SECURITY ANALYSIS OF SMARTPHONE AND CLOUD COMPUTING AUTHENTICATION FRAMEWORKS AND PROTOCOLS

SAILAJA LATCHAMSETTY[1], M.PRAVEEN KUMAR[2]
[1]M.Tech Student in CSE, NALANDA INSTITUTE OF ENGINEERING & TECHNOLOGY, AP
[2]Associate Professor, Dept of CSE, NALANDA INSTITUTE OF ENGINEERING & TECHNOLOGY, AP

Abstract: We live in a digital world where every detail of our information is being transferred from one smart device to another via cross-platform, third-party cloud services. Smart technologies, such as, Smartphones are playing dynamic roles in order to successfully complete our daily routines and official tasks that require access to all types of critical data. Before the advent of these smart technologies, securing critical information was quite a challenge. However, after the advent and global adoption of such technologies, information security has become one of the primary and most fundamental task for security professionals. The integration of social media has made this task even more challenging to undertake successfully. To this day, there are plentiful studies in which numerous authentication and security techniques were proposed and developed for Smartphone and cloud computing technologies. These studies have successfully addressed multiple authentication threats and other related issues in existing Smartphone and cloud computing technologies. However, to the best of our understanding and knowledge, these studies lack many aspects in terms of authentication attacks, logical authentication analysis and the absence of authentication implementation scenarios. Due to these authentication anomalies and ambiguities, such studies cannot be fully considered for successful implementation. Therefore, in this paper, we have performed a comprehensive security analysis and review of various Smartphone and cloud computing authentication frameworks and protocols to outline up-to-date authentication threats and issues in the literature. These authentication challenges are further summarized and presented in the form of different graphs to illustrate where the research is currently heading. Finally, based on those outcomes, we identify the latest and existing authentication uncertainties, threats and other related issues to address future directions and open research issues in the domain of Smartphone- and cloud-computing authentication.

I. INTRODUCTION

The logical design of a system pertains to an abstract representation of the data flows, inputs and outputs of the system. This is often conducted via modeling, using an over-abstract (and sometimes graphical) model of the actual system. In the context of systems design are included. Logical design includes ER Diagrams i.e. Entity Relationship Diagrams. We live in a digital world where every detail of our information is being transferred from one smart device to another via cross-platform, third-party cloud services. Smart technologies, such as, Smartphones are playing dynamic roles in order to successfully complete our daily routines and official tasks that require access to all types of critical data. Before the advent of these smart technologies, securing critical information was quite a challenge. However, after the advent and global adoption of such technologies, information security has become one of the primary and most fundamental task for security professionals. The integration of social media has made this task even more challenging to undertake successfully. To this day, there are plentiful studies in which numerous authentication and security techniques were proposed and developed for Smartphone and cloud computing technologies. These studies have successfully addressed multiple authentication threats and other related issues in existing Smartphone and cloud computing technologies. However, to the best of our understanding and knowledge, these studies lack many aspects in terms of authentication attacks, logical authentication analysis and the absence of authentication implementation scenarios. Due to these authentication anomalies and ambiguities, such studies cannot be fully considered for successful implementation. Therefore, in this paper, we have performed a comprehensive security analysis and review of various Smartphone and cloud computing authentication frameworks and protocols to outline up-to-date authentication threats and issues in the literature. These authentication challenges are further summarized and presented in the form of different graphs to illustrate where the research is currently heading. Finally, based on those outcomes, we identify the latest and existing authentication uncertainties, threats and other related issues to address future directions and open research issues in the domain of Smartphone- and cloud-computing authentication..

