iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com Volume 3 Issue III, March 2015
IC Value: 13.98 ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Session Key Based Password Authentication

M.Nivas[1], A.Divya[2], P.Kanimozhi[3]
[1,2,3] IFET College of Engineering, Villupuram, India

Abstract-- 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, who must hold a valid smart card and the corresponding password to carry out a successful authentication with the server. The authentication is usually integrated with a key establishment protocol and yields smart-card-based password-authenticated key agreement. Using two recently proposed protocols as case studies, we demonstrate two new types of adversaries with smart card adversaries with pre-computed data stored in the smart card adversaries with different data (with respect to different time slots) stored in the smart card. These threats, though realistic in distributed systems, have never been studied in the literature. In addition to point out the vulnerabilities, we propose the countermeasures to thwart the security threats and secure the protocols.

Index Terms—Smart Card, Server, vulnerabilities

I. INTRODUCTION

REMOTE authentication is of great importance to protect a networked server against malicious remote users in distributed systems. Since the introduction by Lamport [11] in 1981, a large number of designs of authentication have been proposed (such as those recent ones :) Most early schemes are solely based on password authentication. To strengthen security, smart-card-based password authentication has become one of the most common authentication mechanisms. A smart-card-based password authentication scheme involves a server and a user, and typically consists of three phases. The first phase is called the registration phase, where the server issues a smart card to the user. The smart card contains the personal information about the user, which will be used later for the authentication. In this phase, an initial

Password for the user is also determined (chosen by the user or by the server). Once the registration phase is completed, the user is able to access the server in the log-in phase, which can be carried out as many times as needed. A successful log-in requires the user to have the valid smart card and the correct password. In other words, the scheme provides two-factor (password and smart card) authentication. In the password-changing phase, the user can freely change his/her password and update the information in the smart card accordingly. Due to the limitation of computational power, a smart card may not be able to afford heavy computations.

Some schemes (e.g., [8]) thus employ an additional pre-computation phase to speed-up the authentication process during the log-in phase. To date, many smart-card-based password authentication schemes have been proposed, and various security goals and properties have been addressed, including (but are not limited to) low computation and communication cost, no password table, security against replay attacks, security against parallel session attacks, mutual authentication, session key agreement and security against adversaries with smart card. It is not trivial to design smart-card-based password authentication satisfying even the basic security requirements, and in fact many schemes have been found broken shortly after their proposals. As an example, an efficient mutual authentication scheme using smart cards proposed by Chien et al. in [2] is insecure against parallel session attacks due to the analysis given by Hsu [6]. An improvement of Chien et al.'s scheme, given by Lee et al. [14], can be broken by adversaries with smart card [23]. This paper shall study two new types of dictionary attacks with smart cards in distributed systems. In smartcard-based password authentication, a user is allowed to choose his/her password in the password-changing phase. It is a well-known problem that human memorable passwords only come from a small domain. This enables adversaries (with the smart card) to guess a user's password by using every ''word'' in a password dictionary, which is known as dictionary attack. Dictionary attack can be further divided into online (active) and offline (passive) dictionary attack. An online-dictionary attacker could try to log on the server by trying every possible password for a specific user. Such attacks can be prevented using lockout mechanisms to lock out the user account after a certain number of invalid login attempts. In an offline-dictionary attack, the attacker tries to uncover the user's password using the information in the smart card and the challenge response messages between the user and the server. Unlike online attacks, offline-dictionary attack cannot be easily detected due to the limitation of detection methods.

