Chennai. His current area of research interest is Energy Mobile Adhoc networks, Wireless Sensor Networks and Software Defined Networks

Dr. Mannar Mannan J., working as a associate professor, department of information science and engineering, MVJ College of Engineering, Bangalore. He completed his Ph.D., in Information and Communication Engineering, Anna University, Chennai. He having 6 years of teaching experience from various reputed engineering colleges from Tamil Nadu and 8 years from Anna university Regional Campus. His research interest is Knowledge engineering using ontology,information retrieval, Sensor Networks.

.