

BUILDING FURTHERMORE, EXAMINING A SECRET KEY STORE THAT IMPECCABLY COVERS UP PASSWORDS FROM ITSELF

E. Saravanan¹, Mr. S. Arunraj², Ms. Sarika Jain³, Dr. S. Geetha⁴

¹M. Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

^{2,3}Center of Excellence in Digital Forensics, Chennai 600 089, Tamilnadu, India

⁴Professor and Head, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

ABSTRACT

We acquaint a novel methodology with secret word the board, called SPHINX, which stays secure in any event, when the secret key chief itself has been undermined. In SPHINX, the data put away on the gadget is hypothetically free of the client's ace secret key. Besides, an assailant with full control of the gadget, even at the time the client connects with it, adapts nothing about the ace secret key – the secret key isn't gone into the gadget in plaintext structure or in whatever other way that may spill data on it. In contrast to existing administrators, SPHINX delivers carefully high-entropy passwords and makes it necessary for the clients to enlist these passwords with the web administrations, which routs web-based speculating assaults and disconnected word reference assault upon administration bargain. We present the plan, execution and execution assessment of SPHINX, offering model program modules, cell phone applications and straightforward gadget customer correspondence. We further give a relative explanatory assessment of SPHINX with other secret phrase administrators dependent on a conventional structure comprising of security, ease of use, and deployability measurements.

1. INTRODUCTION

A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions and is available in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in GSM mobile phones, and USB-based tokens. This paper initiates the study of two specific security threats on smart-card-based password authentication in distributed systems. Smart-card-based password authentication is one of the most commonly used security mechanisms to determine the identity of a remote client. The authentication is usually integrated with a key establishment protocol and yields smart-card-based password-authenticated key agreement. The security analysis made indicates that the improved scheme remains secure under offline-dictionary attack in the smart-card-loss case.

2. LITERATURE SURVEY

R. Deepa et.al, this paper outlines and discusses about the smart card-based password authentication scheme. Smart cards are the commonly used security mechanism used for several application especially security related ones. This paper addresses the two recently proposed protocols: i) attacker with pre-computed data ii) attacker with different data. Therefore, we propose an improved scheme to overcome the weakness and to improve the benefits of our new scheme. In addition, our improved scheme is secure under both online and offline dictionary attack.

Ding Wang et.al, as the most prevailing two-factor authentication mechanism, smart card-based password authentication has been a subject of intensive research in the past decade and hundreds of this type of schemes have been proposed. However, most of them were found severely flawed, especially prone to the smart card security breach problem, shortly after they were first put forward, no matter the security is heuristically analyzed or formally proved. In SEC'12, Wang pointed out that, the main cause of this issue is attributed to the lack of an appropriate security model to fully identify the practical threats. To address the issue, Wang presented three kinds of security models, namely Type I, II and III, and further proposed four concrete schemes, only two of which, i.e., PSCAV and PSCAb, are claimed to be secure under the Type III model, i.e., the harshest security model. However, in this paper, we demonstrate that PSCAV still cannot achieve the claimed security goals and is vulnerable to an offline password guessing attack and other attacks in the Type III security mode, while PSCAb has several practical pitfalls. As our main contribution, a robust scheme is presented to cope with the aforementioned defects and it is proven to be secure in the random oracle model. Moreover, the analysis demonstrates that our scheme meets all the proposed criteria and

eliminates several hard security threats that are difficult to be tackled at the same time in previous scholarship, which highly indicates the settlement of an open problem raised by Madhusudhan and Mittal in 2012. Beyond our cryptanalysis of current schemes and our proposal of the new scheme, the proposed adversary model and criteria set provide a benchmark for the systematic evaluation of future two-factor authentication proposals.

Yu Zhong Yunbin Deng et.al, in this paper we investigate the problem of user authentication using keystroke biometrics. A new distance metric that is effective in dealing with the challenges intrinsic to keystroke dynamics data, i.e., scale variations, feature interactions and redundancies, and outliers is proposed. Our keystroke biometrics algorithms based on this new distance metric are evaluated on the CMU keystroke dynamics benchmark dataset and are shown to be superior to algorithms using traditional distance metrics.