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

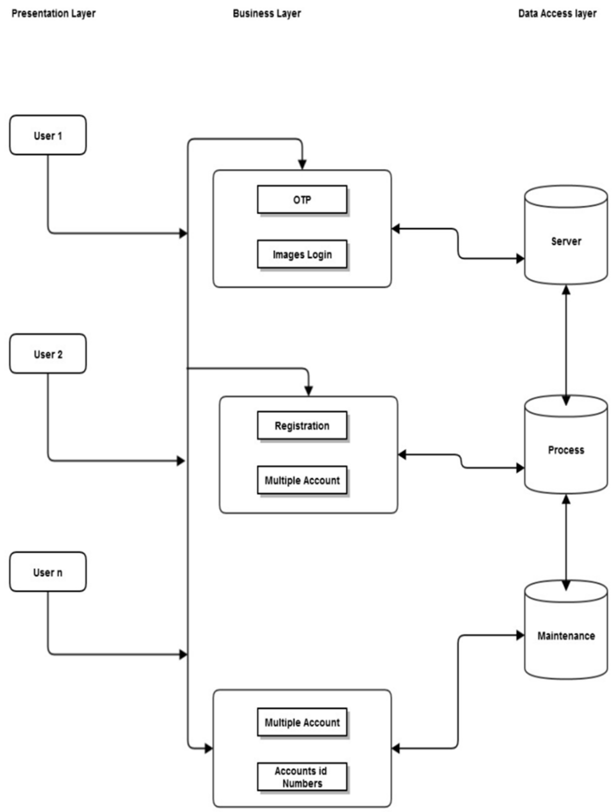


Fig 1 :- Architecture Diagram

A. Objective

Objective of this project is to avoid Use of Active Attack And Passive Attack(Online and Offline attack based)for this purpose we presents a single card number which allows to access the bank accounts. Scope of this project is to give security for transaction purpose and provide single card number to remember instead of remembering stored in smart card itself.

B. Existing/Proposed System

To date, many smart-card-based password authentication schemes have been proposed, and various security goals and properties have been addressed, including (but are not limited to) low computation and communication cost, no password table, security against replay attacks, security against parallel session attacks, mutual authentication, session key agreement and security against adversaries with smart card. It is not trivial to design smart-card-based password authentication satisfying even the basic security requirements, and in fact many schemes have been found broken shortly after their proposals.

C. Disadvantages of Existing System

1) A user is allowed to choose his/her password in the password-changing phase.

2) It is well a known problem that human memorable passwords only come from a small domain.

3) Which a known as dictionary attack. Dictionary attack can be further divided into online (active) and offline (passive) dictionary attack.

D. Proposed System

Very recently, two smart-card-based password authentication schemes were proposed. Juang, Chen, and Liaw described a robust and efficient user authentication and key agreement scheme using smart cards. Juang-Chen-Liaw's scheme can be viewed as an improvement over the one proposed, which is designed to accommodate a number of desirable features including no password table, server authentication, etc. But the major limitation of is a relatively high computation cost. This is improved with a new proposal in by exploiting the advantages of pre-computation. who shows that attackers can successfully impersonate the user with old password and old data in the smart card. Thus, a new scheme was proposed to fix that flaw, together with several other new properties such as forward secrecy and password changing without any interaction with the server. The security analysis made indicates that the improved scheme remains secure under offline-dictionary attack in the smart-card-loss case.

E. Advantages of Proposed System

1) Costly operations are completed in the offline-phase (before the authentication).
2) It is claimed in that their scheme can prevent offline dictionary.
3) Attacks even if the secret information stored in a smart card is compromised.

II. MODULE DESCRIPTION

A. Adversary Models

Intuitively, an attacker on a smart-card-based password authentication protocol should be unable to make successful log-in only with the smart card (or the password),or compromise other additional properties (key agreement).To capture these requirements, we define the potential attacker from two aspects, namely the behavior of the attacker and the information compromised by the attacker. As an interactive protocol, a smart-card-based password authentication protocol may be faced with a passive attacker and an active attacker A passive attacker can obtain messages transmitted between users and the server. This is due to the fact that communication channels are generally insecure, and the attacker can observe messages by eavesdropping. A passive attacker cannot interact with any of the parties in smart-card-based password authentication protocols In addition to message eavesdropping, an active attacker can also inject and modify messages in the communication between the user and the server. In particular, the attacker can initiate a log-in request on behalf of the user, or act as the server by sending messages to the user. An active attacker can also request any session keys adaptively (if the protocol supports key agreement).It is evident that an active attacker is more powerful than a passive attacker.

