# Proposal for Research Methodology

PA2537: Research Methodology in Software Engineering and Computer science

Version NUMBER – March 1, 2015

| | | |
|---|---|---|
| Thesis | Tentative title | Three-tier authentication method for enhancing security of email system. |
| | Classification | User Authentication, Secret Codes, Biometrics, Digital Signature. |
| Student 1 | Name | Kaavya Rekanar |
| | e-Mail | kare@student.bth.se |
| | Social security nr | 9405217184 |
| Student 2 | Name | Biswajeet Mohanty |
| | e-Mail | bimo15@student.bth.se |
| | Social security nr | 9303167754 |
| Supervisor | Name and title | Samuel A. Fricker |
| | e-Mail | Samuel.fricker@bth.se |

## 1. Introduction

Insecurity in humans is a force which triggers specific human traits. Humans always make rational and irrational decisions to secure themselves, their surroundings and everything which holds dear to them. In the current age of Informational Technology, the meaning of security has escalated to a whole new level. IT has today integrated all the facets critical to an individual's identity and life, including his/hers social, financial and professional identity. Security is a very important aspect in every sphere of life [1] and User Authentication is the first security goal that can secure user specific information. This is truly the age of Information and data, and humans are critically vulnerable and threatened if their identity is compromised, their data stolen and used against them. This sense of insecurity in compromising sensitive data to the wrong hands has made user authentication an extremely critical step in IT security.

The most primitive method of user authentication, the secret code, today forms the basis of the concept of secret word or 'password'. This method of authentication is being used since decades and even used extensively in day-to-day life today as it is easy to implement and convenient. But, a breach into the knowledge of the secret word or password compromises the user authentication, as well as the data it is intended to secure. This renders the password system ineffective.
Knowledge of human biometric data being unique to each specific individual led to the next phase of advancements in securing data using biometric based authentication systems. This method though more effective than the traditional password based system, has its own bag of disadvantages. Paradoxically, the greatest strength of biometrics is at the same time its greatest liability. It is the fact that an individual's biometric data does not change over time: the pattern in your iris, retina or palm vein remain the same throughout

your life. Unfortunately, this also means that should a set of biometric data be compromised, it is compromised forever. The user only has a limited number of biometric features (one face, two hands, ten fingers and two eyes). And, if the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication. Also, biometric system installations are capital intensive, highly tedious and not completely precise and accurate. Erratic calibrations to these systems can cause unknown inconsistencies thus compromising an individual's identity and data.

Recent advancements in IT and telecommunications have led to a more effective and evolved means of user authentication called 'One Time Password (OTP)'. An OTP is a key that is valid for only one login session or transaction, on a computer system or other digital devices. One Time Password based two-factor authentication is much more secure than single factor authentication and is also cheaper. But, it is not secure enough to thwart the efforts of dedicated hackers, who have securely broken into highly secured government enterprises and defense systems with ease. OTP is vulnerable to threats as the actions (i.e. username and password) remain on the same device where the first layer of authentication occurs. This may help the hacker to acquire the information and cause malicious activities. OTP hacking uses the Key-Logger software technique. Now, if victim's computer is already vulnerable to key-loggers and other malwares, victim's keying-in details may be tracked and hackers may take actions based on victim's activity. In such a case, one-time password would be compromised.

The making and breaking of technology have been on par always. The One Time Password being considered to be an unbreakable technique in securing data proves to be as insecure as the previous methods that have been proposed and used for years. The need of the hour is of a method which could authenticate a user in a much more secure manner and in a cost effective way, when compared to biometrics and the secret code technique. Intensive research and development in building such a fool proof secure authentication system is hence imminent.

## Related Works

Sensitive information is stored on devices securely. This is made accessible to the user by authenticating his identity to avoid illegal access of data and also to provide security. The methods proposed till now are not sufficient enough in securing the information stored. New theories and techniques are studied and explained to overcome the problems of the existing techniques.

While conducting the Systematic literature revive, the article "The Quest to Replace Passwords" gave us an understanding of the existing user authentication techniques, which are not able to cope up with the advancement in technology and a fresh idea is required in authenticating the user in much more secure manner [1].

Various other theories were proposed. Samaneh Ghandali and Mohsen Ebrahimi Moghaddam, proposed a authentication technique based on image registration and fusion [2]. Other theories were based on the digital signature [3][4].

Our proposal is to add up the existing methods and create a new method, which consists of a combination of secret code technique, one time password and digital signature. The inclusion of digital signature adds up to an extra layer of security. It poses difficulty for a hacker to

break into a system that consists of triple layer authentication.

The table below shows the limitations that were observed after going through the related works and the consequences occur due to these limitations:

| **Limitation** | **Effect** |
|---|---|
| One time password is a two-way authentication, which is carried out on the same system. | The authentication code can be tracked by using key-logger software. |
| In biometrics images are sometimes misinterpret | Hacker can exploit this limitation and break into the system acquiring relevant information with less effort. |
| Digital signatures may be forged. | Signature forgery leads to gaining access to the system for acquiring information. |

## 2. Aims and Objectives

Aim: The aim of our proposal is to provide an alternative to the existing user authentication methods, there by increasing the level of security.

Objectives:

- Systematic literature review on "Replacement for passwords" is done to gain an idea of flaws in the existing system for authentication.
- Analyze the existing authentication methods for identifying the drawbacks.
- Identify the factors that determine the security level while using the identified methods during implementation.
- Propose a new authentication method for enhancing the security, by using three layers i.e. secret code, one time password and digital signature.
- Estimate the extent to which the existing methods are secure compared to the proposed method.

## 3. Research Questions

**RQ1:** What are the drawbacks in existing authentication methods in securing the data?

**RQ2:** How could the combination of secret code technique, one time password (OTP) and digital signature be used to enhance the security of data?

## 4. Method

Based on the drawbacks in existing authentication methods we try to overcome them by using a combination of secret code technique, OTP and digital signature, and evaluate whether this sort of implementation enhances the security. This implementation can be a solution to the problems discussed in RQ1.

We initiate the project by conducting a Systematic Literature Review (SLR) on 'Replacement for passwords'. It helped in getting an insight into various authentication methods used to secure the system.

*Method used for answering RQ1:*
Literature review is done for answering RQ1. From the SLR we came to know about the authentication methods and various drawbacks of these methods. These limitations are the gaps that we intend to answer in our study further.

*Method used for answering RQ2:*
RQ2 can be answered by conducting an experiment using key generation algorithms and respective software tools. The results of the experiment will convey the extent to which the new proposed method is secure compared to existing methods.

# 5. Expected Outcomes

We are aiming to find a better way to address the problems that are currently faced in securing the data. The following are the expected outcomes of the study to be performed:

1) Reason for using digital signatures to enhance security in the new method.

2) A new method that uses a triple layer authentication for enhancing security using secret code, OTP and digital signatures.

# 6. Risk management

The possible risks that might occur are as follows:

- **Analysis of real world example not done within specified duration:** The study will include a shortened version of the real world example, which might be uncomplicated and the problem representation might not be consistent.
  *Solution: Analysis is done, by giving the main importance to the elements that vary and rectify the elements that cause problems, considering that this element may vary in the real world example as well.*
- **Convenient programming language selection and use:** Programming language could be chosen by the writer, according to his convenience, expertise and as supported by the software tools used for executing the experiment.
  *Solution: Various programming languages are studied and then the suited one is selected to execute the experiment.*
- **Time restriction:** Shortened version of real world example is considered, as there might not be enough time allotted to the study and analyze the real world example.
  *Solution: Efficient time management among the team mates might help solving the problem, such that analysis of shortened version of real world example is done effectively.*

## 7. Time Plan

The time plan for implementing is as follows:

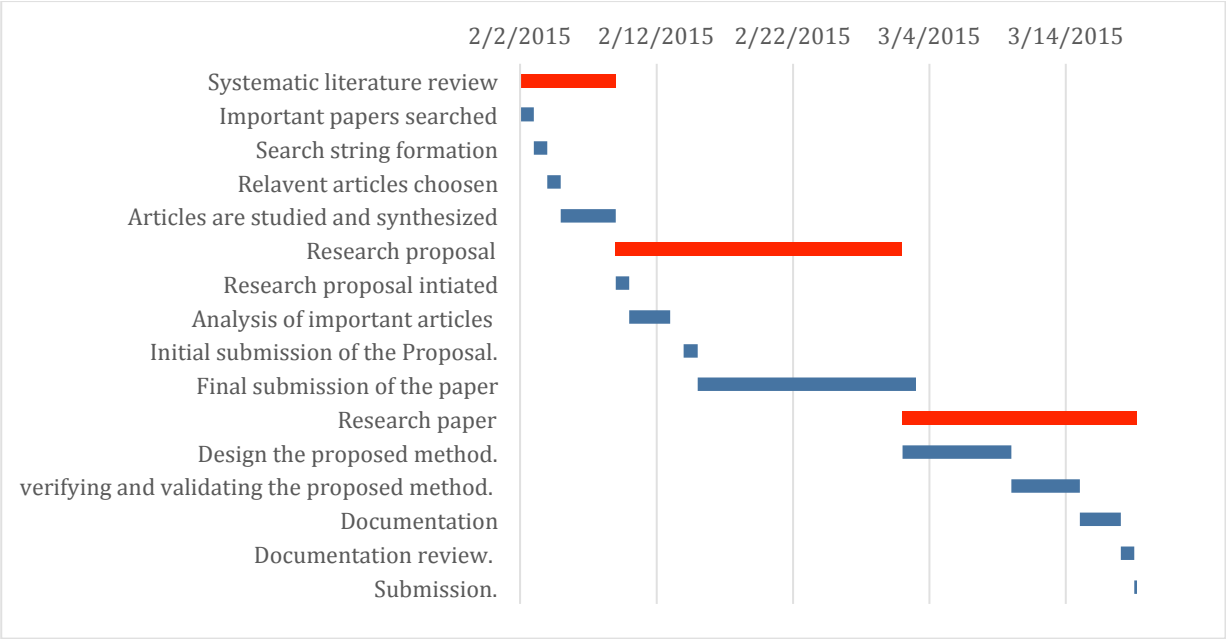


Figure 1: Gantt chart

## 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] Joseph Bonneau, Cormac Herley, P.C. van Oorschot, Frank Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", *2012 IEEE Symposium on Security and Privacy*, p 553-67, 2012.

[3] S.Ghandali and M. Ebrahimi Moghaddam, "Off-Line Persian Signature Identification and Verification based on Image Registration and Fusion", *Journal of Multimedia*, Vol 4, No 3 (2009), 137-144, Jun 2009.

[4] Meenakshi S Arya, and Vandana S Inamdar, "A Preliminary Study on Various Off-Line Hand Written Signature Verification Approaches". *International Journal of Computer Applications* 1(9):55–60, February 2010.

[5] Indrajit Bhattacharyaa, Prabir Ghoshb, and Swarup Biswasb, "Offline Signature Verification Using Pixel Matching Technique", Procedia Technology Volume 10, 2013, Pages 970–977, International Conference on Computational Intelligence: Modeling Techniques and Applications, (CIMTA) 2013.