Sung-Woon Lee et.al, in 2000, sun proposed an efficient remote user authentication scheme using smart cards. Later, Chien et al. pointed out that Sun's scheme does not provide the mutual authentication between the user and the server and allow users to freely choose password themselves. Chien et al. further proposed a new efficient and practical solution to solve the problems. However, Hsu showed that Chien et al.'s scheme is vulnerable to the parallel session attack. This paper proposes an improved scheme to overcome the weakness while maintaining the advantages of Chien et al.'s scheme.

Xinyi Huang et.al, as part of the security within distributed systems, various services and resources need protection from unauthorized use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper investigates a systematic approach for authenticating clients by three factors, namely password, smart card, and biometrics. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. The conversion not only significantly improves the information assurance at low cost but also protects client privacy in distributed systems. In addition, our framework retains several practice-friendly properties of the underlying two-factor authentication, which we believe is of independent interest.

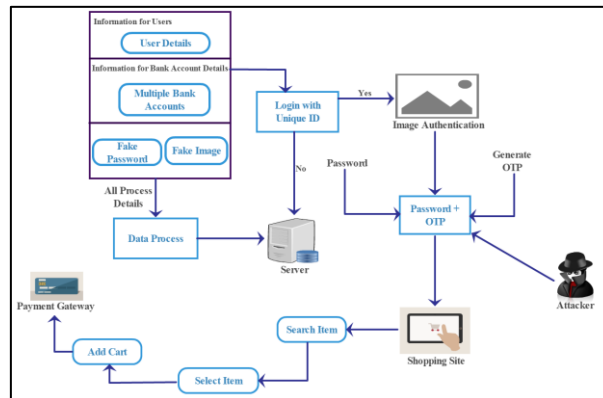
3. EXISTING SYSTEM

The central role of passwords for authentication and for gaining access to resources, from casual website visits to national security, is well known. Equally well known are the major security vulnerabilities of such mechanisms spawned by the limitations of human memory and the consequent low entropy of passwords. Candidate passwords for authenticating a user to a server can be tested by an attacker through online interactions with the server. Even more seriously, an attacker breaking into a server can mount an offline attack that uses information stored on the server to test the different passwords in the dictionary. Traditional password managers allow the user to store and retrieve passwords, denoted by *rwd*, for her multiple password-protected services by interacting with a "device" serving the role of the manager (a smartphone or an online third-party service) on the basis of a single master password, these password managers clearly alleviate the memorization burden on the user, and work well to defeat offline dictionary attacks upon web service compromise. However, they are vulnerable to leakage of *rwd*'s in the event the device is compromised or is itself malicious, denoted *pwd*. Cracking-resistant password encoding strategies have been proposed in the literature to render offline dictionary attacks ineffective. However, such a scheme seems to be vulnerable to an attack presented in a very recent work, based on differences in the distribution of the passwords.

4. PROPOSING SYSTEM

The Internet of Things (IoT) describes the network of physical objects or things that are embedded with. We introduce, build and study SPHINX, a new password manager that offers a high level of security even in case the password manager itself is compromised. SPHINX's most appealing features are: (1) the information stored in the device is information theoretically independent of the user's master password *pwd*; hence, an attacker breaking into the device learns no information on *pwd* or the user's individual passwords *rwd*'s; and (2) an attacker with full control of the device, even at the time the user interacts with it, learns nothing about *pwd*; *pwd* is never entered into the device in plaintext form or in any other way that may leak information. The above properties hold unconditionally, even against a computationally unbounded attacker. SPHINX offers the following simultaneous combination of security features: Resistance to online guessing attacks, Resistance to offline dictionary attacks under server compromise, Resistance to phishing attacks, Resistance to offline dictionary attacks under device compromise, Resistance to eavesdropping and man-in-the-middle attacks on the device-client channel without the need to establish a confidential channel. The last two security properties are unique to SPHINX, not offered by any existing password managers. We introduce SPHINX, a novel cryptographic password manager application that perfectly hides passwords from itself. We present the design, implementation and performance evaluation of a full smartphone-based SPHINX system offering a prototype browser (Chrome) plugin and a device (Android) app. As a main component of our design, we highlight and address the challenges associated in building transparent and robust bidirectional browser device communication.