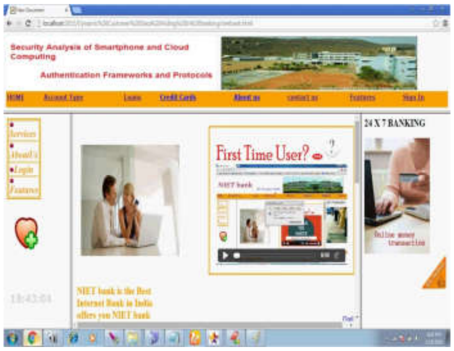
II. EXISTING SYSTEM

Modern day technologies are evolving from smartcards to more advanced and smart technologies such as Smartphones. Since 1968, smartcard based privacy and security challenges were addressed, with numerous proposals emerging on smartcard based authentication frameworks and protocols. However, due to the existing smartcard limitations, the security and privacy challenges were not completely addressed and presented [1]. On the other hand, Smartphones are playing a vigorous role to accomplish our daily tasks and routines. From waking-up to going-to-bed, every routine is now linked and performed with the help of Smartphone applications. Based on Web of Sciences citation analysis, the rising trend of Smartphone usage has made information security a more challenging task, and a consequent increase in research and citations in the past two decades. Additionally, with the advent and integration of Cloud Computing (CC) technologies, security and privacy issues have become more challenging. Our data, which was initially stored on our hard drives, is now mainly stored on third-party Cloud Servers. Moreover, according to [3], 75% of Smartphone applications require access to critical user data, including Location, Device ID, Camera, Contacts etc. The use of those technologies has made Smartphones vulnerable to Smartphone-level security threats, and has increased susceptibility to third-part security threats [1]

III. Proposed System

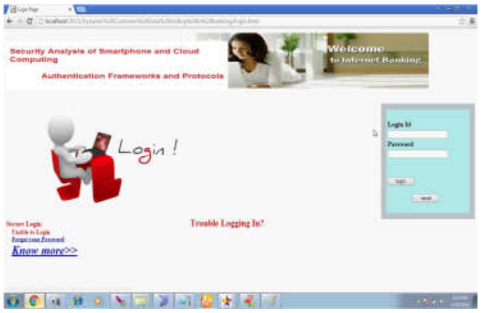
Nowadays, Smartphones are well equipped with numerous authentication mechanisms such as, Multiple Factor Authentication (MFA),Two Factor Authentication (2FA) and Three Factor Authentication (3FA) [18-20]. A 3FA based Smartphone is able to provide higher security for critical information [21]. However, it is not necessary that cloud resources (integrated within a Smartphone application) provide support for MFA or 3FA based authentication. Additionally, the risk of a security breach is higher when such cloud resources are involved in transferring user critical information and have access to built-in Smartphone resources (Figure 2). On the other hand, without such access permissions, those applications will fail to perform essential tasks associated with either daily routines or professional chores. Those risks are not only limited to Smartphones. Nowadays, Smart devices such as tablets and phone-tabs have replaced our regular Personal Computers and Laptops. Moreover, almost all domains and sectors are utilizing those smart technologies to perform their normal or critical operations[22 and 23]. The security risk is very high when we consider sensitive domains and sectors that include: Military, Defense, Telecommunications, Health and other governmental or non-governmental entities [24 - 29]. Based on the above understanding, multiple authentication frameworks and protocols are proposed and developed to provide end-to-end security, privacy and verification to all entities and domains. However, there remains plenty to cover and explore in terms of security and privacy in Smartphones and CC authentication frameworks. The purpose of this study is to analyze and document existing and primary security challenges pertaining to Smartphones and CC Authentication Frameworks and Protocols.

IV. SCREEN SHOTS

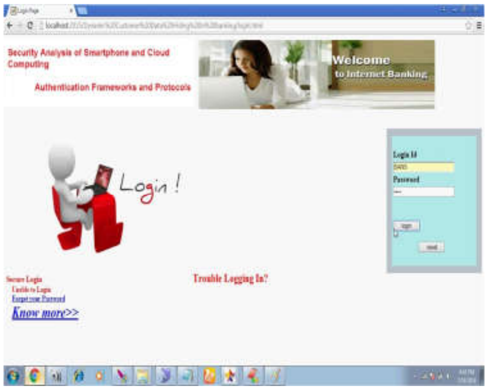

Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

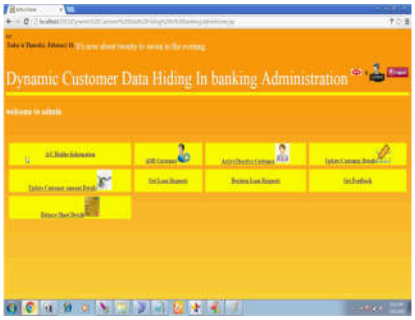
NIET bank is the Best Internet Bank in India offers you NIET bank