B. Session-Key-Extraction

I first show that a passive attacker with smart card can calculate the session key between the server and the user in the protocol proposed. At the end of the log-in phase the session key between the user and the server is It suffices to compute Sk and u. stored in the smart card before the log-in phase. More precisely, Vi is generated in the registration phase, and c is added to the memory of the smart card in the pre-computation phase. The purpose of pre-computation is to speed up the computation in the authentication, which should be regarded as a separate phase from the log-in phase. Thus, to reduce the computational load in log-in phase in, the smart card must complete the calculation of before the log-in phase, rather than performing the calculation at the beginning of the log-in phase. Where the computational cost in the log-in phase does not include the calculation of the attacker can obtain if he/she can extract the information in the smart card before the log-in phase. It remains to show that the adversary can obtain u as well. The sever sends to the smart card, which enables an eavesdropping (passive) adversary to obtain this completes the description of how a passive attacker with smart card can obtain and calculate the session key.

C. Security Flaws with the Session-Key

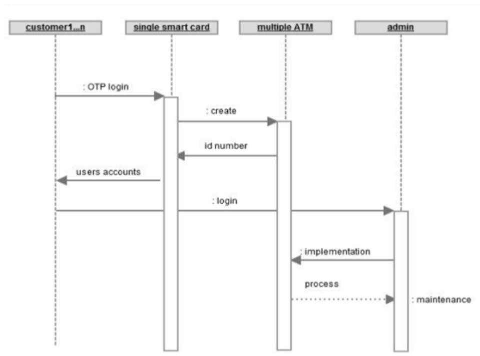
I now show that a successful attack against the session key will undermine the security of whole system from at least two aspects. First, the communication between the user and the server is no longer secure the purpose of the session is to establish a secure communication between the user and the server. The communication, thus, will not be secure if Sk is compromised. As an example, an adversary with Sk is able to decrypt any cipher texts which are generated using the encryption key Sk. Message authentication could also fail if it solely relies on Sk. Second , the adversary can freely change the user’s password. The given attack is different from the common offline dictionary attack with the smart card, as the adversary does not guess the user’s password. In other words, the adversary does not have the user’s password at the end of the attack. This, however, cannot prevent a successful login from the attacker on behalf of the user, since the adversary is able to change the password with the session key Sk. Once the log-in phase is completed, the adversary can immediately invoke the password-changing phase, namely the adversary chooses a new pair. Let the response from the server be which can be decrypted by the adversary with the session key Sk. After that, the adversary can successfully login to the server (on behalf of the user with identity) with the new password i and the new smart card.

D. Password-Changing Phase

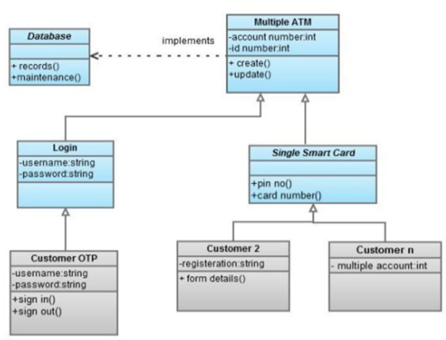
I note that such an adversary is stronger than that considered, where the adversary can obtain the information in the smart card but only once. If the adversary can capture the information in the smart card once, we believe the adversary can also do it for the second time. As an example, one can obtain the information in the smart card via an illegal card reader. This could occur more than once without the awareness of the smart card owner (e.g., the attacker could steal the smart card and send it back after extracting the data stored in the smart card). In the above attacking scenario, the other assumption is that the user will change the password at least twice. We believe this is also a reasonable assumption as changing password on a regular basis has been regarded as one of good password habits. This completes the description of the attacking scenario we are concerned about, which we believe falls into the category of passive attacker with smart card defined. It remains to show how to extract the two passwords.