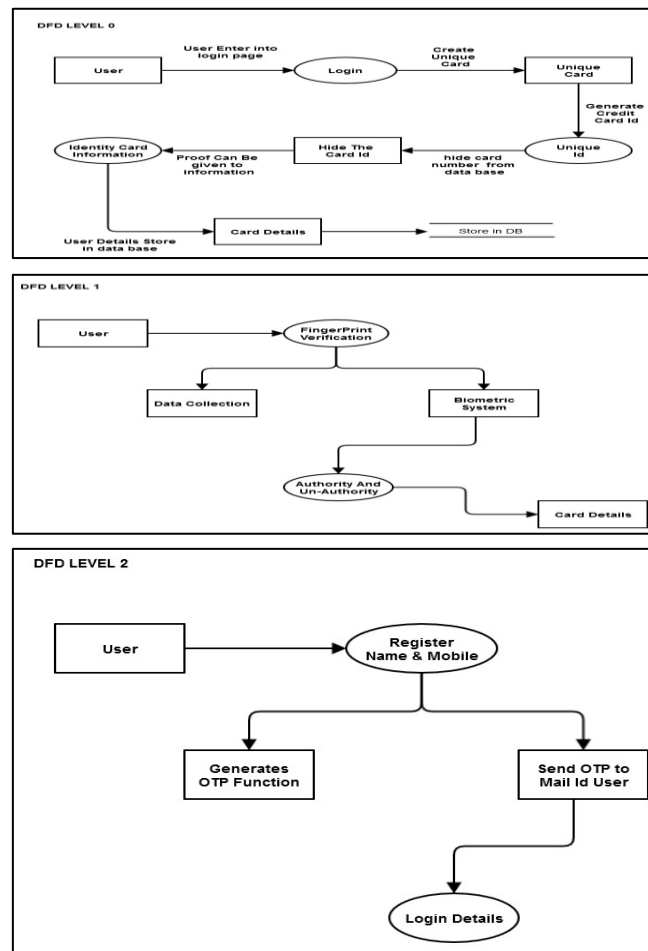
5. ARCHITECTURE DIAGRAM

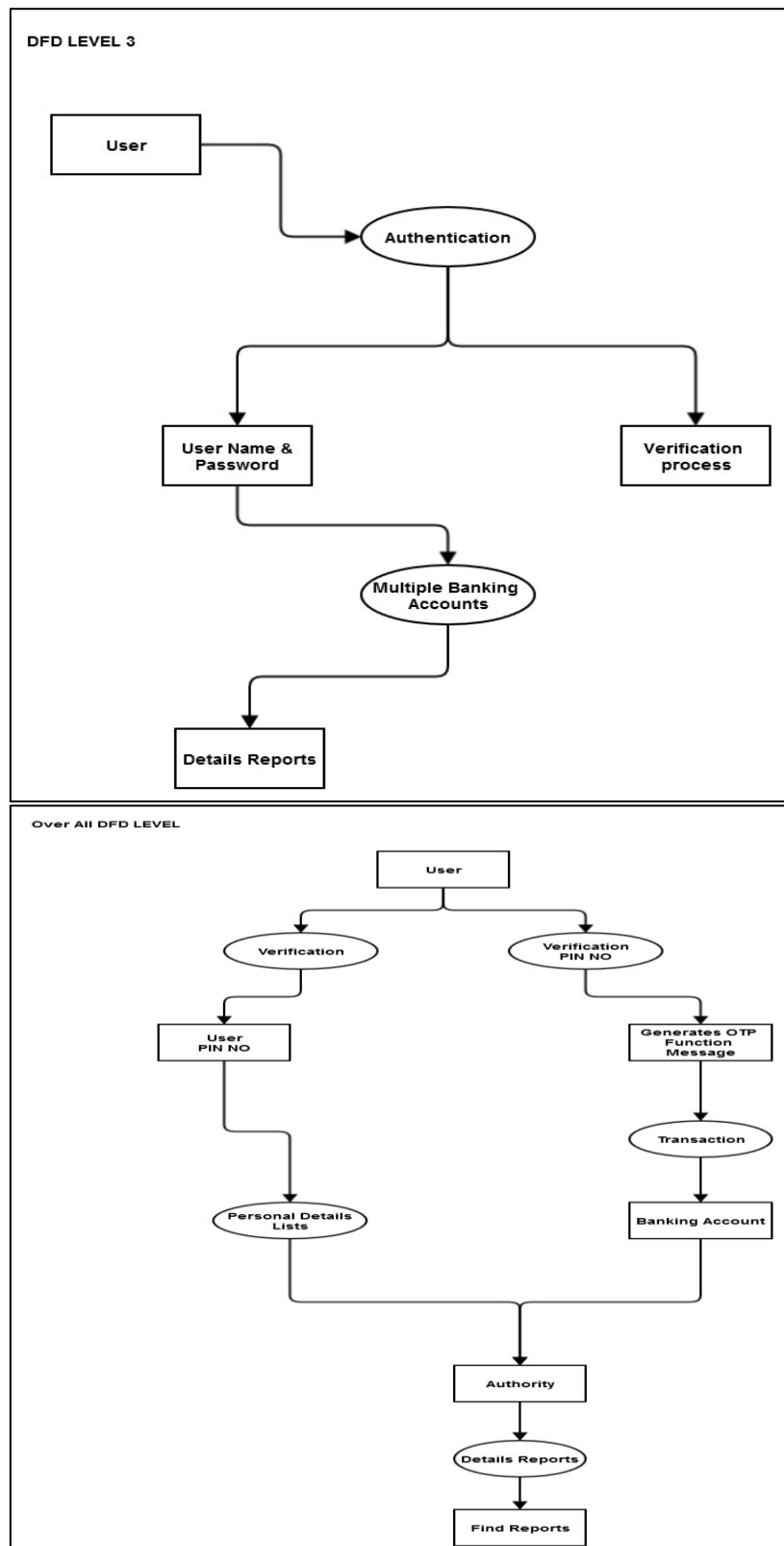


5.1 Architecture Diagram

6. DATA FLOW DIAGRAM

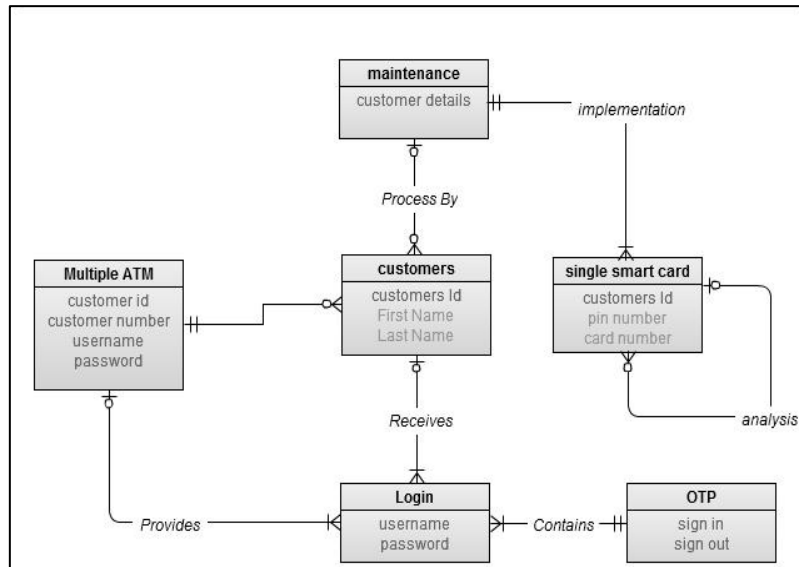
A data flow diagram (DFD) is a graphical representation of the “flow” of data through an information system. It differs from the flowchart as it shows the data flow instead of the control flow of the program. A data flow diagram can also be used for the visualization of data processing. The DFD is designed to show how a system is divided into smaller portions and to highlight the flow of data between those parts. Data Flow Diagram (DFD) is an important technique for modeling a system’s high-level detail by showing how input data is transformed to output results through a sequence of functional transformations. DFDs reveal relationships among and between the various components in a program or system. DFD consists of four major components: entities, processes, data stores and data flow.





7. ER Diagram

In software engineering, an entity-relationship model (ERM) is an abstract and conceptual representation of data. Entity-relationship modeling is a database modeling method, used to produce a type of conceptual schema or semantic data model of a system, often a relational database, and its requirements in a top-down fashion. Diagrams created by this process are called entity-relationship diagrams, ER diagrams, or ERDs. An entity-relationship (ER) diagram is a specialized graphic that illustrates the relationships between entities in a database. ER diagrams often use symbols to represent three different types of information. Boxes are commonly used to represent entities. Diamonds are normally used to represent relationships and ovals are used to represent attributes.



