SECURE KEY AGREEMENT AND KEY PROTECTION FOR MOBIL DEVICE USER AUTHENTICATION

V.Sarala [1], D.Kiran,

[1]**Assistant professor , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-vedalasarala21@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- kirandondapati2001@gmail.com

ABSTRACT

As mobile devices ownership becomes more prevalent (e.g. a user owns multiple mobile devices), the capability to offer secure and user-friendly authentication becomes increasingly important. While a large number of identity-based user authentication mechanisms for wireless mobile environment have been proposed. However, they are not generally designed for situations where a user's private key and some other sensitive data can be exposed if his/her mobile device is remotely or physically controlled by an attacker. Threshold secret sharing is one of the solutions to this problem, but it is limited in the requirement that there should exist an honest third-party to hold the complete key after secret reconstruction process. Therefore, in this paper, we consider the special case that only two devices (i.e. no honest party) at the user's side jointly perform user authentication with a server, and neither device can successfully complete the authentication process alone. Moreover, the key reconstruction is not needed during authentication so that neither device can hold a complete key. We then analyze the security of the proposed protocol and show that it satisfies all known security requirements in practical applications, particularly the key exposure attack resistance.

1 INTRODUCTION

WITH the rapid development of wireless communication technologies, the mobile devices (i.e. smartphones and PADs) have become more popular and ubiquitous owing to the fact that they enable users to access the Internet anytime and anywhere. According to a recent survey [1], the number of smartphones users in the United States has risen steadily in recent years. Up to 2017, the number of smartphones was approximately 224.3 million, with the number of smartphone users worldwide exceeding 2 billion users. It is also increasingly common for individuals to travel with at least two mobile devices, including wearable devices (e.g. smart watch) that are being paired to their smartphones. Advances in wireless telecommunication technology have paved the way for a wide variety of mobile services, such as on-line shopping, mobile banking. This technology revolution brings much convenience to the end-users who are limited to the distance and time. However, the more we use the mobile service in wireless networks, the higher risk we will have. For example, Kaspersky Lab reported that mobile banking usage in Brazil reached 11.2 billion transactions in 2015, with more than 33 million active accounts (according to the Brazilian Federation of Banks). Kaspersky Lab also claimed that such numbers and the possibility of cheaply sending SMS messages

are very attractive to cybercriminals [2]. Fig. 1 briefly depicts the system model of a typical mobile communication setup. Owing to the openness of network environment, attackers are capable of intercepting, modifying or replaying messages, as well as impersonating a legal user to access the remote servers for services. Therefore, an effective and user-friendly mutual authentication between mobile devices and remote servers is indispensable.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

Guo et al. proposed an attribute-based authentication protocol with user privacy preservation for electronic healthcare (e-Health) systems [22]. Although attribute-based encryption can provide fine-grained access control to resources, it also incurs high energy consumption [23]. Bilinear pairings are commonly used in identity-based authentication protocols. However, bilinear pairing operation is time-consuming and computationally expensive for a mobile device. Hence, a number of mobile user authentication protocols without bilinear pairings have been presented in the literature. Similar to the history of key establishment and agreement protocols, several protocols were found to be insecure after they have been published (e.g. the protocol in [30] was found to be vulnerable to impersonate attack mentioned in [31]).

Disadvantages:

- Existing authentication and key agreement protocols are generally designed to provide message security against external attackers and establish session secure key.
- No existing user authentication protocol can provide both secure key agreement and private key security with acceptable efficiency for the system.

Proposed System & alogirtham

- In this paper, we propose a new identity-based anonymous authentication protocol, designed to provide both secure keg agreement and key protection for mobile authentication, which yields better security and efficiency for mobile Internet environment. Specifically, the major contribution of the proposed protocol can be summarized below.
- First, we are the first to propose a secure authentication protocol based on the two-party computation for mobile Internet environment, which can resist the key exposure attack (considering a mobile device maliciously controlled by an attacker) and maintain the essential efficiency.

4.1 Advantages:

- The system has more security on data due to Two-factor Security and Mutual Authentication scheme.
- The system adopts data security to avoid any single entity having the complete key ownership in a sharing group.