III. FUNCTIONAL DIAGRAMS

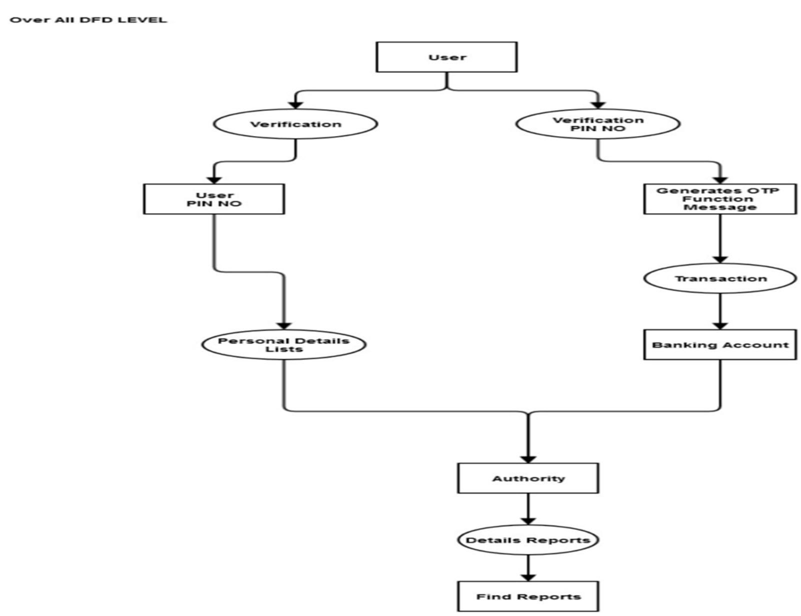
A. Sequence Diagram



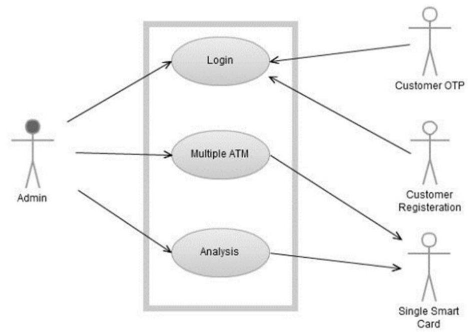
B. Class Diagram



C. Data Flow Diagram



D. Use Case Diagram



IV. CODING DESIGN

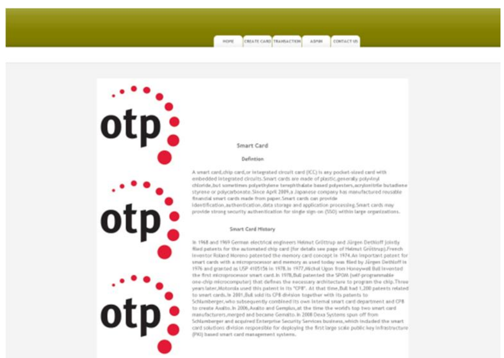
Createcard.jsp:

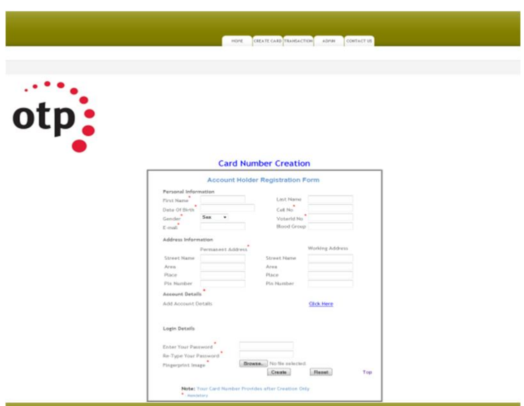
```
<%--
   Document   : Createcard
   Created on : Mar 16, 2013, 11:22:38 AM
   Author     : sluser
--%>

<%@page import="java.util.Calendar"%>
<%@page import="java.text.SimpleDateFormat"%>
<%@page import="java.text.DateFormat"%>
<%@ page import="org.apache.commons.fileupload.servlet.ServletFileUpload"%>
<%@ page import="org.apache.commons.fileupload.disk.DiskFileItemFactory"%>
<%@ page import="org.apache.commons.fileupload.*"%>
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE html>
<html>
<head>
 <script language="javascript" type="text/javascript" src="datetimepicker.js"></script>
  <link rel="stylesheet" href="http://code.jquery.com/ui/1.10.2/themes/smoothness/jquery-ui.css" />
  <script src="http://code.jquery.com/jquery-1.9.1.js"></script>
  <script src="http://code.jquery.com/ui/1.10.2/jquery-ui.js"></script>


<script>
  $(function() {
    $( "#datepicker" ).datepicker({
     changeMonth : true,
      changeYear : true,
      yearRange: '-100y:c+nn'

    });
  });
  </script>

    <script type="text/javascript">
// Popup window code
function db(ele)
{
    alert("hi");
}
```