Security Analysis of Smartphone and Cloud Computing

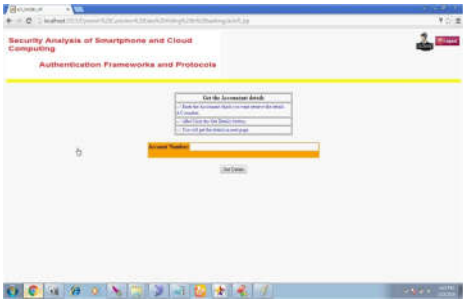
Authentication Frameworks and Protocols


Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

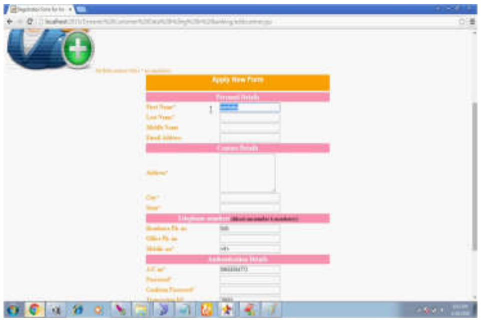


Dynamic Customer Data Hiding In banking Administration



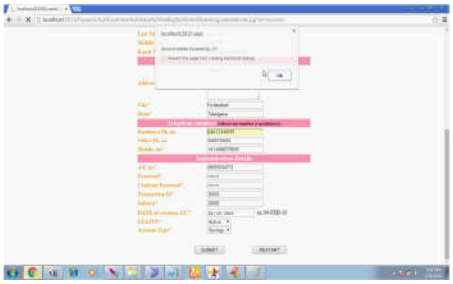
Security Analysis of Smartphone and Cloud Computing

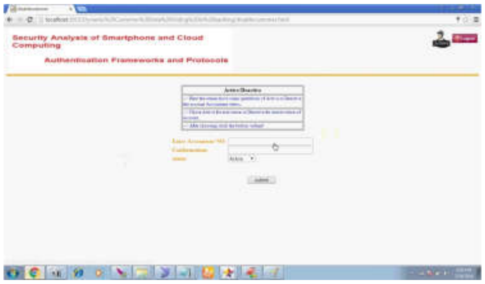
Authentication Frameworks and Protocols



Apply New Form

Dynamic Customer Data Hiding In banking Administration





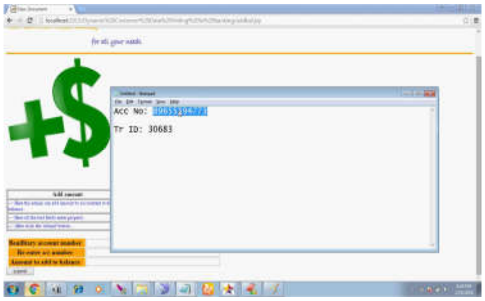
Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

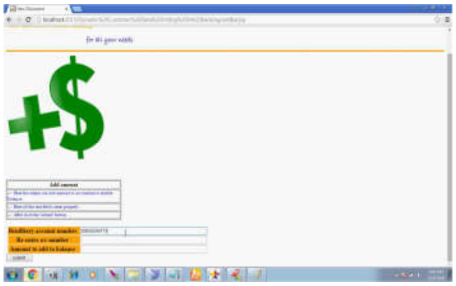
Security Analysis of Smartphone and Cloud Computing

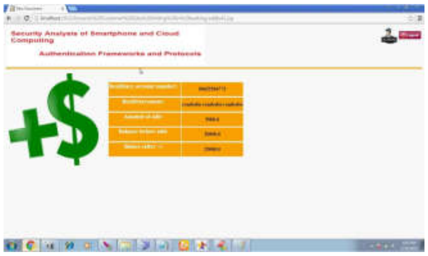
Authentication Frameworks and Protocols

Update Accountant Details



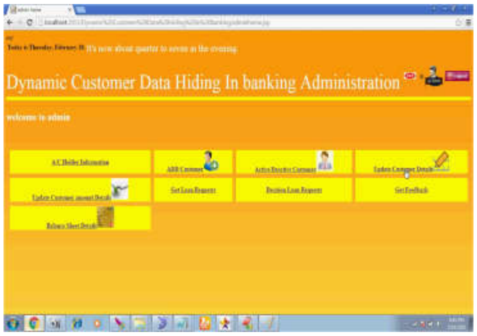
```
Acc No: 39655394773
Tr ID: 30683
```