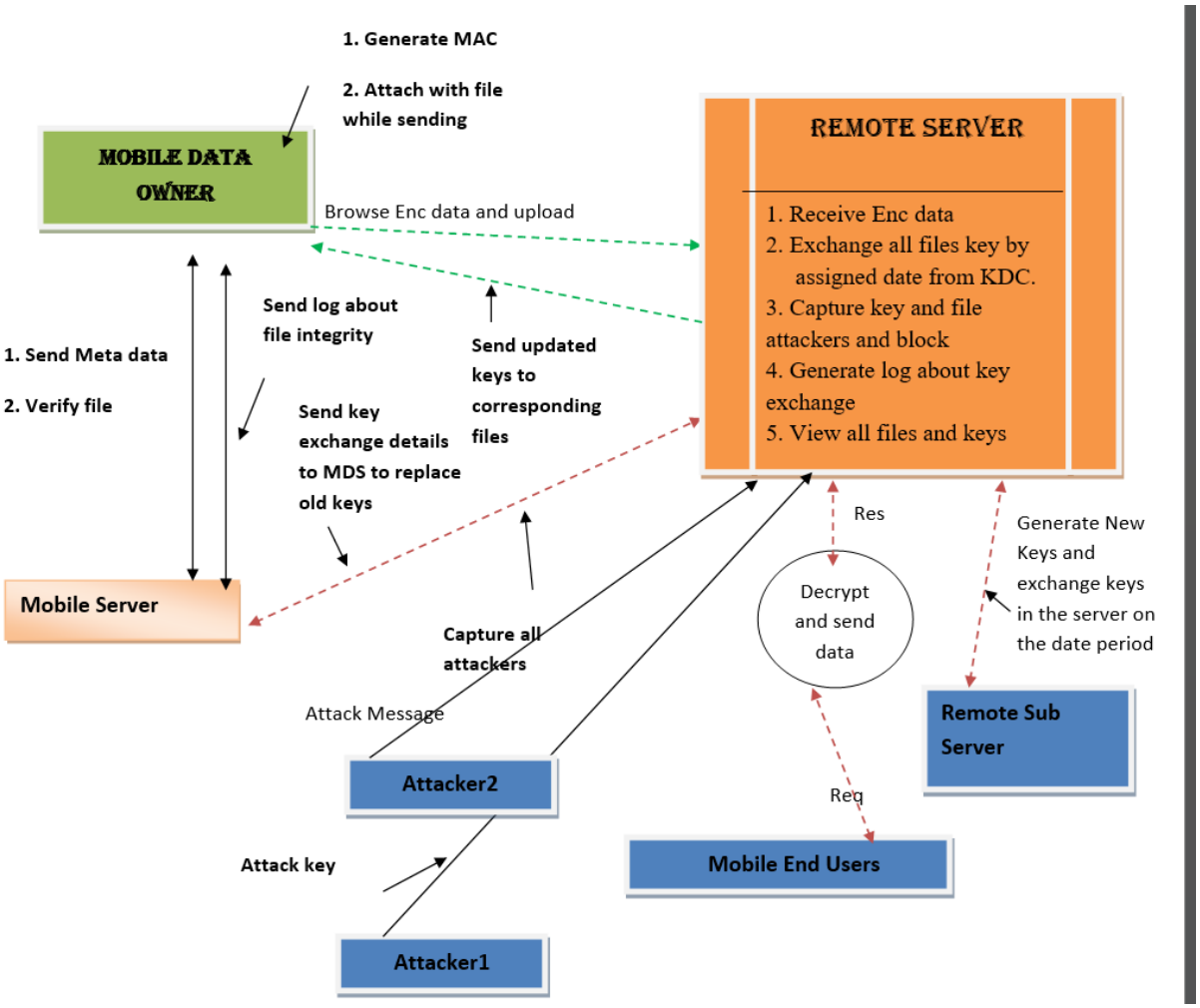


Fig:3.1 System Architecture

IMPLEMENTATION

MODULES

Mobile Data Owner

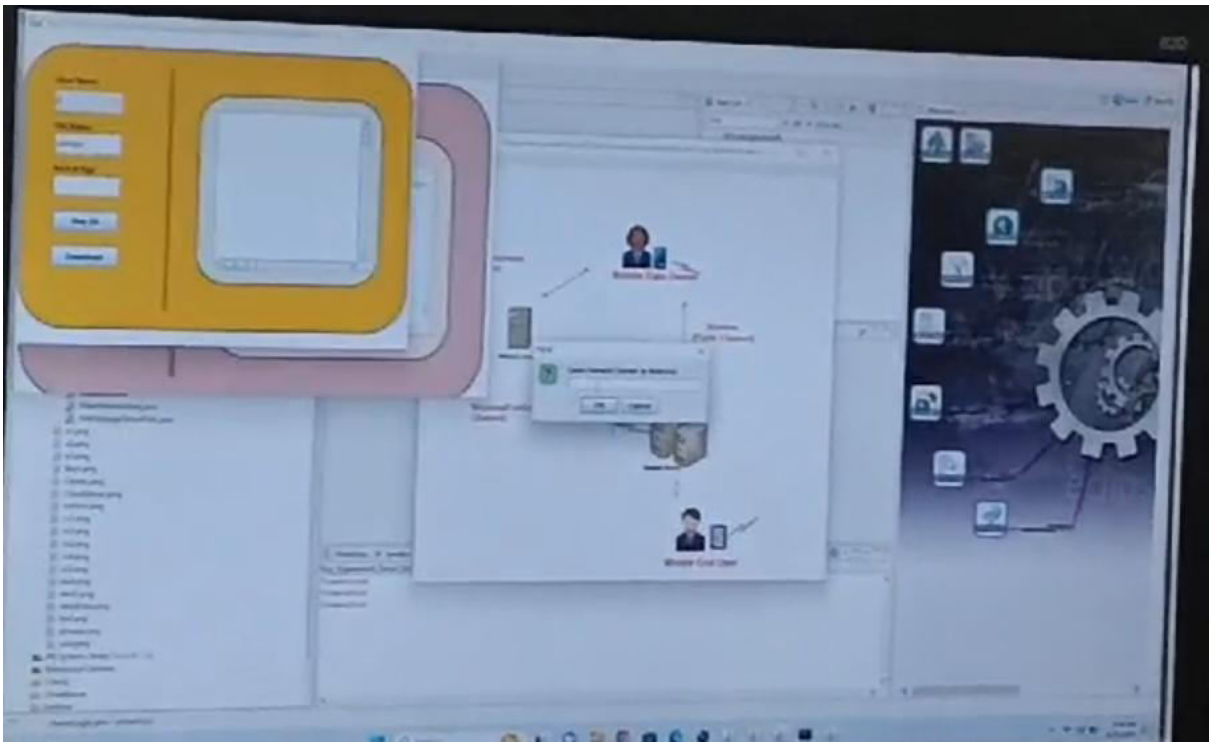
In this module, the client has to register by providing user name, password, and group, after registering Client has to Login by using valid user name and password. The Data Client browses and uploads their data to the Remote server. For the security purpose the data provider encrypts the data file and then stores in the Remote server. The Client is also responsible for uploading metadata to the Meta data server. The Data Client can also verify file. Data Client can also verify the file it is safe or not.