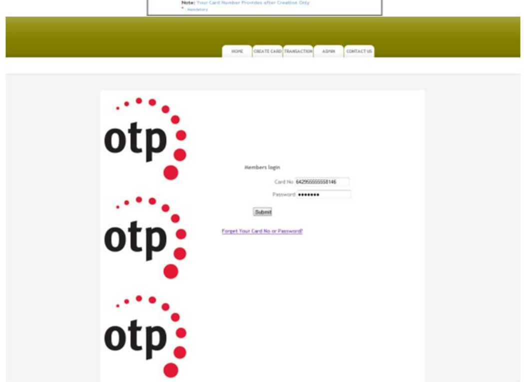
Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

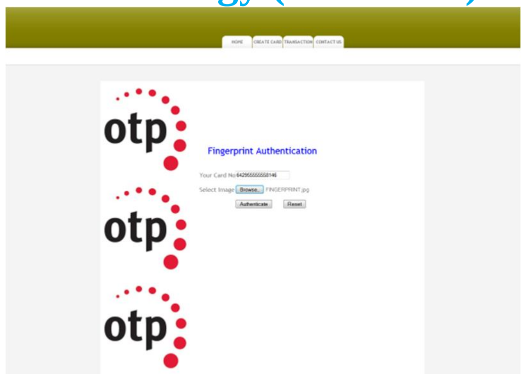
```
function newPopup(url) {
	popupWindow = window.open(

	url,'popUpWindow','height=500,width=500,left=300,top=100,resizable=yes,scrollbars=yes,toolbar=yes,menubar=no,location=no,directories=no,status=yes')
}
</script>

	<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
	<title>STCARD - Create Card</title>
	<link rel="stylesheet" type="text/css" href="style.css" />
    <%
 String Servlet_Msg = (String) session.getAttribute("msg");
	String color = (String) session.getAttribute("color");
```

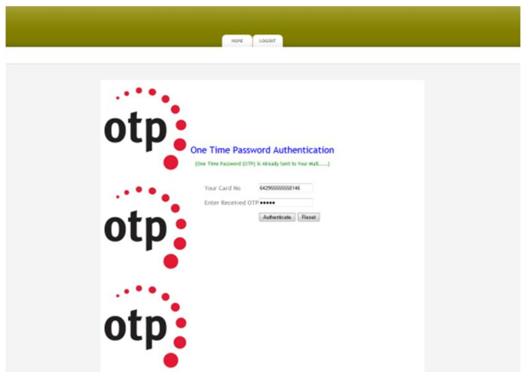
V. SCREENSHOTS



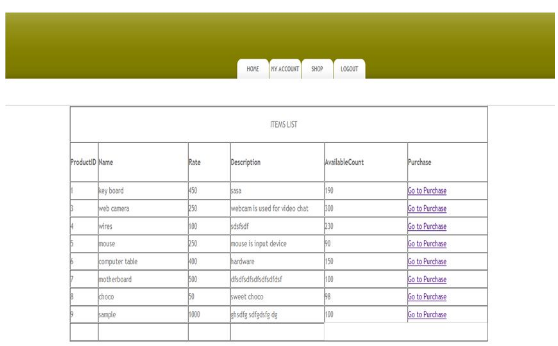





otp
otp
otp
Fingerprint Authentication
Authenticate
Reset


otp
otp
otp
One Time Password Authentication
Authenticate
Reset

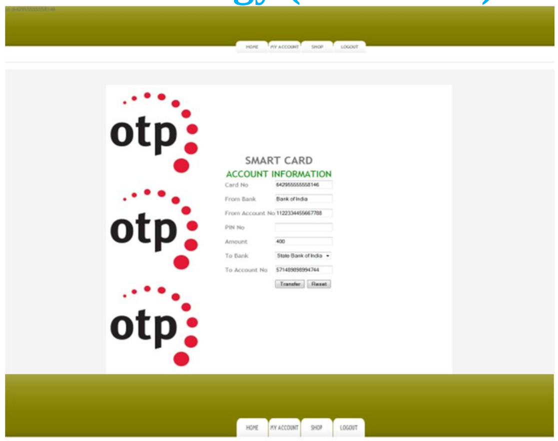

otp
MY ACCOUNT DETAILS
Card No
Bank Name
Account No
Balance
Status
6429555555558146
Bank of India
1122334455667788
10000.0
Balance available