Security Analysis of Smartphone and Cloud Computing

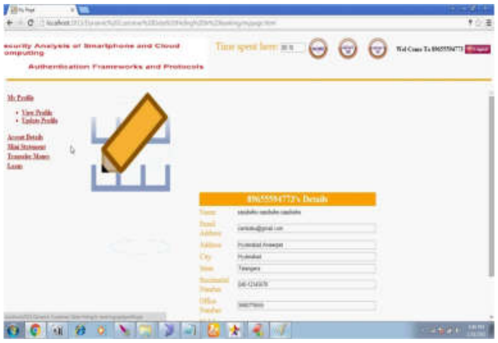
Authentication Frameworks and Protocols



Today is Thursday, February 18. It's now about quarter to seven in the evening.

Dynamic Customer Data Hiding In banking Administration

welcome to admin



Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Time spent here:

Wel Come To 89655594773

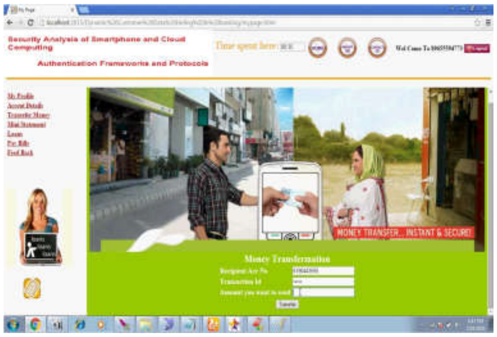
89655594773's Details

Name	[illegible]
Email Address	[illegible]@gmail.com
Address	Hyderabad [illegible]
City	Hyderabad
State	Telangana
Residential Number	040-1234[illegible]
Office Number	[illegible]

Today is Thursday, February 18. It's now about quarter to seven in the evening.

Dynamic Customer Data Hiding In banking Administration

welcome to admin



Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Time spent here:

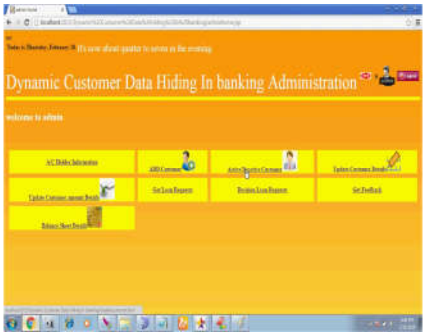
Wel Come To 89655594773

Money Transformation

Recipient Acc No

Transaction Id

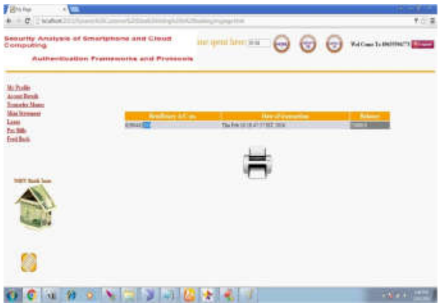
Amount you want to send



Today is Thursday, February 18. It's now about quarter to seven in the evening.

Dynamic Customer Data Hiding In banking Administration

welcome to admin



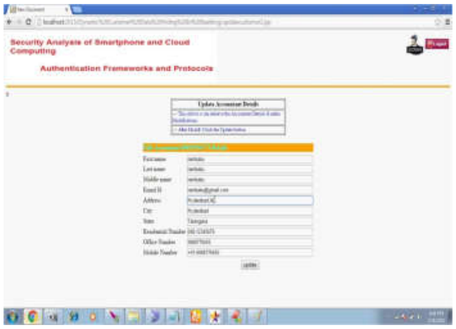
Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Time spent here:

Wel Come To 89655594773

Beneficiary A/C no	Date of transaction	Balance
[illegible]	Thu Feb 18 18:47:17 IST 2016	[illegible]

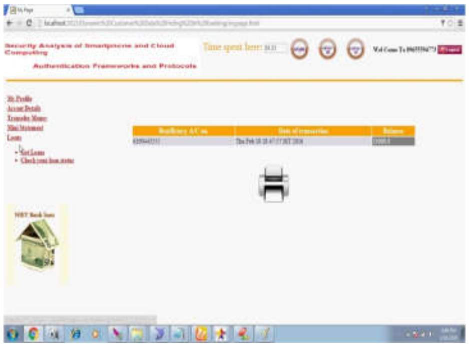


Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Update Accountant Details

First name	[illegible]
Last name	[illegible]
Middle name	[illegible]
Email Id	[illegible]@gmail.com
Address	Hyderabad [illegible]
City	Hyderabad
State	Telangana
Residential Number	040-1234[illegible]
Office Number	[illegible]
Mobile Number	+91 [illegible]



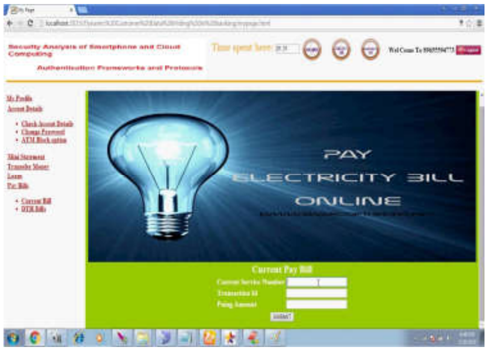
Security Analysis of Smartphone and Cloud Computing

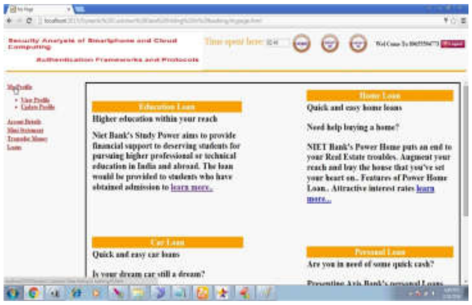
Authentication Frameworks and Protocols

Time spent here:

Wel Come To 89655594773

Beneficiary A/C no	Date of transaction	Balance
[illegible]	Thu Feb 18 18:47:17 IST 2016	[illegible]





Education Loan

Higher education within your reach

Niet Bank's Study Power aims to provide financial support to deserving students for pursuing higher professional or technical education in India and abroad. The loan would be provided to students who have obtained admission to learn more..

Home Loan

Quick and easy home loans

Need help buying a home?

NIET Bank's Power Home puts an end to your Real Estate troubles. Augment your reach and buy the house that you've set your heart on.. Features of Power Home Loan.. Attractive interest rates learn more..

Car Loan

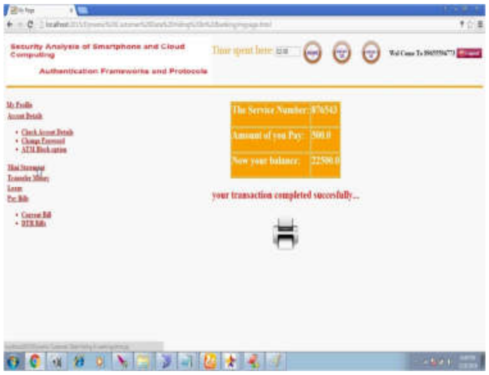
Quick and easy car loans

Is your dream car still a dream?

Personal Loan

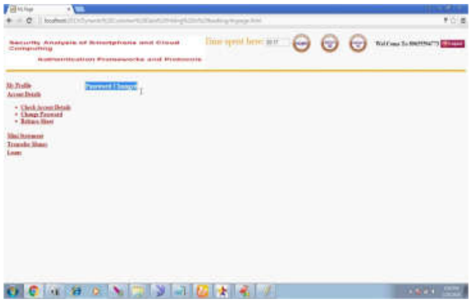
Are you in need of some quick cash?

