THREE TIER AUTHENTICATION MODEL FOR ENHANCING SECURITY

Research Report

Kaavya Rekanar

9405217184

kare@student.bth.se

Biswajeet Mohanty

9303167754

bimo15@student.bth.se

I. GROUP MEMBERS PARTICIPATION

The group members participated in idea creation and in report writing with the following amount of involvement:

Group Member	*Idea Creation*	*Report Writing*
Kaavya Rekanar	50%	50%
Biswajeet Mohanty	50%	50%

***Abstract*— Security is a very important aspect in every sphere of life [1]. With the advancement of information and technology, protection and security of data from cyber criminals has become a crucial aspect. This raises a question on the security aspects provided by the existing user-authentication methods. A survey was conducted for this report, to gather information from users about the security issues they face and to understand if they were satisfied and felt secure with the existing authentication methods. Analysis of the survey showed us that most of the users expect for a better and robust security system. This survey also helped us to understand the impeding concerns of the users and device a new authentication method.**

II. INTRODUCTION

A. Background:

Authentication is a process used by users to confirm the account belonging to him/her. It is a key requirement for securing today's user specific sensitive data. But, traditional Username-Password system has always been plagued by security problems [3]. Each user account needs a set of username and password for authentication. Increasing number of accounts makes it difficult for a user to remember usernames and passwords for each profile. So, users prefer to maintain a single unique username-password or something, which is easier to remember for all the accounts. This in turn has helped the hackers in penetrating into the users' account and retrieve sensitive information. Hackers find it easy to crack these types of accounts with the help of existing hacking tools available over the net. This has resulted in widespread discontentment and hatred for the username-password system [2].

Enormous efforts are now being taken to systematize the knowledge in a better manner regarding both passwords and its alternatives [4]. Many newer authentication methods are now being proposed which include One-time-password, and biometrics as additional security layers over the traditional username-password authentication system to enable them to be breach free and user friendly.

B. Problem:

We recognize that there are many loopholes in the methods available, which are prone to breakdowns and loss of data. This is a concern for the users and large organizations whose data cost over millions. Recently many security issues have been reported. Hackers penetrate into the users system seeking valuable information with ease by finding the loopholes in the existing system and in some cases it is due to the negligence of the users for not keeping a safe password. Existing user authentication methods make use of tokens (passwords) with OTP (One time password) used as an extra layer of protection. OTP increases the security level but there exists some loopholes in the method as well, which might be cracked into. This flaw in the system needs to be looked upon and a more secure system needs to be invented, resisting hacker's attack. Biometrics has its own share of shortcomings, which makes it imminent for devising a new robust authenticating mechanism.

C. Objectives:

The main objective of this report is to identify current security shortcomings and provide the users with an authentication system, better than the existing one, which is much more secure, user friendly and less susceptible to attacks. A research plan was designed to systematically deal with the current situation. Research questions were framed and adequate research was done accordingly to answer each of the research questions. A survey was also conducted for understanding the users' perspective on the existing methods of authentication and devising a new approach to provide the users with a trustworthy authentication system keeping their feedbacks in mind.

D. Methods:

A research plan was chalked out as per which multiple methods were implemented in order to build the research

report. A survey was conducted, collecting information from the users on their views regarding the existing authentication method. The survey was conducted by creating a questionnaire for the users as shown in Appendix A. This form was sent to the users over the web and their feedback were recorded and analyzed. Many users provided us with some excellent new ideas. This helped us in experimenting with different test cases/methods. At last, these methods are analyzed, adopted and the research questions are answered accordingly.

E. Contribution:

Existing authentication methods have many loopholes, which needs to be dealt with, as soon as possible, without causing loss of data to users and organizations. This report presents a new authentication mechanism consisting of passwords, OTP (one time password), and digital signatures. The conducted survey helped us in acquiring information about the problems faced by users in authenticating themselves. The survey also helped us in assessing the satisfaction level of the users with respect to the existing authentication methods. This motivated us in creating a new authentication method, keeping in mind the disadvantages of the existing authentication methods.