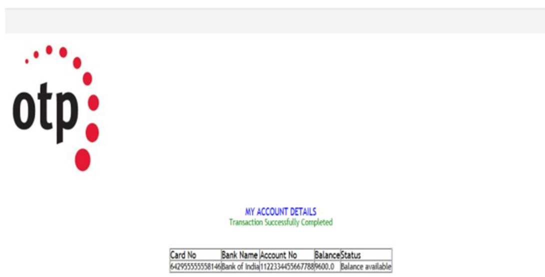

HOME
MY ACCOUNT
SHOP
LOGOUT
ITEMS LIST
ProductID
Name
Rate
Description
AvailableCount
Purchase
1
key board
450
sasa
190
Go to Purchase
3
web camera
250
webcam is used for video chat
300
Go to Purchase
4
wires
100
sdsfsdf
230
Go to Purchase
5
mouse
250
mouse is input device
90
Go to Purchase
6
computer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

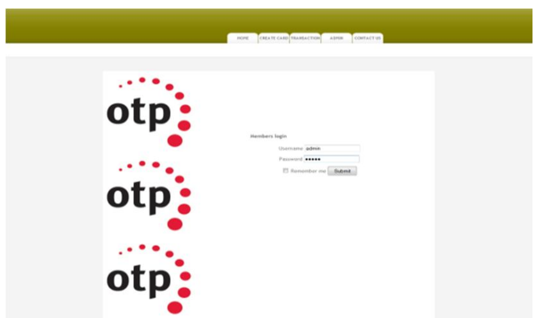
www.ijraset.com
IC Value: 13.98

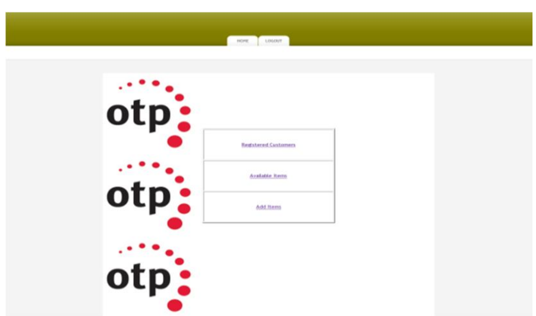
Volume 3 Issue III, March 2015
ISSN: 2321-9653

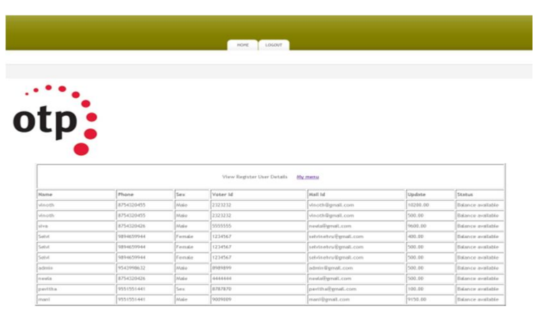
International Journal for Research in Applied Science & Engineering Technology (IJRASET)