8. SCREEN SHOTS

Table Design

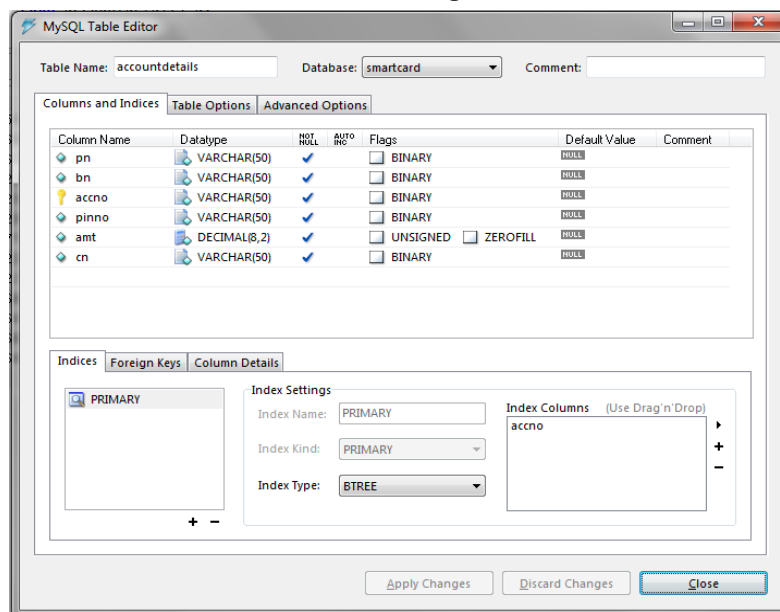


Table Name: accountdetails Database: smartcard Comment:

Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
pn	VARCHAR(50)	✓		BINARY	NULL	
bn	VARCHAR(50)	✓		BINARY	NULL	
accno	VARCHAR(50)	✓		BINARY	NULL	
pinno	VARCHAR(50)	✓		BINARY	NULL	
amt	DECIMAL(8,2)	✓		UNSIGNED ZEROFILL	NULL	
cn	VARCHAR(50)	✓		BINARY	NULL	

Indices Foreign Keys Column Details

PRIMARY

Index Settings

Index Name: PRIMARY

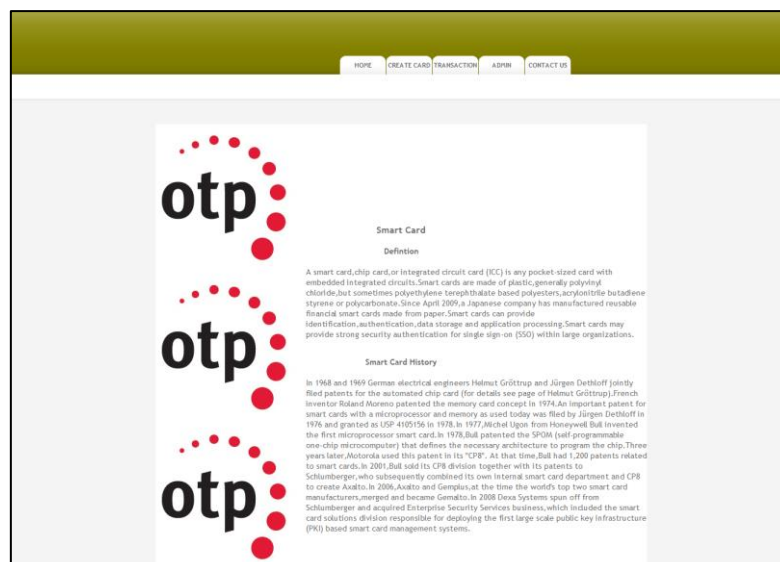
Index Kind: PRIMARY

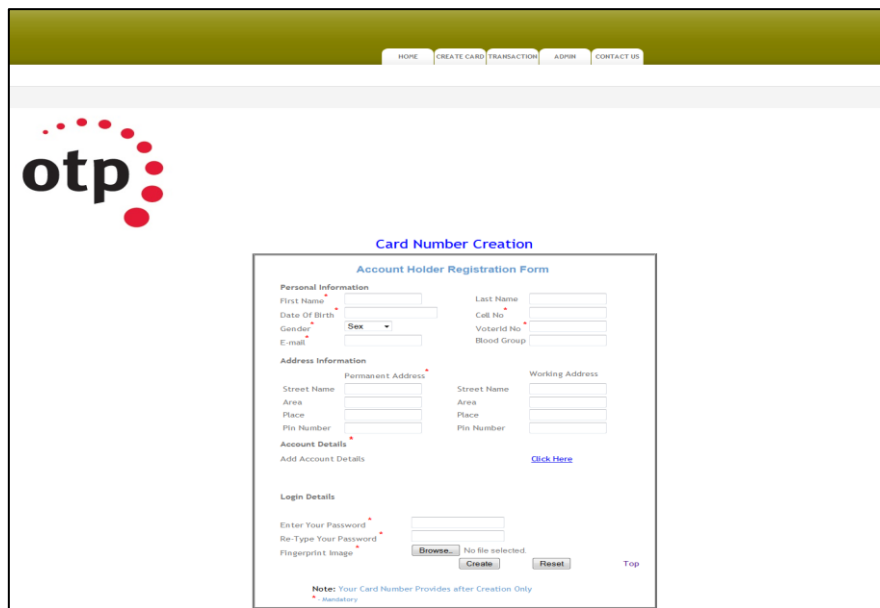
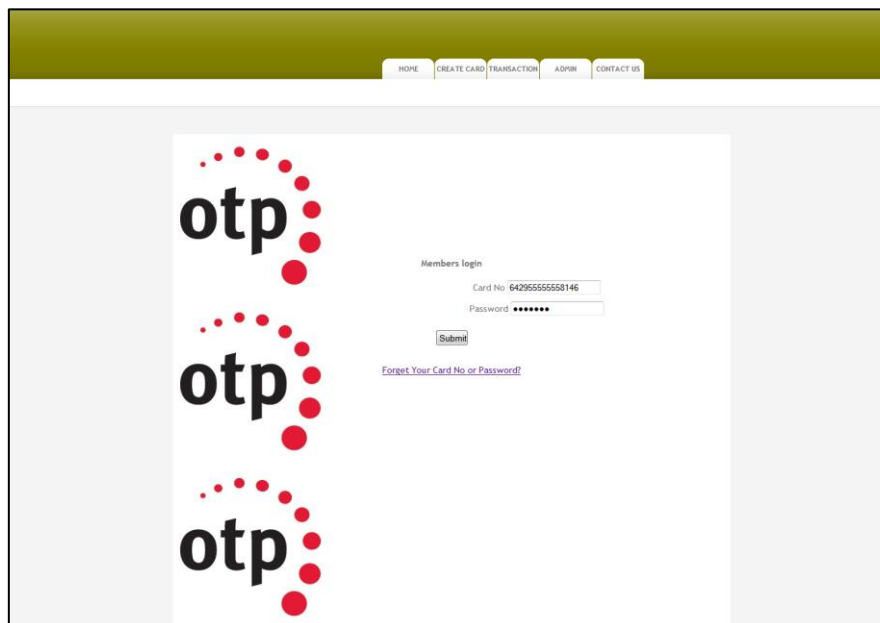
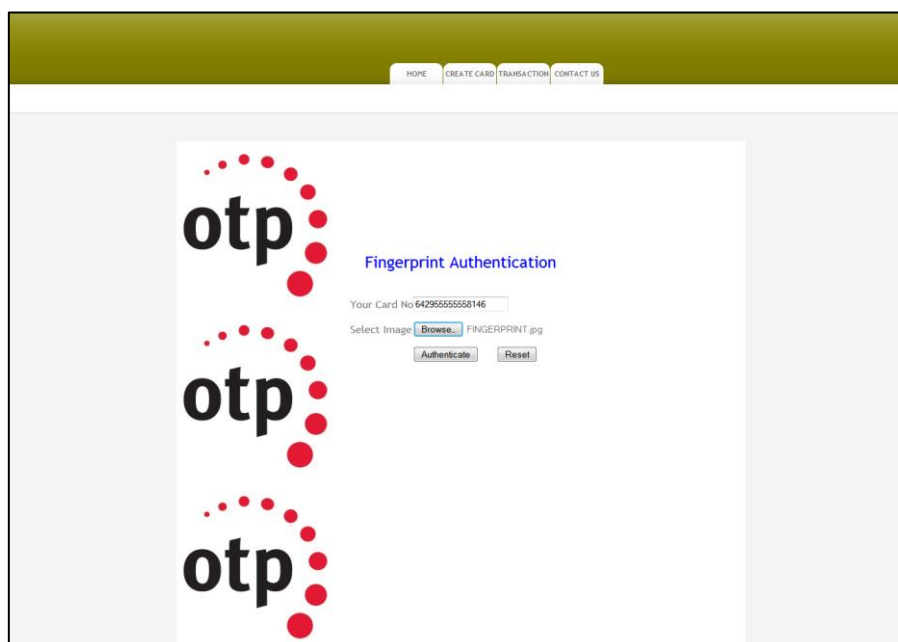
Index Type: BTREE

Index Columns (Use Drag'n'Drop)

accno

Apply Changes Discard Changes Close



[HOME](#)
[LOGOUT](#)



otp

One Time Password Authentication

(One Time Password (OTP) is Already Sent to Your Mail.....)