III. BACKGROUND AND MOTIVATION

Literature search has been done and relevant information corresponding to user authentication methods was considered from the papers and articles, by searching the online databases. In these papers, researchers have proposed many user authentication methods, which mainly makes use of the trending method of authentication that is "Biometrics" and also some methods make use of the persisting authentication methods that is tokens (passwords) and OTP (one time password).

The different approaches used by the researchers for authenticating an user were steganocryptographic approach [5], SSL and 3-D secure protocol [6], keystroke biometrics [7], Elliptic Curve Cryptography with Biometrics [8] etc..

The different methods used in the above mentioned approaches were cryptography [5], steganography [5], SSL protocol with fingerprint [6], 3-d secure protocol with iris [6], keystroke biometrics [7], OTP using ECC (elliptic curve cryptography) [8], RSA algorithm, DSA algorithm.

Cryptography is a process of securing the messages sent and received by encrypting and decrypting the messages used in secure communication between two parties. It makes use of a key for encrypting and decrypting the messages. The various cryptographic approaches are data encryption standard (DES), the advanced encryption standard (AES), the Rivest-Shamir-Adleman (RSA) method, and the Pretty Good Privacy (PGP) method. [5]

Steganography is the science of concealing information within different types of media, such that only the sender and the receiver are aware of its exact location [5]. Communication path is secured along with the messages sent, overcoming the burden of cryptography.

Secure socket layer (SSL) protocol is a cryptographic protocol, which is used in secure communication of messages.

3-D secure protocol provides an extra layer of security for online transactions made using credit cards and debit cards. It is an XML (Extensive Markup Language) based protocol.

Keystroke biometrics [7] uses the natural typing pattern of a user for authentication. It makes use of multiple sensors to gather information of the user. Artificial neural network is used to model users behavior and Alternate verification code (AVC) is used if the user is unable to login using keystroke biometric.

ECC (elliptic curve cryptography) [8] is an alternative to RSA algorithm due to its better performance than the later.

RSA (Rivest-Shamir-Aldeman) is a cryptographic method to encrypt and decrypt messages. It uses two keys: public key and private key. Biometrics is implemented using RSA algorithm.

DSA (Digital signature algorithm) is used for digital signatures. It uses two phases in its execution. First phase makes use of the cryptographic hash function and the second phase makes use of public and private keys.

OTP is generated, by executing the HOTP algorithm (HMAC based One Time Password algorithm) [9]. It makes use of the HMAC (Hash Message Authentication Code). HMAC uses a hash function and a key to calculate the message authentication code (MAC).

These methods have proven to be very useful in protecting the data, but when it comes to robustness of the authentication methods, there is lack of consistency in performance of these methods. Recent cyber attacks have proven that these methods have loopholes through which the hackers break into the system and perform malicious activities. These loopholes need to be focused on and dealt with to make a more robust authentication method, which is main motivation for deciding this topic.

IV. RESEARCH DEFINITION AND PLAN

A. Research Objectives

The main objective of our research is to provide an alternative solution for the existing authentication methods, which is much more effective and simple, that is user friendly and robust in its nature. For this, first we need to analyze the

existing authentication methods and find the drawbacks of these methods. And, then we need to figure out the factors affecting the existing methods. At last, find a solution to all these problems by creating a new alternative method. But before all this, we need to know the interests of the users regarding the existing authentication methods and whether they need a change in the existing authentication methods. We conducted a survey to identify the need of the users and then work accordingly to form the research questions and answer them for preparing the report.

B. Research Questions

RQ1: What are the flaws in the existing methods of user authentication?

Motivation: We figured out the problems faced by users while authenticating themselves, using the existing methods. And, then decisions were taken to tackle these problems.

RQ2: Can the combination of password, OTP and digital signature prove to be an enhanced user authentication method?