Presenting Axis Bank's personal Loans

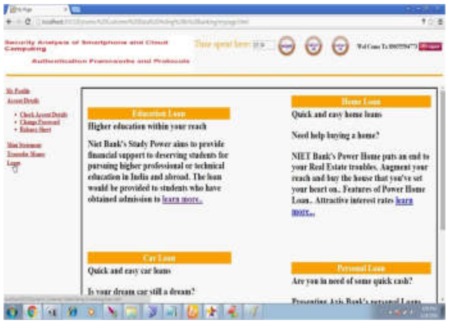


The Service Number:	876543
Amount of you Pay:	500.0
Now your balance:	22500.0

your transaction completed succesfully...



Password Changed



Education Loan

Higher education within your reach

Niet Bank's Study Power aims to provide financial support to deserving students for pursuing higher professional or technical education in India and abroad. The loan would be provided to students who have obtained admission to learn more..

Home Loan

Quick and easy home loans

Need help buying a home?

NIET Bank's Power Home puts an end to your Real Estate troubles. Augment your reach and buy the house that you've set your heart on.. Features of Power Home Loan.. Attractive interest rates learn more..

Car Loan

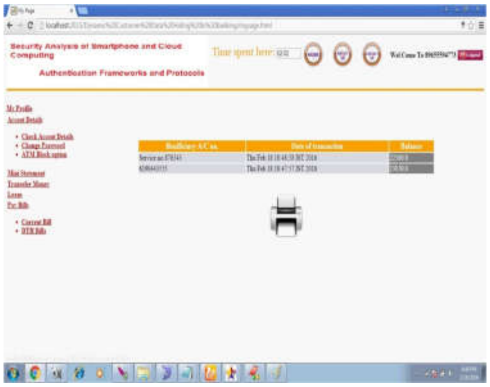
Quick and easy car loans

Is your dream car still a dream?

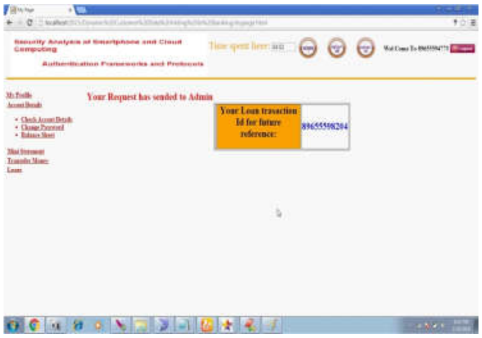
Personal Loan

Are you in need of some quick cash?

Presenting Axis Bank's personal Loans

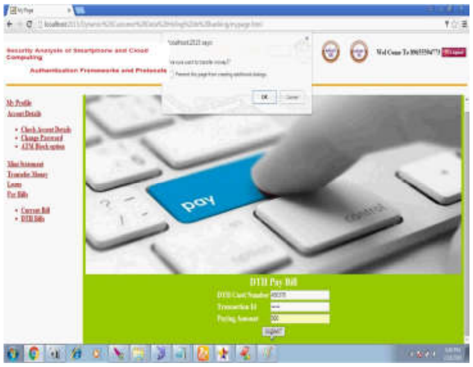


Beneficiary A/C no.	Date of transaction	Balance
Service no:876543	Thu Feb 01 18:46:38 IST 2018	22500.0
[illegible]	Thu Feb 01 18:47:57 IST 2018	[illegible]



Your Request has sended to Admin

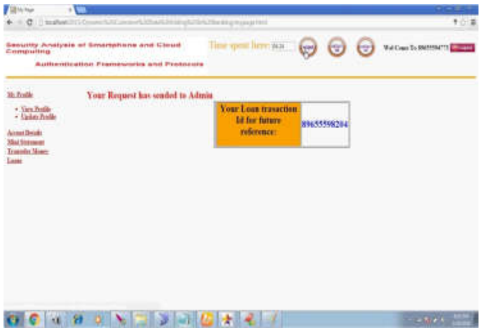
Your Loan transaction Id for future reference:	89655598204



localhost:2015 says:

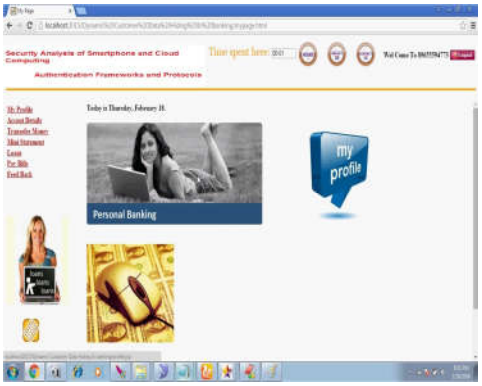
Are you sure want to transfer money?