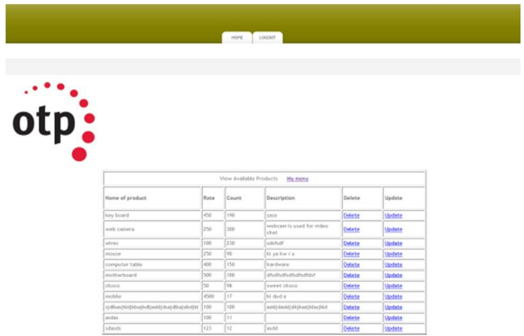


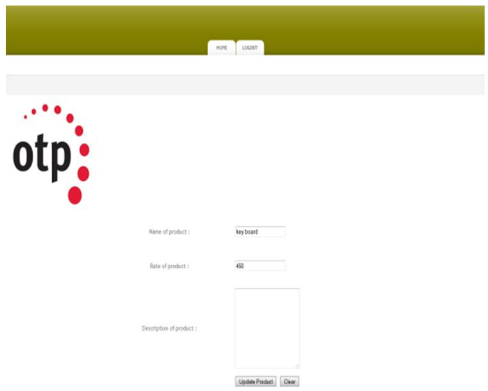


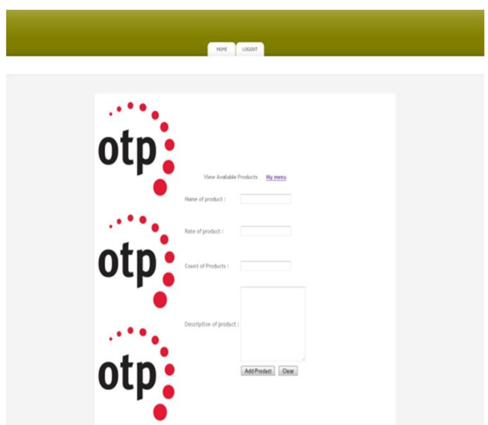


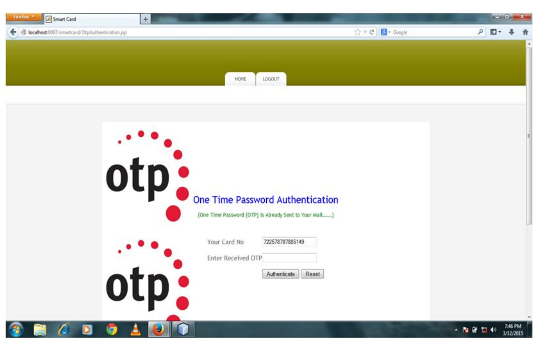
Volume 3 Issue III, March 2015
ISSN: 2321-9653

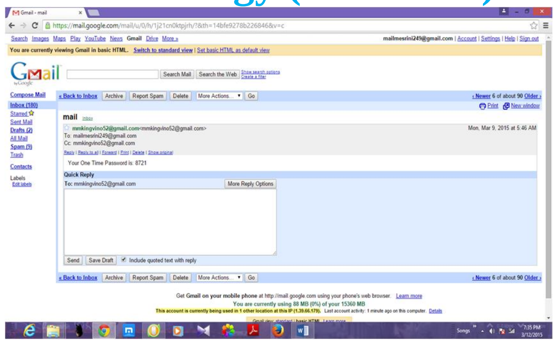
International Journal for Research in Applied Science & Engineering Technology (IJRASET)











VI. CONCLUSION

This paper revisited the security of two password-authenticated key agreement protocols using smart cards. While they were assumed to be secure, we showed that these protocols are flawed under their own assumptions respectively. In particular, we took into account some types of adversaries which were not considered in their designs, e.g., adversaries with pre computed data stored in the smart-card and adversaries with different data (with respect to different time slots) stored in the smart-card. These adversaries represent the potential threats in distributed systems and are different from the commonly known ones,which we believe deserve the attention from both the academia and the industry.We also proposed the solutions to fix the security flaws. Once again, our results highlight the importance of elaborate security models and formal security analysis on the design of password-authenticated key agreement protocols using smart cards.