Motivation: By finding the loopholes in the existing methods, a new method can be implemented by adding an extra layer of security to the existing methods. Using digital signatures as an additional layer will help in securing data, as it increases the level of security.

C. Research Methods

Research questions helped us in selecting the proper research methods for conducting the research. These methods were chosen in a way that it would help us in building a new authentication method consisting of three layer authentication, that is password as the first layer, OTP as the second layer and digital signature as the last layer. This additional layer will help in providing extra security, which will prove to be a problem for the hackers to break into the system with ease.

Survey method and experimentation were both used for our research. Survey was mainly conducted to know the interests of the users regarding security and whether they were satisfied with the existing authentication methods due to the recent security attacks, which caused loss of privacy to many users. Suggestions were also taken from the users, which helped us in selecting the methods of research.

Method used for answering RQ1:
The method chosen here is literature review. Literature search was done from the online databases for finding the relevant information about the various authentication methods. A systematic literature review was prepared to find the flaws in the existing authentication methods. We try to solve these problems by creating a new authentication method, which uses a three-tier authentication method (password, OTP and digital signature).

Method used for answering RQ2:
The method chosen here is experimentation. We build a new authentication method consisting of three layers as shown in figure 1. Passwords act as the first layer, where the user needs to type the pin to authenticate himself/herself. Next layer has OTP, where a user gets the pin through message/mail. This pin is valid for only a single session. Last layer consists of digital signature, where the user needs to sign on a digital pad for authenticating. This added layer of security will help in protecting data from cyber attacks, as breaking into this system will a very time consuming and troublesome process.

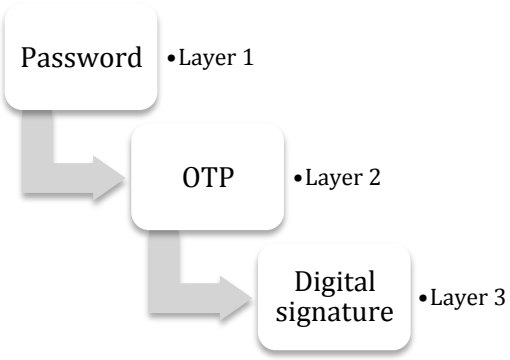


Figure 1: Three-layer authentication model

D. Unit of analysis

Two different approaches were chosen for constructing our report, the survey approach and the experimentation approach. Users formed the Unit of Analysis for both the approaches but the key performance drivers differed for them.

Unit of analysis for survey method:
Unit of analysis in this method are the users, as user perspective is important for us to figure out their understanding towards security and their responsibility to secure the data from their side as well. Here User perspective was the chosen driver.

Unit of analysis for experimentation method:
Here too Users formed the Unit of analysis but the drivers were much more objective as compared to the survey method.

i. Time, is the first driver for this analysis. There is a restricted amount of time available to get access using the new authentication method. This may prove to be very effective, as the hacker has a minimal time to invade the system.

ii. Cost, is the second driver for the analysis. Compared to the biometric method, digital signature is a very cost effective way of authentication and even the hardware

for implementing digital signature is cheaper than the hardware used in biometrics. This makes the new method of authentication to be affordable to users.

iii. Lastly, simplicity in usage formed the last driver of the analysis. The new method was meant to be simple to implement and remain user friendly.

E. Data collection

Data collection for survey method:
Data collection is done by, preparing a questionnaire for the users. The data collected over here helps us in selecting proper techniques to tackle the problems that user face while authenticating themselves.

Data collection for experiment method:
Data collection is done by, searching the relevant papers from the online databases. Analysis of these papers is done and then the papers relevant to our topic were considered. These papers formed the basis for answering our RQ1. These results help us in solving the problems faced by users in securing their data, by constructing a new authentication method as answered for RQ2.

F. Data Analysis

Data analysis for survey method:
Answers provided by the users through the questionnaire were analyzed. User interests were understood and then important suggestions were taken into consideration while building the new authentication method.