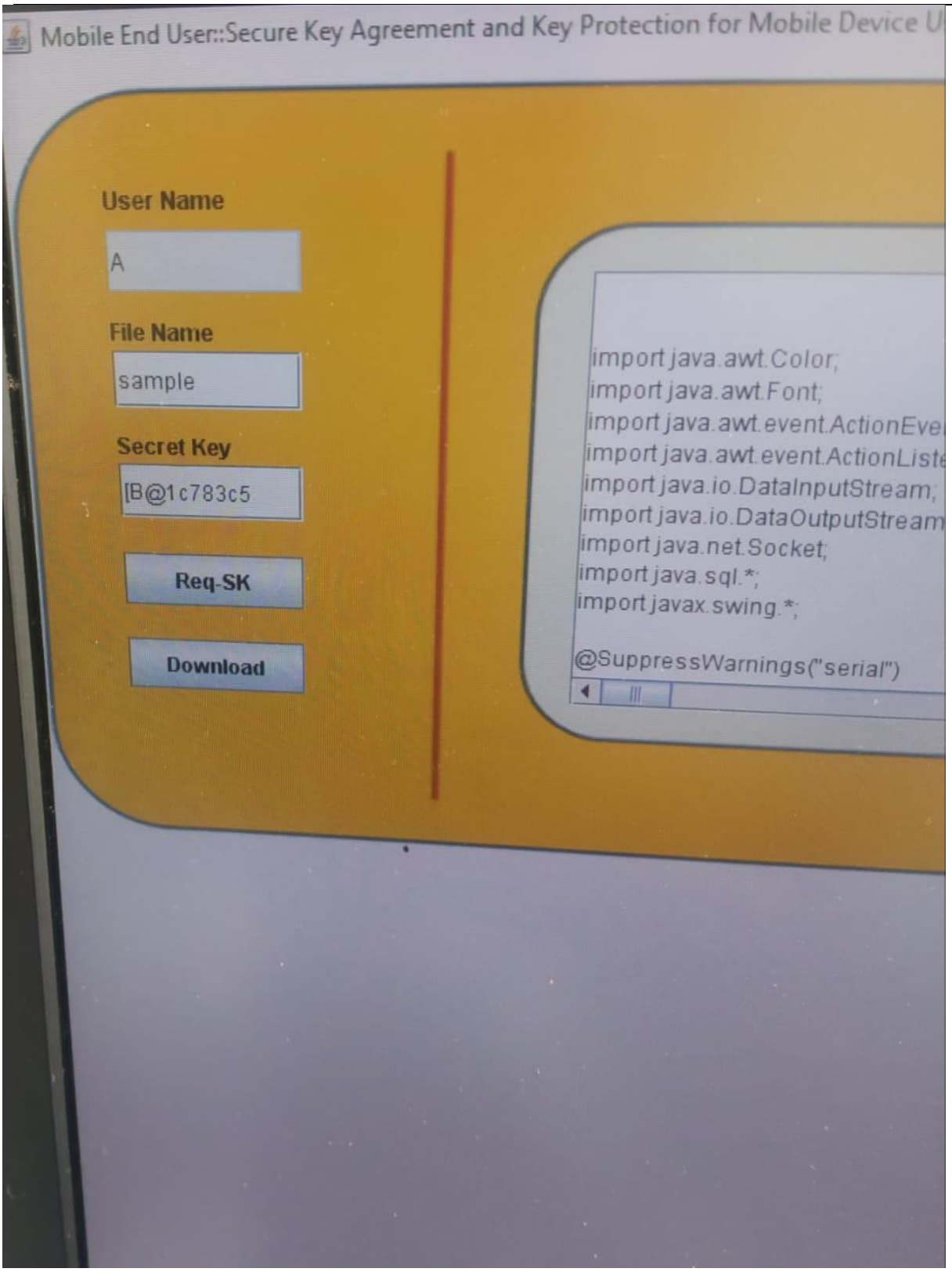
Remote Server

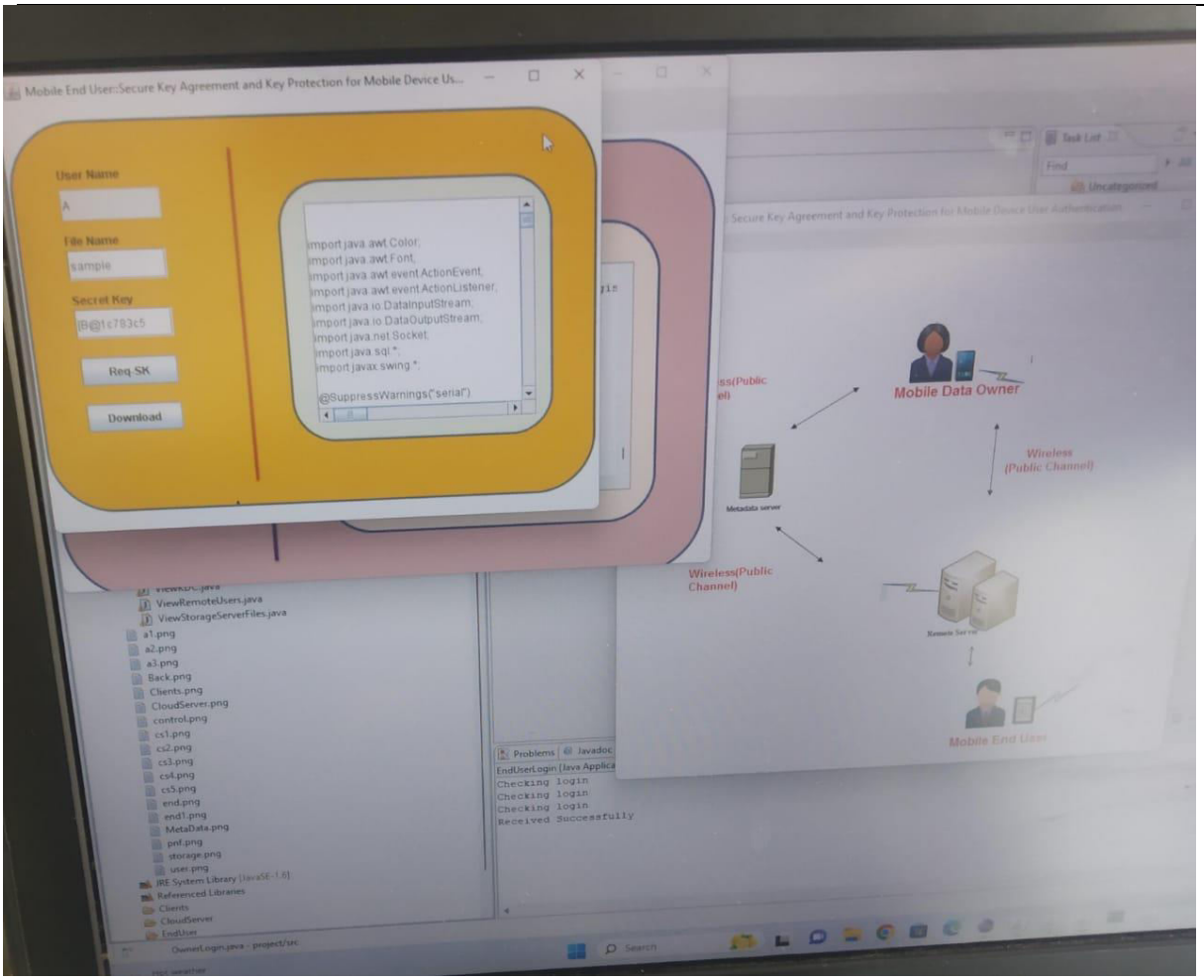
The Remote server is responsible for data storage and file authorization for an end user. The data file will be stored in Remote server with their tags such as Client, file name, secret key, MAC and private key, can also view the registered Clients and End-users in the Remote server. The data file will be sending based on the privileges. If the privilege is correct then the data will be sent to the corresponding user and also will check the file name, end user name and secret key. If all are true then it will send to the corresponding end user.

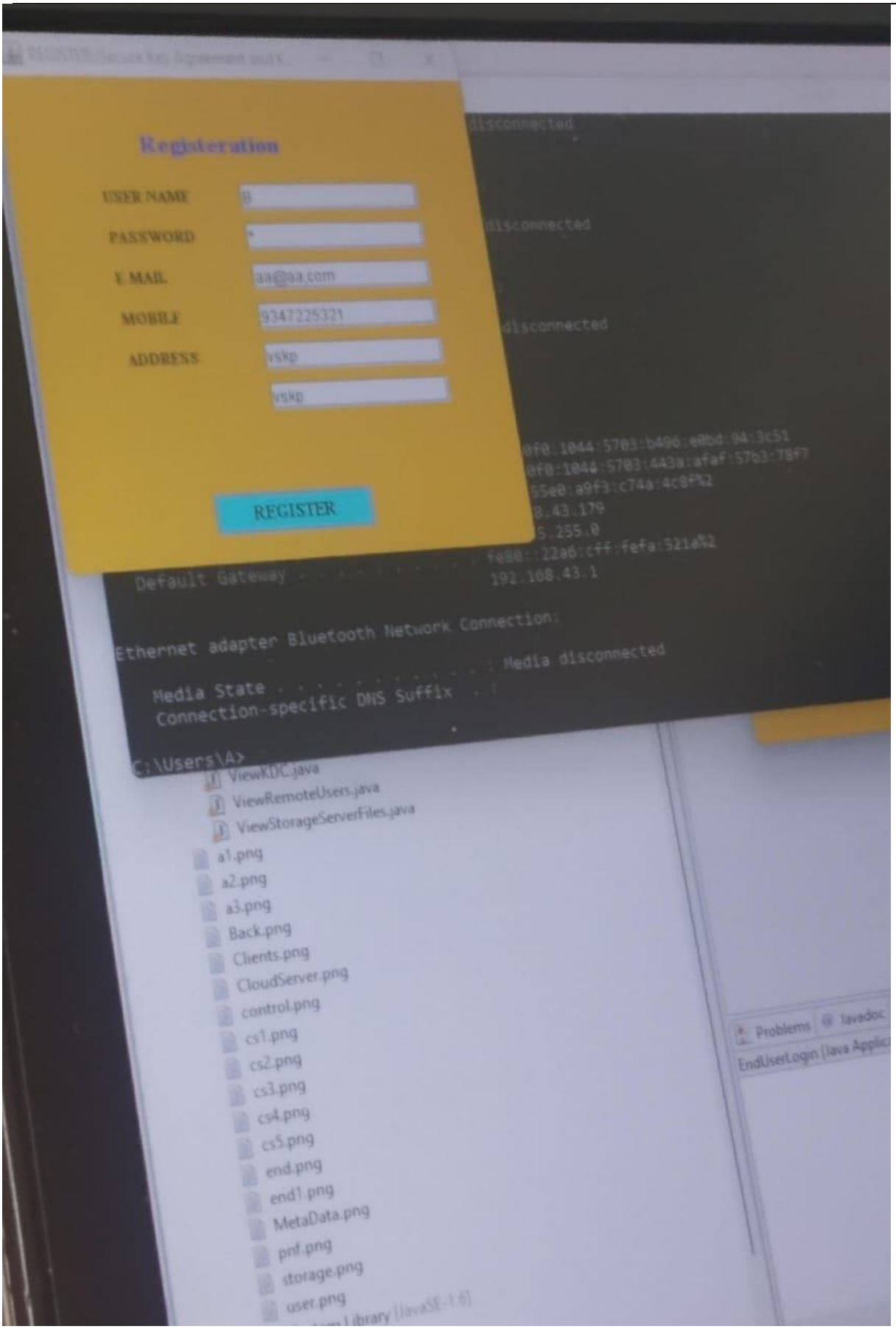
5 RESULTS AND DISCUSSION

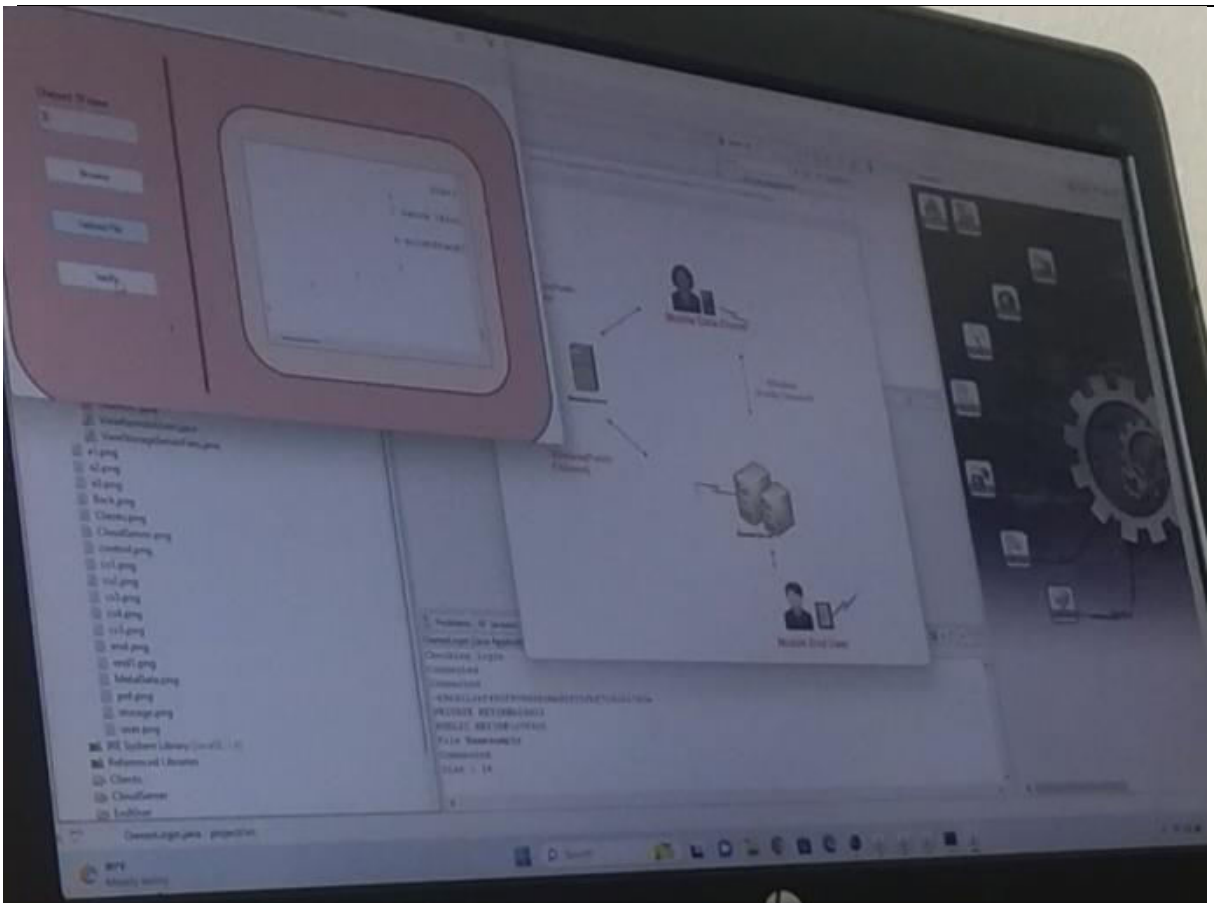
SCREEN SHORTS

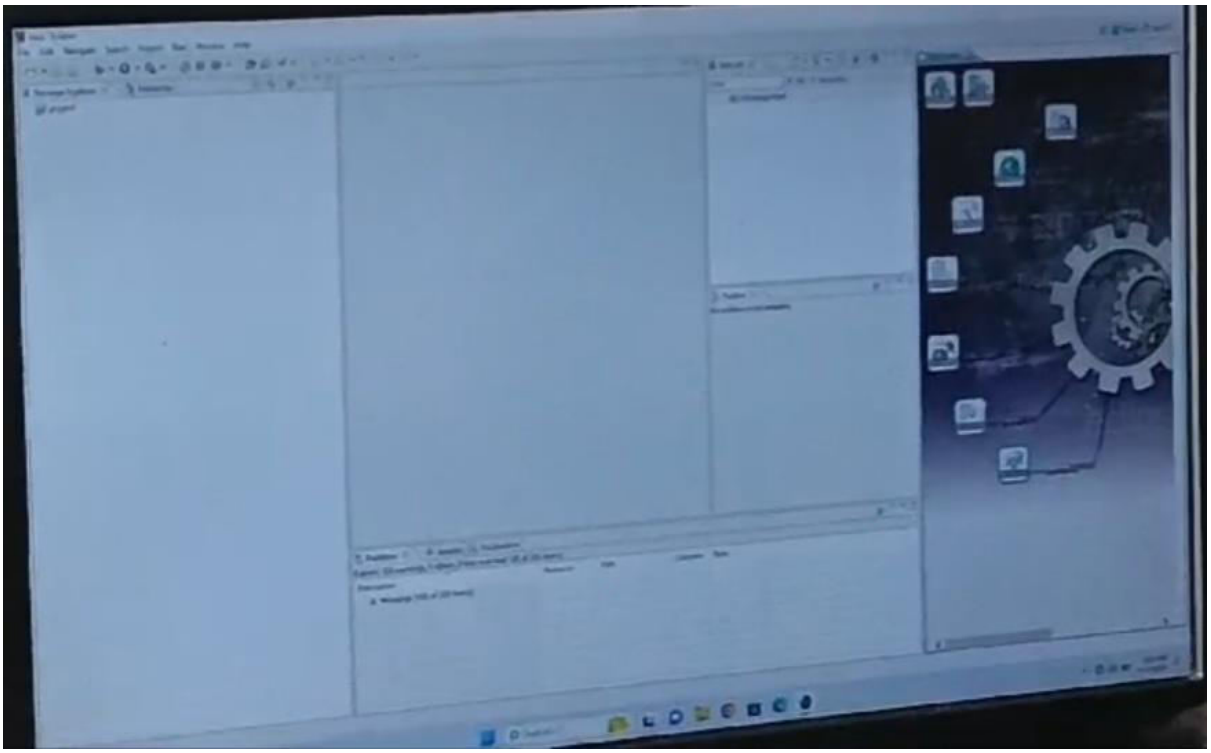


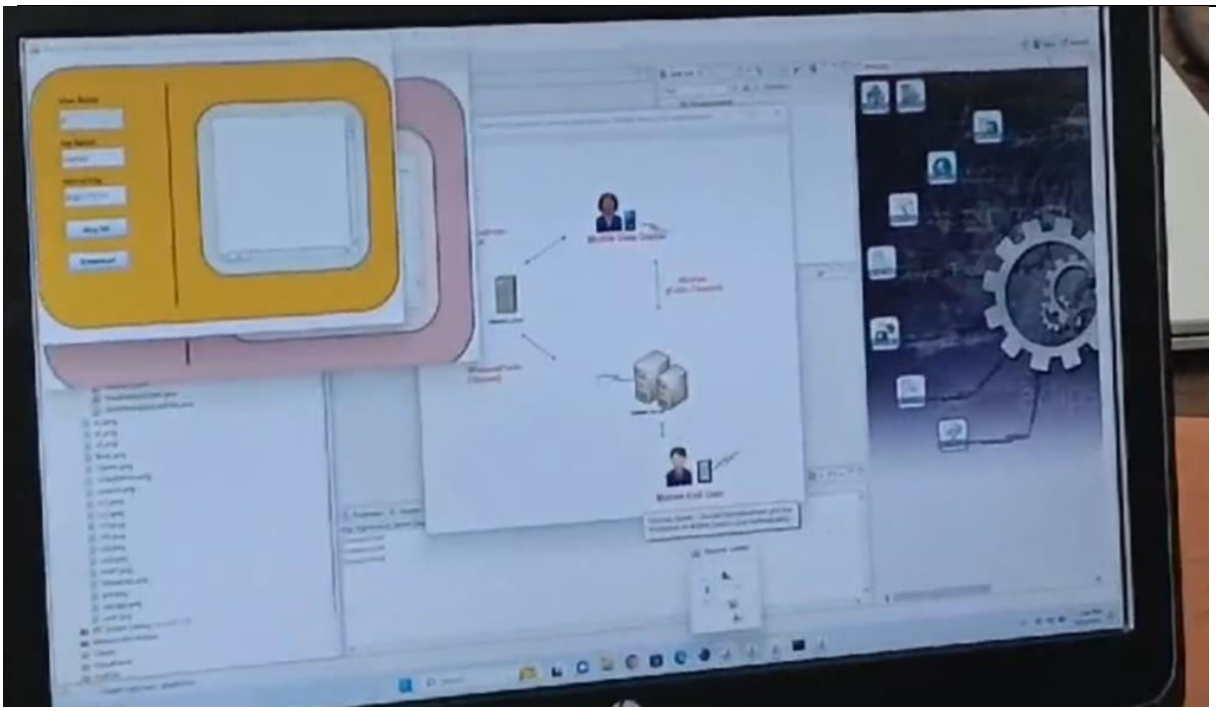

Mobile End User::Secure Key Agreement and Key Protection for Mobile Device U
User Name
A
File Name
sample
Secret Key
[B@1c783c5
Req-SK
Download
import java.awt.Color;
import java.awt.Font;
import java.awt.event.ActionEve
import java.awt.event.ActionListe
import java.io.DataInputStream;
import java.io.DataOutputStream
import java.net.Socket;
import java.sql.*;
import javax.swing.*;
@SuppressWarnings("serial")

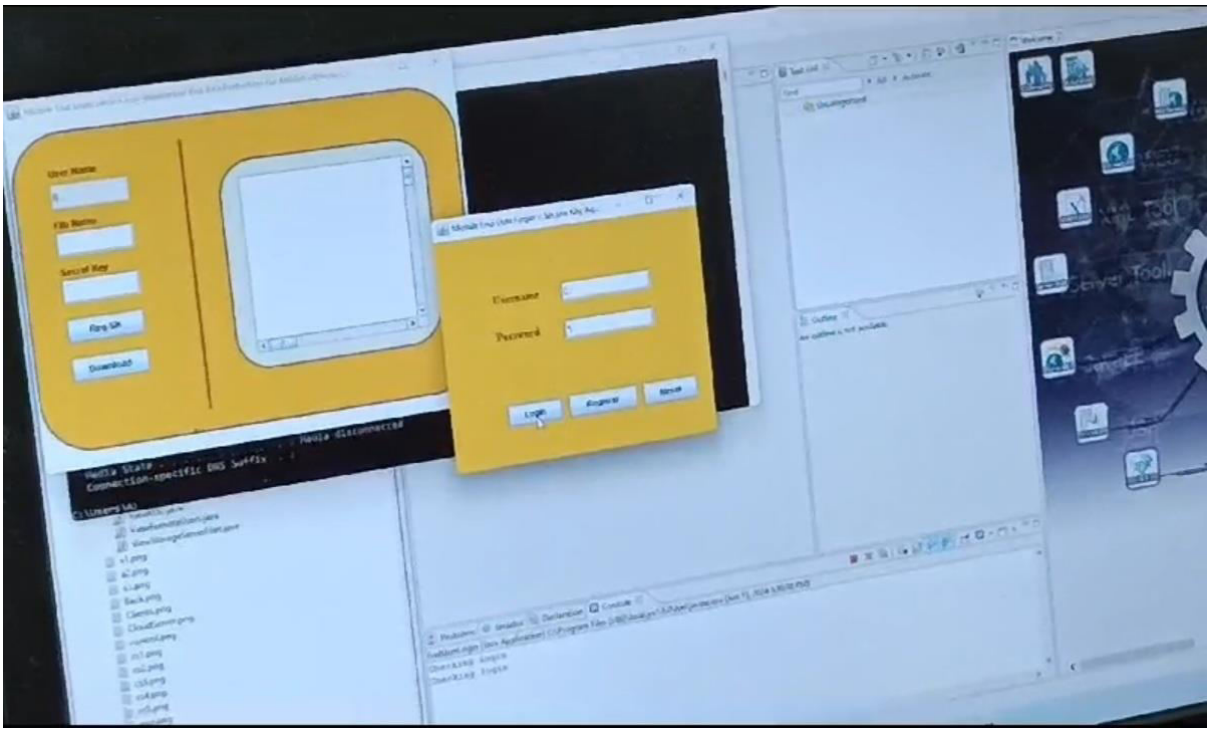

Mobile End User::Secure Key Agreement and Key Protection for Mobile Device Us...
User Name
A
File Name
sample
Secret Key
Req SK
Download
Mobile Data Owner
Wireless
(Public Channel)
Metadata server
Wireless(Public
Channel)
Mobile End User
Checking login
Checking login
Checking login
Received Successfully


Registeration
USER NAME
PASSWORD
E MAIL
MOBILE
9347225321
ADDRESS
vskp
vskp
REGISTER
Default Gateway
192.168.43.1
Ethernet adapter Bluetooth Network Connection:
Media State
Media disconnected
Connection-specific DNS Suffix
C:\Users\A>
ViewKDC.java
ViewRemoteUsers.java
ViewStorageServerFiles.java
a1.png
a2.png
a3.png
Back.png
Clients.png
CloudServer.png
control.png
cs1.png
cs2.png
cs3.png
cs4.png
cs5.png
end.png
end1.png
MetaData.png
pnf.png
storage.png
user.png
Problems
Javadoc
EndUserLogin [Java Applic








Username
Password
Login

6. CONCLUSION AND FUTURE WORK

CONCLUSION

Mobile device security will be increasingly important as more of such devices become part of the Internet-of-Things era (e.g. Internet-of-Vehicles, Internet-of-Battlefield-Things, and Internet-of-Military-Things). However, designing secure and efficient mutual authentication protocol for practical mobile device deployment remains challenging. In this paper, we proposed a novel user authentication protocol based on two-party computation. The protocol is also designed to mitigate key exposure attack when one of the user's devices is obtained or compromised by some attackers. Our security and performance evaluations demonstrated the practicality of our proposed protocol. However, we will need to develop a prototype implementation of the protocol in a real-world environment in order to be fully assured of its real-world utility. Therefore, one future research agenda is to collaborate with a mobile device developer to implement the proposedprotocol for real-world evaluation.

7. REFRENCES

[1] The Statistics Portal. Number of smartphone users in the unitedstates from 2010 to 2022. https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/.

[2] Fabio Assouline. Smishing and the rise of mobile banking attacks. https://securelist.com/smishing-and-the-rise-of-mobile-banking-attacks/75575/.

[3] Wenhao Liu, Shembo Wang, Xiao Tan, Qi Xie, and Qishan Wang.Identity-based one round key agreement protocol without bilinear pairings.In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC),2015 10th International Conference on, pages 470–473. IEEE, 2015.

[4] Mohammad Sabzinejad Farash and Mahmoud Ahmadian Attari. Aprovably secure and efficient authentication scheme for access control in mobile pay-tv systems. Multimedia Tools and Applications, 75(1):405–424, 2016.

[5] Jia-Lun Tsai and Nai-Wei Lo. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal,9(3):805–815, 2015.

[6] Debiao He, Sherali Zeadally, Neeraj Kumar, and Jong-Hyouk Lee.Anonymous authentication for wireless body area networks with provablesecurity. IEEE Systems Journal, 2016.

[7] Libing Wu, Yubo Zhang, Yong Xie, Abdulhameed Alelaiw, and Jian Shen. An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. Wireless Personal Communications, 94(4):3371–3387, 2017.

[8] Niken Dwi Wahyu Cahyani, Ben Martini, Kim-Kwang Raymond Choo,and AKBP Al-Azhar. Forensic data acquisition from cloud-of-things devices: windows smartphones as a case study. Concurrency and Computation: Practice and Experience, 29(14), 2017.

[9] Darren Quick and Kim-Kwang Raymond Choo. Pervasive social networking forensics: intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications, 86:24–33,2017.

[10] Kaspersky Lab: One in Every Six users suffer loss or theft of mobile devices.

[11] Adi Shamir. How to share a secret. Communications of the ACM,22(11):612–613, 1979.

[12] Lein Harn. Comments on'fair (t, n) threshold secret sharing scheme'.IET Information Security, 8(6):303–304, 2014.

[13] Lein Harn and Miao Fuyou. Multilevel threshold secret sharing based on the chinese remainder theorem. Information processing letters,114(9):504–509, 2014.

[14] Andrew C Yao. Protocols for secure computations. In Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on, pages 160–164. IEEE, 1982.