Your Card No

Enter Received OTP

[Authenticate](#) [Reset](#)

[HOME](#)
[MY ACCOUNT](#)
[SHOP](#)
[LOGOUT](#)

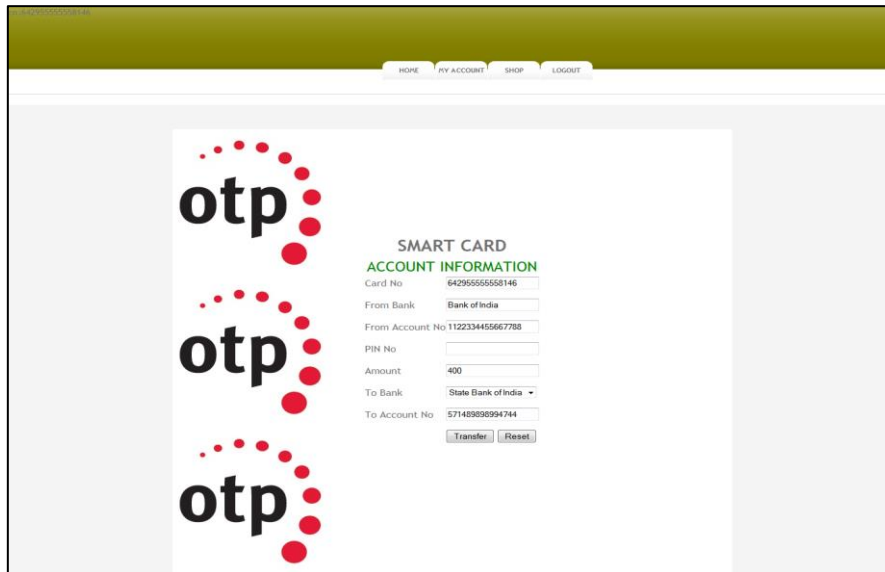
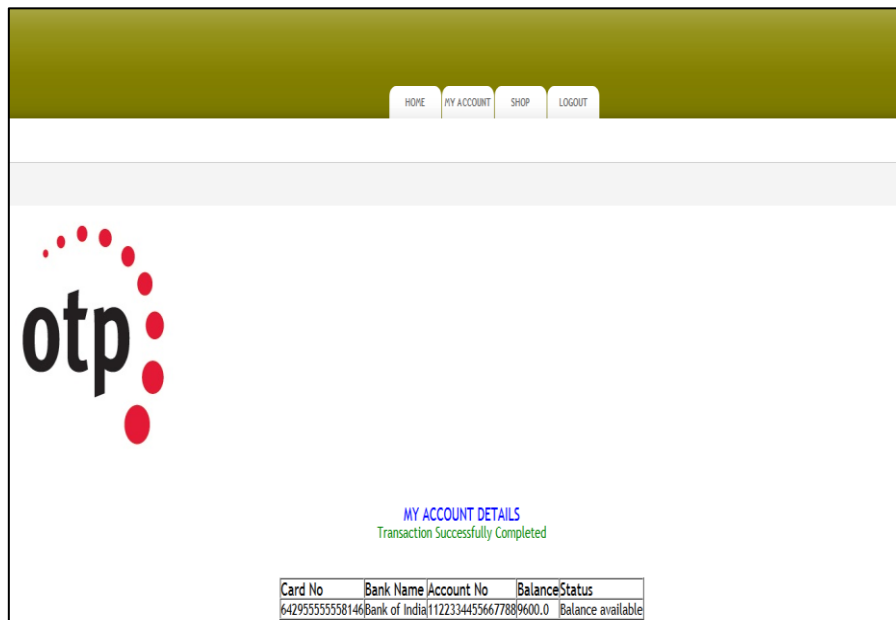


[MY ACCOUNT DETAILS](#)

Card No	Bank Name	Account No	Balance	Status
64295555558146	Bank of India	1122334455667788	10000.0	Balance available

[HOME](#)
[MY ACCOUNT](#)
[SHOP](#)
[LOGOUT](#)

ITEMS LIST					
ProductID	Name	Rate	Description	AvailableCount	Purchase
1	key board	450	sasa	190	Go to Purchase
3	web camera	250	webcam is used for video chat	300	Go to Purchase
4	wires	100	sdfsdf	230	Go to Purchase
5	mouse	250	mouse is input device	90	Go to Purchase
6	computer table	400	hardware	150	Go to Purchase
7	motherboard	500	dfsdfsdfsdfsdfsdf	100	Go to Purchase
8	choco	50	sweet choco	98	Go to Purchase
9	sample	1000	ghsdfg sdfgdfg dg	100	Go to Purchase

Card No	Bank Name	Account No	Balance	Status
64295555558146	Bank of India	1122334455667788	9600.0	Balance available

9. CONCLUSION

Passwords are an "essential malice". We endeavoured to react to the developing security and ease of use issues with passwords by proposing SPHINX, a cryptographic secret key director that can address most security and convenience issues with passwords from the customer/client side alone (i.e., straightforward to most existing web validation administrations). SPHINX is a secret word the board approach, worked on a current absent PRF (OPRF) plot that changes a human-paramount secret phrase into an arbitrary secret key with the guide of a gadget without the need to store the passwords on the gadget. SPHINX offers a few key securities ensures, to be specific, protection from: (1) internet speculating assaults, (2) disconnected word reference assaults under server bargain, (3) disconnected lexicon assaults under gadget bargain, (4) phishing assaults, and (5) spying also, man-in-the-center assaults on the gadget customer channel. SPHINX additionally gloats to give nearly the equivalent level of client experience as that of validation utilizing a simple to retain secret phrase. In contrast to other secret word supervisors, SPHINX consummately shrouds passwords and the ace secret word from itself, and in this manner stays secure under the sensible danger of the trade-off of secret key supervisors. Additionally, in contrast to other secret word chiefs, SPHINX doesn't require a classified gadget customer channel. At the equivalent time and like numerous other secret phrase administrators, SPHINX can oppose web-based speculating, disconnected lexicon under web administration bargain and phishing assaults. We structured and actualized a cell phone-based launch of SPHINX. Our execution and logical assessment of this launch shows that it is proficient, profoundly secure, likely easy to utilize, furthermore, simple to send practically speaking.

10. REFERENCES

- [1] H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," *Comput. Security*, vol. 21, no. 4, pp. 372-375, Aug. 2002.
- [2] T.F. Cheng, J.S. Lee, and C.C. Chang, "Security Enhancement of an IC-Card-Based Remote Login Mechanism," *Comput. Netw.*, vol. 51, no. 9, pp. 2280-2287, June 2007.
- [3] C.-I. Fan, Y.-C. Chan, and Z.-K. Zhang, "Robust Remote Authentication Scheme with Smart Cards," *Comput. Security*, vol. 24, no. 8, pp. 619-628, Nov. 2005.
- [4] J. Hu, D. Gingrich, and A. Sentosa, "A k-Nearest Neighbor Approach for User Authentication Through Biometric Keystroke Dynamics," in *Proc. IEEE ICC Conf.*, Beijing, China, May 2008, pp. 1556-1560.
- [5] C.L. Hsu, "Security of Chien et al.'s Remote User Authentication Scheme Using Smart Cards," *Comput. Stand. Interfaces*, vol. 26, no. 3, pp. 167-169, May 2004.
- [6] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R.H. Deng, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390-1397, Aug. 2011.
- [7] W.S. Juang, S.T. Chen, and H.T. Liaw, "Robust and Efficient Password Authenticated Key Agreement Using Smart Cards," *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2551-2556, June 2008.
- [8] W.C. Ku and S.M. Chen, "Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 204-207, Feb. 2004.
- [9] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. Adv. CRYPTO*, vol. LNCS 1666, M.J. Wiener, Ed., 1999, vol. LNCS 1666, pp. 388-397.
- [10] L. Lamport, "Password Authentication with Insecure Communication," *Commun. ACM.*, vol. 24, no. 11, pp. 770-772, Nov. 1981.
- [11] C. Lee, M. Hwang, and I. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1683-1687, Oct. 2006.
- [12] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 1, pp. 32-43, Jan. 2012.