Data analysis for experimentation method:
Searched papers were analyzed. This was done to find the relevant papers for our topic. Most recent papers were chosen for analysis, which would help us in gaining knowledge about the on going researches and make our research to be up-to-date.

V. RESEARCH OPERATION

A. Operation

Research operation was done by, carrying out steps as shown in figure2. This operation started with a thorough review of the ongoing researches in the field of security. Then relevant articles were collated from the online databases to prepare the systematic literature review (SLR). This SLR helped us in identifying the flaws in the existing system and identify the prime requisites for the new system. This motivated us to rectify the flaws and provide the users with a more enhanced version of authentication method. The next step was to transform our motivation into reality.

The research proposal was prepared based on SLR. This was done to rectify the flaws found in the existing system using the SLR. These gaps/flaws were correctly addressed in the proposal, so as to make a much enhanced and robust authentication method. After the feasibility of the proposal, the actual research was carried out. This proposal helped us in assessing the flaws in the system and it gave us a direction to tackle it. Actual research started with the process of selecting appropriate research methods. We have used both survey method and experimentation method for conducting our research.

Survey method is mainly carried out for analyzing the knowledge and understanding of the users about the security of data. This also gave us a brief idea of the satisfaction levels of the users with the existing authentication methods. Some users also showed interest in giving their suggestions for betterment in the existing system. The survey method was carried out by, preparing a questionnaire for the users. The feedbacks were recorded and then they were analyzed. These feedbacks helped us in carrying forward the proposal to the next level, that is, carrying out the experimentation method.

The experimentation method started by considering the three different authentication methods-password, OTP and digital signature. Coding was done for each of the methods. Password was coded by using DES algorithm, OTP uses the HMAC for one-time-passwords, and digital signature is coded by using DSA algorithm. These methods are combined together to form a new authentication process. A three-tier process starting with password, then OTP and at last the digital signature is constructed. This new method is checked for its functionality by, storing the data in the database and making the new authentication method to work for granting access to the user.

This completes the process of our research for preparing a more enhanced, simple, reliable, and robust authentication method.

Appendix A and Appendix B provides the snapshots of the survey and experimentation method respectively.

B. Quality Assurance

Quality assurance for the survey method is determined by considering the feedbacks from users, which were related to our research topic. These feedbacks were judged and relevant data was considered. Important advices from users were also considered for preparing the report.

Quality assurance for the experiment method is determined by choosing the authentication methods (password, OTP and digital signature), which have already proved to be successful in securing the data for decades. These methods have been the base for securing the data and combining the three methods will boost the authentication to be more enhanced.

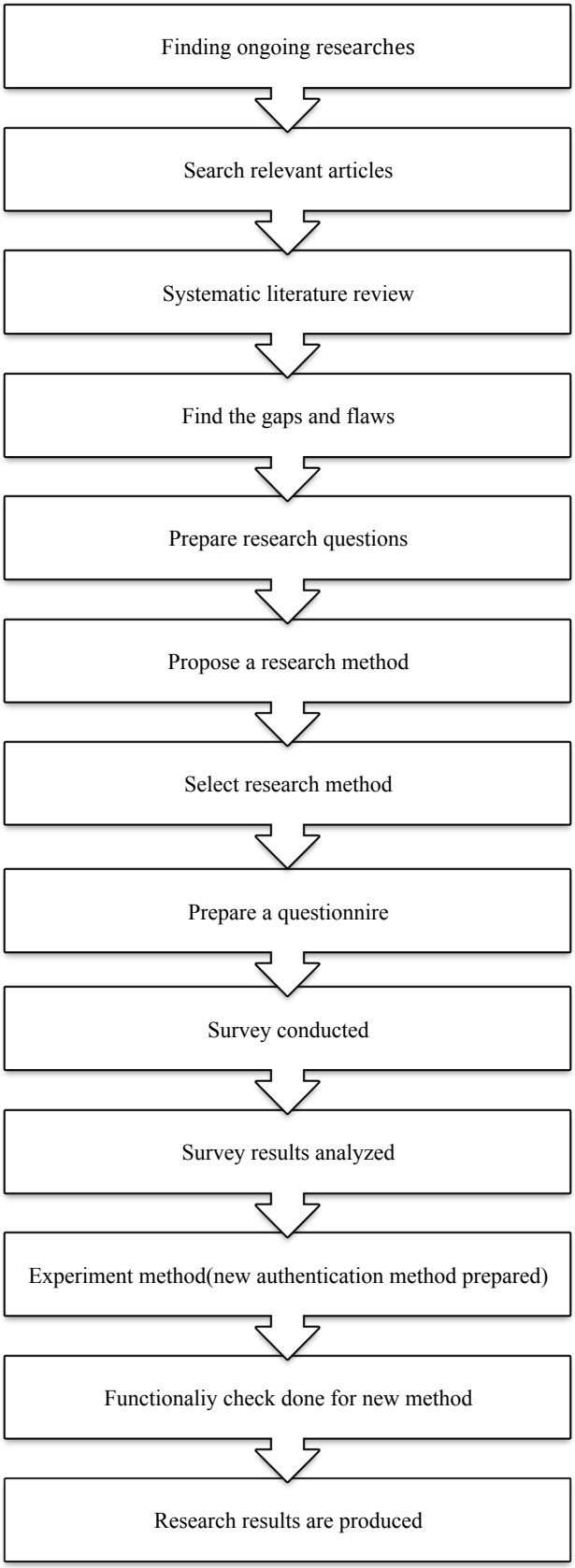


Figure 2: Research operation

VI. DATA ANALYSIS AND INTERPRETATION

Survey method:

A questionnaire was prepared and was sent to a total of 100 fellow students and lecturers on the Its-learning portal. We received 38 responses for the survey conducted. Out of those 38 responses, 13 responses were effective in their responses answering all the asked questions, and the other 25 members didn't answer all the questions in the questionnaire. This helped us in calculating the response rate and the effective response rate. The response rate yielded to be 38% and the effective response rate yielded to be 13%. The other 25% of the users just participated in the survey as shown in Table 1.

Table 1: *Respondents for the survey*

Rate	No of users	User percentage
Total	100	100%
Response rate	38	38%
Effective response rate	13	13%

These responses were very helpful in preparing our research report. The responses were studied and analyzed, which helped us in interpreting the attitude and concern of the users pertaining to security. Most of the users were satisfied with the existing authentication methods and some users were satisfied in a halfhearted manner as shown in Table 2.

Table 2: Satisfied users with the existing authentication methods.

Users	Satisfied	Partly	Not satisfied
No of satisfied users	20	11	7
% of satisfied users	52.6%	28.9%	18.5%

The effective responses provided us with some suggestions pertaining to the authentication methods. Most of the respondents wanted for a change in the existing system of authentication and they thought that a new authentication method consisting of a three layer authentication process (password in the first layer, OTP in the second layer and the third layer consisting of digital signature) could be a solution to tackle the problems faced by the users in securing their data as shown in Table 3. This motivated us in creating the new authentication method.

Table 3: Users thought about the new authentication method to be helpful

Users	Yes	May be	No
No of users	15	18	5
% of users	39.5%	47.4%	13.1%

Experiment method:
Data was gathered by searching in the online databases. This data was analyzed and systematic literature review was prepared. SLR helped us in finding the flaws in the existing authentication methods and demanded for a change in the system. This SLR forms the base for answering our RQ1.

The new authentication method is prepared and the performance of this method needs to be examined. This new method needs to be examined on a large scale and then the results can be derived to support our research. Theoretically, the new method can overcome some of the problems faced by the users, using the existing methods of authentication. Theoretical and practical results can vary from each other, which makes the consideration of theoretical results to be vague. Further research needs to be carried out in order to compare the performance results of the new authentication method with the existing ones, which would help us in answering our RQ2.

VII. DISCUSSION

A. Results

We conclude the following from the data we have analyzed:

i. Users have the tendency to use the same password for all the accounts they possess. This is due to the trouble faced while remembering all the passwords for the different accounts they possess. This helps the hackers in breaking into the system with ease.

ii. Most of the users are satisfied with the existing methods of authentication, despite of there being recent attacks, where the privacy of the users has been put on risk.

iii. Many users who understood the need of security, wanted for a change in the existing authentication methods with a more enhanced method, which would reduce their concerns in securing data.

iv. New authentication method might overcome the problems faced by using the existing methods, as there is an added layer of security, which may prove to be problematic for the hackers to break into.

v. Further research needs to be carried out to find the practicality and behavior of the new authentication method in the real world.

B. Threat to validity

i. **Time restriction** reduced the scope of the research, which might influence the outcomes of our research.

ii. **Proper programming language** is preferred by, the writer, according to his/her convenience and knowledge about the programming language.

iii. **User bias** was avoided by maintaining the integrity of the user.

iv. **External validity threat** is limiting the scope of our research due to the restriction of time, which might affect our research outcomes.

v. **Internal validity threat** is the execution of codes and programs required to implement the new authentication method.

vi. **Construct validity threat** is avoided by choosing the algorithms, which are in use from decades and have proven to be successful. And then the three-tier authentication method is implemented on a real world example.

VIII. SUMMARY AND CONCLUSIONS

Every person and every organization have their personal data, which needs to be protected. Security to this data is provided by, using many authentication methods. But, with advancement of technology, the scare of loosing this data is also increasing simultaneously. There is an imminent need for a robust and effective authentication method, which can outperform the existing authentication methods by overcoming the disadvantages of those methods. For this, we have devised a new three-tired authentication method.

We have used both survey and experiment method for our research. Survey method is used to find the satisfaction level of the users regarding the existing authentication methods in use and also, whether the users wanted for a change in the existing system with our new system. In the experiment method, a new authentication method is prepared. This method consists of a three-tier model, that is, password, OTP and digital signature. This method is prepared to overcome the difficulties faced by users.

Security remains the prime concern of the users today. New authentication methods are being proposed by the researchers, due to the ever growing cyber attacks. Further research for a robust authentication method is being carried-out as the scope in this field is very vast.

IX. REFERENCES

[1] Pura, M.-L.(Dept. of Mil. Inf. & Math., Mil. Tech. Acad., Bucharest, Romania); Patriciu, V.-V. “Security analysis of robust user authentication protocol”, *Proceedings 2010 8th International Conference on Communications (COMM)*, p

457-60, 2010.

[2] R. Morris and K. Thompson, "Password security: a case history," *Communications of the ACM*, v 22, n 11, p 594-7, Nov. 1979

[3] A. Adams and M. Sasse,"Users Are Not The Enemy," Source of the Document, Communications of the ACM, 42 (12), pp. 41-46, 1999.

[4] C.Herley and P.C.van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Security & Privacy*, v 10, n 1, p 28-36, Jan.-Feb. 2012.

[5] Tulpan D., Regoui C., Durand G., Belliveau L., Léger S., "HyDEn: A Hybrid Steganocryptographic Approach for Data Encryption Using Randomized Error-Correcting DNA Codes", BioMed Research International, 2013.

[6] Hosseini, Z.Z. (Dept. of Eng. & Technol., Payame Noor Univ., Tehran, Iran); Barkhordari, E., "Enhancement of security with the help of real time authentication and one time password in e-commerce transactions", *The 5th Conference on Information and Knowledge Technology*, p 268-73, 2013

[7] D'Lima, N. (Comput. Dept., St. Francis Inst. of Technol., Mumbai, India); Mittal, J., "Password authentication using Keystroke Biometrics"**,** *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, p 1-6, 2015

[8] Mahto, D. (Dept. of Comput. Applic., Nat. Inst. of Technol. Jamshedpur, Jamshedpur, India); Yadav, D.K., "Enhancing security of one-time password using Elliptic Curve Cryptography with biometrics for e-commerce applications", *Proceedings of the 2015 3rd International Conference on Computer, Communication, Control and Information Technology (C3IT)*, p 6 pp., 2015

[9] Yakut, S.; Ozer, A.B., "HMAC based one tıme password generator", *2014 22nd Signal Processing and Communications Applications Conference (SIU)*, p 1563-6, 2014

APPENDIX A: QUESTIONNAIRE

Replacement for existing User Authentication methods

This survey is conducted as a part of the course Research Methodology in Software Engineering at Blekinge Institute of Technology. This survey is to find out whether the users are satisfied with the existing authentication methods and is there any need to replace the existing user authentication methods with a better robust method for securing the data.

Thank you.

Survey Responsible:
Kaavya Rekanar (rekanarkaavya@gmail.com)
Biswajeet Mohanty (biswajeetm17@gmail.com)

Do you have any problem in remembering passwords?
- Yes
- No
- partly

How do you remember your passwords?
- Same password for all accounts
- Save on computer
- Sync to cloud
- Others

Are you satisfied with the existing user authentication methods(password, OTP, biometric)?
- Yes
- No
- Partly

If No, can you suggest a better user authentication method? (optional)

Can Digital Signature be a better user authentication method then the existing methods?
- Yes
- No
- May be

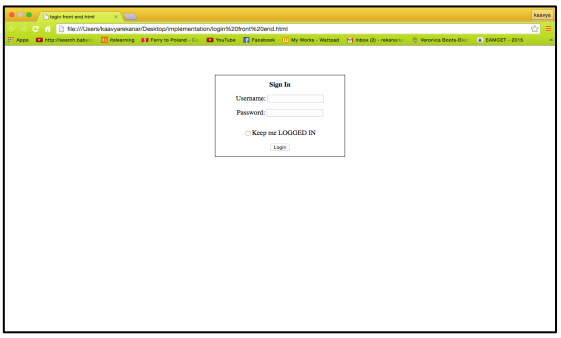
If No, Why?

Can a 3-step verification method(Password, OTP, and Digital signature) solve the existing user authentication problems of securing the data?
- Yes
- No
- May be

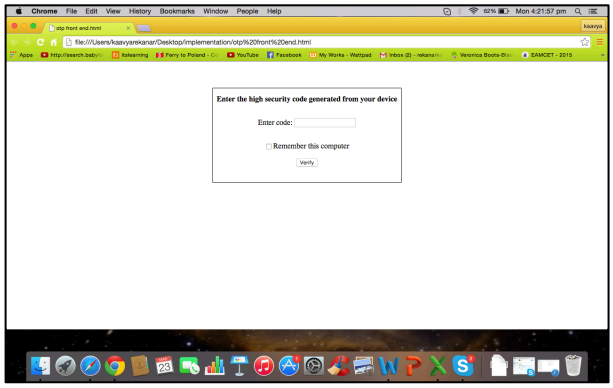
Comments on the survey

APPENDIX B: GUI Screenshots

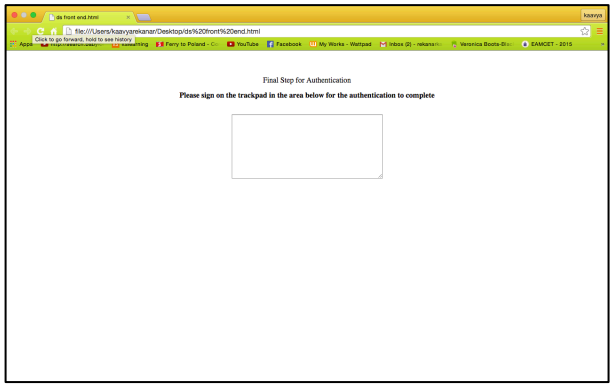
1) SECRET CODE MECHANISM (Password)



2) ONE TIME PASSWORD (OTP)



3) DIGITAL SIGNATURE



4) LOGGED IN