□ Prevent this page from creating additional dialogs



Your Request has sended to Admin

Your Loan transaction Id for future reference:	89655598204

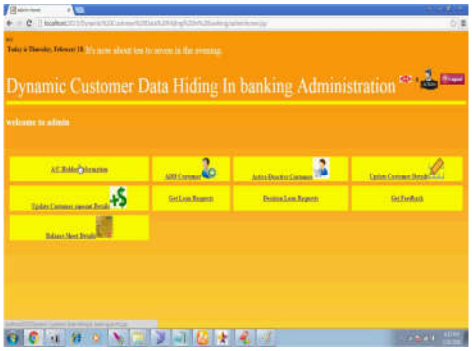


Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Time spent here:

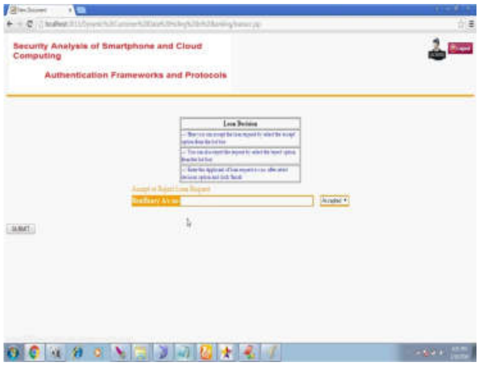
Today is Thursday, February 18.



Today is Thursday, February 18. It's now about ten to seven in the evening.

Dynamic Customer Data Hiding In banking Administration

welcome to admin



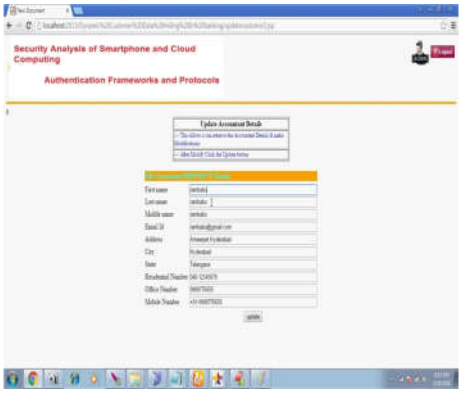
Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Loan Decision

Accept or Reject Loan Request

Beneficiary A/c no

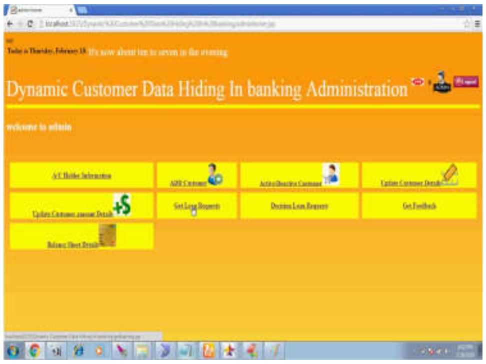


Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

Update Accountant Details

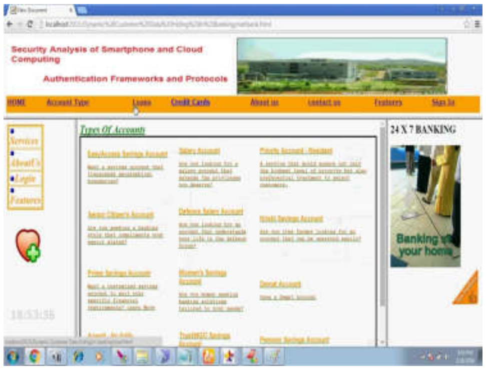
First name	[illegible]
Last name	[illegible]
Middle name	[illegible]
Email Id	[illegible]@gmail.com
Address	[illegible] Hyderabad
City	Hyderabad
State	Telangana
Residential Number	040-1234576
Office Number	[illegible]
Mobile Number	+91-[illegible]



Today is Thursday, February 18. It's now about ten to seven in the evening.

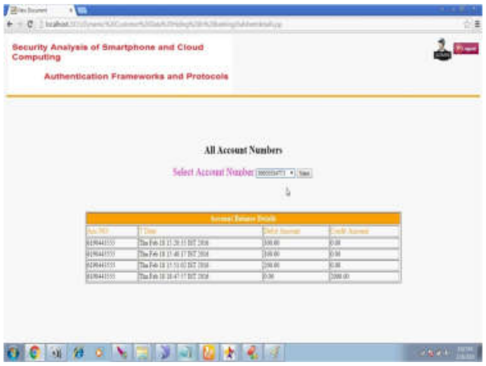
Dynamic Customer Data Hiding In banking Administration

welcome to admin



Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols



Security Analysis of Smartphone and Cloud Computing

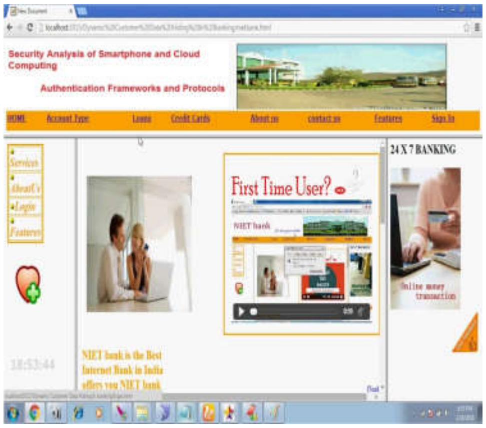
Authentication Frameworks and Protocols

All Account Numbers

Select Account Number

Account Balance Details

Acc NO	Time	Debit Amount	Credit Amount
[illegible]	Thu Feb 18 15:28:15 IST 2016	100.00	0.00
[illegible]	Thu Feb 18 15:48:17 IST 2016	100.00	0.00
[illegible]	Thu Feb 18 15:51:02 IST 2016	200.00	0.00
[illegible]	Thu Feb 18 18:47:17 IST 2016	0.00	2000.00



Security Analysis of Smartphone and Cloud Computing

Authentication Frameworks and Protocols

CONCLUSION

To the best of our knowledge, this paper is the first study about optimal encoding parameters for representation sets in free-viewpoint adaptive streaming. We have defined an optimization problem for the selection of the representation set that maximizes the average satisfaction of interactive users while minimizing their view-switching delay. We define a novel variable, namely the multi-view navigation segment, and formulate an optimization problem that can be solved as a tractable ILP problem. We characterize the satisfaction of interactive users as the quality experienced by the user during the navigation. This function is able to take into account both coding and view synthesis artifacts. We finally measure the performance of representation sets based on content provider recommendations and show the suboptimality of baseline algorithms that do not adapt the coding parameters to the video and users characteristics. We therefore highlight the gap between existing recommendations and solutions that maximize the average user satisfaction. In particular, we show that an unequal allocation of the storage capacity among different video types as well as camera views is essential to strike for the right balance between storage cost and users satisfaction in interactive multi-view video systems.

REFERENCES

[1]“Google cardboard,” https://www.google.com/get/cardboard.

[2] “Oculus rift,” https://www.oculus.com/en-us/rift.

[3] “Lytro immerge,” https://www.lytro.com/immerge.

[4] “BBC ressearch,” http://www.bbc.co.uk/rd/projects/iview.

[5] D. Tian, P.-L. Lai, P. Lopez, and C. Gomila, “View synthesis techniques for 3D video,” in SPIE Optical Engineering Applications, vol. 7443, 2009.

[6] K. Calagari, K. Templin, T. Elgamal, K. Diab, P. Didyk, W. Matusik, and M. Hefeeda, “Anahita: A system for 3D video streaming with depth customization,” in Proc. ACM Int. Conf. on Multimedia, Orlando, Florida, November 2014.