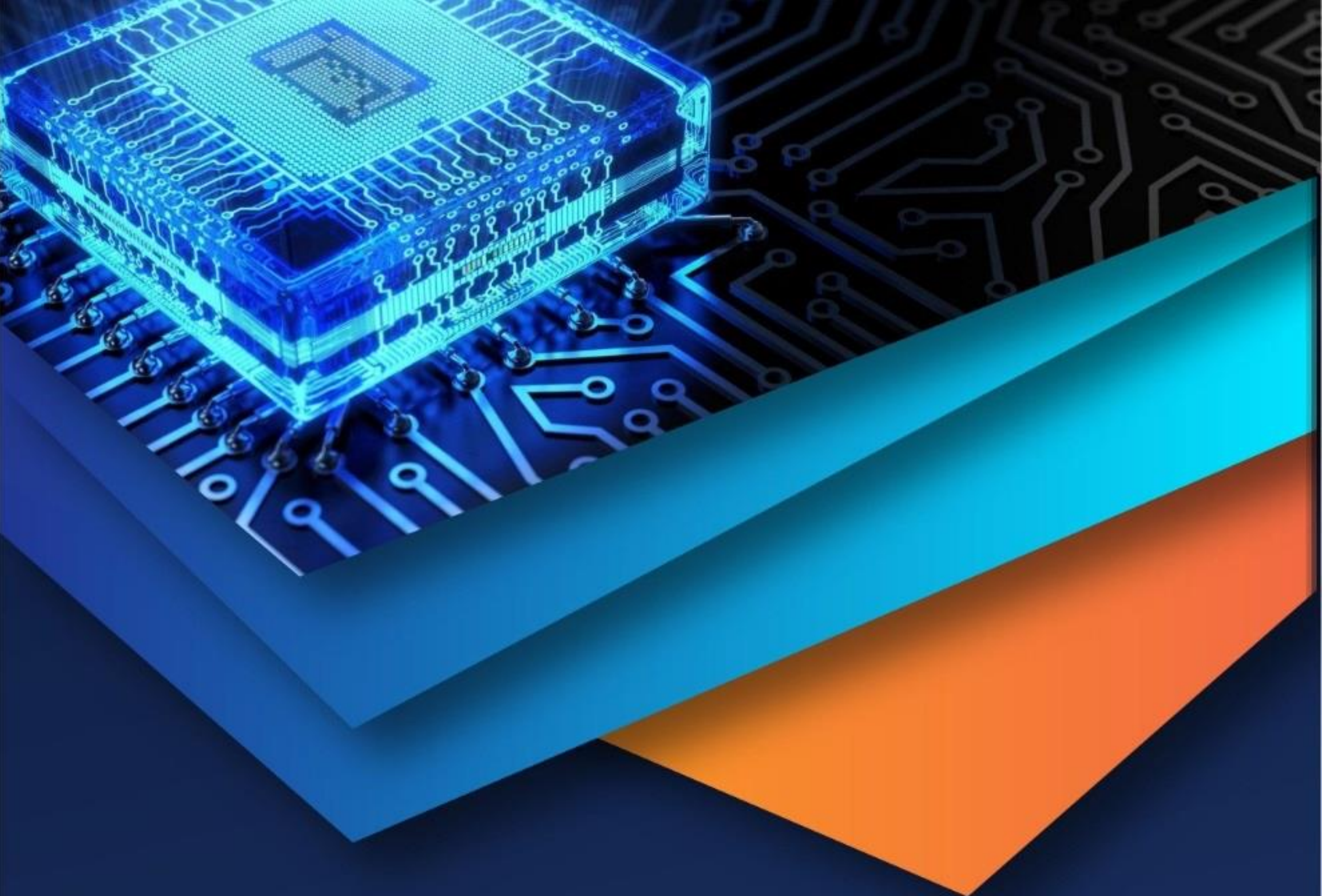
VII. ACKNOWLEDGMENTS

I thank our HOD P.Kanimozhi, Ph.D (Department of Computer Science and Engineering) to help us for creating this paper with his sincere guidance and Technical Expertise in the field of communication. The help of our guide Ms. A.Divya, M.Tech, Department of CSE, IFET College of Engineering is really immense and once again I thank her for her great motivation. I thank IFET College of Engineering to provide me such a standard educational environment so that I am able to understand the minute concepts in the field of Engineering.

REFERENCES

[1] K.-K.R. Choo, C. Boyd, and Y. Hitchcock, ''The Importance of Proofs of Security for Key Establishment Protocols: Formal Analysis of Jan-Chen, Yang-Shen-Shieh, Kim-Huh-Hwang-Lee,Lin-Sun-Hwang, Yeh-Sun Protocols,'' Comput. Commun., vol. 29,no. 15, pp. 2788-2797, Sept. 2006.
[2] 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.
[3] 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.
[4] 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.
[5] J.Hu, D. Gingrich, and A. Sentosa, ''A k-NearestNeighbor Approach for User Authentication Through Biometric Keystroke Dynamics,'' in Proc. IEEE ICC Conf., Beijing, China, May 2008, pp. 1556-1560.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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. 388-39.

Nivas M received diploma from "Elumalai Polytechnic College, Villupuram" in 2012.Currently he pursues his B.E from IFET College of Engineering from Department of Computer Science Engineering. His area of expertise is Java Technology, HTML, XML,C and C++.



10.22214/IJRASET

INDEX COPERNICUS

45.98

ISRA JIF

IMPACT FACTOR: 7.129

SJIFactor

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY