

**Czech University of Life Sciences Prague**

**Faculty of Economics and Management**

**Department of Information Technology**



**Diploma Thesis.**

**Authentication in an information system**

**Supervisor:** Ing. Martin Havránek, Ph.D.

**Author:** BSc. Samson NTAMBARA

**© 2019 CULS Prague**

# CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

## DIPLOMA THESIS ASSIGNMENT

BSc. Samson NTAMBARA

System Engineering and Informatics

Thesis title:

**Authentication in an information system**

### Objectives of thesis

---

My diploma thesis is divided into two particular parts defined according to the authentication methods. The main goal is to implement a process of authentication in the information system for a constant user and for marketable solutions.

In order to achieve the main goal, the following partial goals have to be met:

- ✓ Reliable information source will be evaluated.
- ✓ Examine the current authentication method.
- ✓ Select a suitable authentication method according to the old one.
- ✓ Implement the chosen authentication method.
- ✓ Assess and making a conclusion.

### Methodology

The preparation of the diploma thesis will be preceded by analyzing and combining literature sources.

Based on different research, different authentication methods to secure information systems will be compared to make an overview of the current problem and any other relevant information.

In the theoretical part of this diploma thesis, all methods will be described, and in the practical part will be analyzing the significance of different authentication methods and why are they important.

The final application will be selected based on specific goals of individuals or groups of persons and will be described steps needed to achieve it. The proposed results will be summarized in the conclusions of the work.

**The proposed extent of the thesis**

60 – 80 Pages

**Keywords**

: encryption, authorization, authentication, Token, OTP, hashing.

---

**Recommended information sources**

- Huige W, Kefei C, Joseph KL, Ziyuan H, Yu L. 2018. Access control encryption with efficient verifiable sanitized decryption. *Information sciences*. 465(2018) 72-85.
- Dipankar D, Arunava R, Abhijit N. 2016. Towards the design of adaptive selection strategies for multi-factor authentication. *Computer and Security*. 63(2016) 85-116.
- Yimin G, Zhenfeng Z. 2017. LPSE: Lightweight password -strength estimation for password meters. *Computers and Security*. 73(2018) 507-518.
- Yun H, Zheng H, Haoran Z, Xuejia L. 2013. A new One -time Password Method. *IERI Procedia* 4(2013)
- Toan N, Nasir Memon. 2018. Tap-based user authentication for smartwatches. *Computers and Security*. 78(2018) 174-186.

**Expected date of thesis defence**

2018/19 WS – FEM (April 2019)

**The Diploma Thesis Supervisor**

Ing. Martin Havránek, Ph.D.

**Supervising department**

Department of Information Technology

Electronic approval: 15/10/2018

**Ing. Jiří Vaněk, Ph.D.**

Head of department

Electronic approval: 19/10/2018

**Ing. Martin Pelikán, Ph.D.**

Dean

## **Declaration**

I Samson NTAMBARA, hereby declare that except for references to other people's work which have been duly cited and acknowledged, this action research is the result of my own effort and that it has neither in whole nor in part been presented elsewhere.

In Prague on 27/03/2019

---

BSc. Samson NTAMBARA

## **Acknowledgements**

I hereby wish to express my appreciation and gratitude to my supervisor prof. Ing. Martin Havránek, Ph.D. for all guidance and teaching me during my work on this thesis.

I would like to thank my family and friends for supporting and encouraging me to write this thesis.

## **Abstract**

As the technology is a way of enhancing and improving both public and private services and makes it less stressful for everybody to access such services, Rwanda online transaction should also have an effective way of protecting and providing its service to the level of excellence. Bank of Kigali internet banking system should lead to a higher operational effectiveness expressed in terms of more successful fulfillment of security, the authenticity of their information, customer satisfaction, and quality goals. This research provides evidence that authentication in an information system will be a strategy that enhances customer satisfaction from a security perspective. The thesis will be analyzing the current situation that is working now in Rwanda. Rwanda online banking (mobile providers and banks) is quite hard to ensure security of the use of the internet banking where you need to log in on your online account by filling out only your username and static password information, it is realized as an issue of security compared to other developed countries especially in Europe.

The research, conducted by collecting the responses from the respondents showed that around 89% are not satisfied with the current technology, based on the outcomes, to ensure the security of the customers' accounts, One Time Password based email will be implemented to authenticate an information system for a constant user and for marketable solutions.

**Key words:** encryption, authorization, authentication, Token, OTP, hashing.

## **Souhrn**

Vzhledem k tomu, že technologie je využívána ke zlepšení a zkvalitnění veřejných i soukromých služeb a činí přístup k těmto službám jednodušší, měla by mít online transakce v Rwandě účinný způsob ochrany a poskytovat excelentní služby. Internetové bankovníctví banky Kigali by mělo vést k vyšší provozní efektivitě vyjádřené v podobě úspěšnějšího plnění bezpečnosti, autentičnosti informací, spokojenosti zákazníků a cílů kvality. Výzkum dokazuje, že autentizace v informačním systému bude strategií, která zvýší spokojenost s účinností bezpečnostních služeb pro společnost. Ve své diplomové práci budeme analyzovat současnou situaci, která nyní funguje ve Rwandě. Internetové bankovníctví Rwanda online (poskytovatelé mobilních služeb a banky) obtížně zajišťuje bezpečnost používání internetového bankovníctví, když se na svůj online účet přihlásíte pouze vyplněním informací o uživatelském jménu a statickým heslem, což je považováno jako bezpečnostní problém ve srovnání s ostatními rozvinutými zeměmi, zejména v Evropě. Výzkum ukázal, že přibližně 89% respondentů není spokojeno se současnou technologií, dle výsledků výzkumu, aby byla zajištěna bezpečnost účtů zákazníků, bude implementován email s jednorázovým heslem, aby potvrdil informační systém pro stálého uživatele a pro obchodovatelná řešení.

**Klíčová slova:** šifrování, autorizace, autentizace, Token, OTP, hash.

## Contents

Introduction .....	13
1.1 Aim and objective .....	13
1.2 Research questions .....	15
CHAPTER TWO .....	16
Theoretical basis .....	16
2.1 Identification, Authentication, and Authorization .....	16
2.2 Password.....	17
2.2.2 Standard strong-password vector.....	18
2.3 Cryptography .....	19
2.3.1 Symmetric key cryptography.....	19
2.3.2 Asymmetric key cryptography .....	20
2.3.3 Hashes and applications .....	21
2.3.4 MD5 .....	22
2.3.5 Digital signatures .....	22
2.3.7 Security services (CIA) .....	26
2.3.8 Cryptographic attacks.....	27
2.4 encryption algorithms.....	28
I.4.1 Data Encryption Standard (DES) .....	28
2.4.2 Triple Data Encryption Standard (3DES) .....	28
2.4.3 RSA .....	29
2.4.4 The Advanced Encryption Standard (AES) .....	29
2.5 Practical application of encrypting data .....	29



2.5.1 symmetric key encryption by using automatic security .....	30
2.6 Practical application of user authentication.....	31
2.6.1 Eyes free, the two-factor authentication method for smartwatches .....	31
2.6.2 StarSign Mobility Token as the next generation of USB security tokens .....	32
1.6.3 Strong mobile signature service.....	35
2.7 Multifactor authentication .....	36
2.7.1 Three elements of authentication .....	37
2.8 Mutual authentication technique.....	40
2.8.1 Quick Response Code .....	41
2.9 One Time Password .....	42
2.10 Security Token.....	43
2.10.1 Software token .....	44
2.11 Different types of two-factor authentication which are most used in networks .....	44
2.11.1. Challenge Response Authentication .....	44
2.11.2. Event Synchronous Authentication.....	44
2.11.3. Time Synchronous Authentication.....	45
2.12 Google Authenticator .....	45
CHAPTER THREE.....	47
Practical parts –Methods and selecting solution.....	47
3.1 Bank of Kigali.....	47
3.2 Web-based application .....	48
3.3 Design.....	48
3.3.1 Use case diagram .....	48
3.3.2 Activity diagram .....	49
3.4 Study area. ....	52

3.5 Technologies used .....	53
3.5.1 PHP .....	56
3.5.2 MySQL.....	56
3.6 Security side of the application.....	57
3.6. 1.One-time password .....	57
3.6. 2.Users side blueprint.....	57
3.6. 3 Database blueprint.....	58
3.6. 4. Server blueprint.....	58
3.7 Statistical analysis .....	58
CHAPTER FOUR.....	59
Practical part ---Results and implementation of the proposed system.....	59
4.1 Statistical analysis based Results .....	59
4.3.1 Software Specifications requirements.....	61
4.3.2 Hardware specification requirement .....	62
4.4 proposed system analysis .....	62
3.4.1 Web application .....	62
4.5 System implementation .....	62
4.5.1 Sign Up.....	63
4.5.2 Login .....	63
4.5.3 OTP received via email .....	64
CHAPTER FIVE .....	65
Discussion.....	65

## List of figures

Figure 1: Symmetric Encryption .....	20
Figure 2: Asymmetric encryption .....	21
Figure 3: Implement Forward-secure ID-based digital signature (FSIBS) with forwarding secure PKG into a surveillance system. ....	23
Figure 4: The StarSign Mobility Token .....	33
Figure 5: System components of Finnish mobile signature service, only the basic Internet-based service channels are shown .....	36
Figure 6: Conceptual authentication examples.....	37
Figure 7: Biometrics has retina and Fingerprint checking .....	40
Figure 8: QR Code architecture .....	41
Figure 9: RSA security tokens .....	43
Figure 10: use case diagram .....	49
Figure 11: User side activity diagram Source my own processing) .....	50
Figure 12: Server activity diagram .....	51
Figure 13: Frequency of respondents responding Yes, No and No idea .....	59
Figure 14: Number of participants per towns .....	60
Figure 15: number of participants based on their gender .....	60
Figure 16: Proportion of the all respondent .....	61
Figure 17: sign up screenshot .....	63
Figure 18: Login screenshot .....	64

## LIST OF ABBREVIATIONS

**AES:** Advanced Encryption Standard

**BK:** Bank of Kigali

**CA:** Certificate Authority

**CSS:** Cascading Style Sheet

**GB:** Gigabyte

**HTML:** Hypertext Markup Language

**IT:** Information Technology

**MD5:** Message Digest Algorithm 5

**MFA:** Multifactor Authentication

**OTP:** One Time Password

**PC:** Personal Computer

**PHP:** Hypertext Preprocessor

**PIN:** Personal Identification Number,

**PIV:** Personal Identity Verification

**PKI:** Public Key Infrastructure

**QR:** Quick Response

**RSA:** Rivest-Shamir-Adleman

**SHA:** Secure Hash Algorithm

**SQL:** Query Language

**VPN:** Virtual Private Network

**WLN:** Wireless Local Area Network

## **CHAPTER ONE**

### **Introduction**

Towards the end of the year 2016 in Rwanda, Computer and network security, authentication of the data and all information technology is increasingly more vital for our study to ensure the best reputation in secure service, contemplate and so forth. Almost in all online banking, “added layer of authentication” was proposed as support for the core of the protection of the users accounts information, like sign up and sign in to the online banking etc. but have not been implemented. Starting from this innovation in technology, BK (Bank of Kigali) was also surveyed their customers to ensure satisfaction in terms of security.

The targeted customers in this research were University of Rwanda students that has the main branch in capital Kigali and branches in the four provinces of Rwanda, as it will be described later in the research methodology. The main reason of survey was to find out the satisfaction level when they are using online banking. Data analysis was processed and also the technology of ensuring the authentication in an information system was proposed based on the results from the survey. Apart from this information, we will go after the solution of the authentication issues, which is also the case of the bank described in this thesis -Bank of Kigali -hereafter addressed just as the selected case study. Multi-factor authentication is commonly used in all developed countries to access online banking but in some developing countries, they are still using a static password to access their accounts.

Associating with an online service, for example, a banking web application regularly requires a certain level of the specialized refinement that not all Web clients have because of many internet attack like phishing (Hamdare, Nagpurkar and Mittal, 2014).

This research gave us a way of thinking about the countries where they are still using static password, the financial system must allow a customer to verify his account using his/her something he knows of a type of unknown or qualification (Hiltgen, Kramp and Weigold, 2006) .

The current system utilized by the web-based banking, the clients are therefore presented to hazard for this reason the bank cannot expect the authenticity for them, Authentication will be a critical issue during this research on selected bank.

## **1.1 Description of the selected Bank**

Bank of Kigali is one of the major banks that are currently working in Rwanda. It has branches in all over the thirty districts in Rwanda, the main customers of the bank are: students, foreigners who want to use a local bank and some public servants who are obliged to use BK because of the partnership with their organizations. Bank of Kigali's development in the course of the most recent five decades is a genuine story of versatility, diligent work and solid organizations dependent on Rwandan qualities.

## **1.2 Aim and objective**

### **1.Aim**

The main aim of the present study is to assess the current satisfaction of BK customers that uses online banking and implement a process of authentication in the information system for a constant user and for marketable solutions.

### **2.Objectives**

In order to achieve the main goal, the following partial goals have to be met:

**Reliable information source will be evaluated:** To get data to assess in this assignment, trusted information source will be evaluated where the participants will be the students of the University of Rwanda which has the branches across the country which will help us to get significance data and trusted sample to use

**Examine the current authentication method:** To identify the users of the online banking the current method of authenticating them in order to get access is used. The research was carried out to ensure the satisfaction of the users. The questionnaires were used and the data was collected and analyzed so that we should implement the accurate new technology to the system

**Select a suitable authentication method according to the old one:** From the previous, after analysis of the current technology drawback and also analysis to the target customers, we realized

that two-step to authenticate their account should be successful. this means that the user will use to log in by using the static password and the one-time password sent via Email.

**Implement the chosen authentication method:** After assessing and proposed the new technology, the remaining is to find a right way to implement it, Login system will be integrated into the current running system to enhance the security of the users. Obviously, there is something else entirely to Web Verification than simply utilizing it as a second factor but in our implementation we will start by improving login to authenticate the users.

**Assess and making a conclusion:** The final work will be the comparison of our implemented system and the current system, we will be emphasizing why we chose OTP as the best one among all the technology and why it should be successful, later we will come up with the conclusion to proposed results as solutions from the conducted research.

### **1.3 The Scope and research questions**

#### **1.The scope**

This work is emphasizing on the authenticating BK online banking system which is going to be used for effectively providing security to their customers' needs and services from them by providing to its clients to receive access to their accounts, the application will be able to respond to all devices like to be able to run on computers (Desktop and/or Laptop), smartphones and tablets.

#### **2.Research questions**

Is this research going to solve the problem of authentication in an information system?

Is OTP via email the best technology according to the target market? And why?

## CHAPTER TWO

### Theoretical basis

In the domain of computer, network or Authentication in information security, it is important to understand the meaning of the following terms and it is connected to guarantee security.

#### 2.1 Identification, Authentication, and Authorization

##### Identification

Identification occurs when the user of a given system applies or confirms an identity. A user has to be concluded with username, user smart card and any other particularity or uncommon that identify the user. It is used to know if users have access to a given system. It might be an eternal person who don't have access to it username (Sagar and Waghmare, 2016)..

##### Authentication

Authentication could be a mechanism in which the credentials given are compared to those on record in a database of authorized users' data on a nearby working framework or inside an authentication server or it is the ways of supporting an identity and it happens when a user gives correct credentials to prove their existence. For example, when a user gives the correct password with a username, the password confirms that the user is the holder of the username (Sagar and Waghmare, 2016).

The essential target of security in communication is to guarantee that just dependable vehicles are incorporated into the communication and that all recipients can verify their legitimacy, separately(Stübing, 2013)

In summary, the authentication support evidence of a requested identity.

There are several methods of authentication that we will be covered in this project which are:

Something you know, for example a password or PIN

Something you have, for example a smart card, CAC, PIV, or RSA token

Something you are, like by using biometrics



## **Authorization**

When a user is done with identifying and authenticating themselves, the remaining is to give them authorization according to their declared identity.

To have authorization, you have to prove first your user identity and password as authentication, otherwise, you will not have authorization.

Identification happens when a subject cases an identity, (for example, with a username) and Authentication happens when a subject demonstrates their identity, (for example, with a secret word). Once the subject has a demonstrated identity, authorization systems can give or square access to objects dependent on their demonstrated identities.

In general, **authentication** fix the problem of “Who said this?”, while **authorization** fix the problem of “Who is trusted to access this?”. (Aiash and Loo, 2015)

## **2.2 Password**

They are may be the foremost broadly utilized strategy for user authentication. Passwords are both simple to get it and utilize, and simple to execute. With these focal points, password-based authentication is likely to remain as a critical portion of the security for the predictable in the future. major weakness of password-based authentication is that numerous users tend to choose powerless passwords that are simple to figure. Addressing this challenge has been a dynamic and imperative investigate the area. An essential instrument for password security inquire about is that of probabilistic password models (password models for short). A password show allows likelihood esteem or value to each string. The objective of such a show is to surmise as accurately as conceivable an obscure password dispersion (Ma *et al.*, 2014)

### **2.2.1 Password authentication**

To have access to the protected network system, you have to prove your first line defense in that case, you will be having a specific authorization. To ensure security, it is important to have a password as an explanation of the existence of authentication.

To have access to the system, you will be asked to create a password to ensure security but most of the time we prefer to use the one that is easy to remember but which can be also easy one for hacker, to avoid this it Is important or recommended to create stronger password which is hard to

guess and also difficult to remember for the users as it has been applied in many systems by creating different measures and policies to a password in order to be accepted.

certain requirements are met by every password that password composition require are: 8 characters at least in length and at least from three of four character classes, to use this can help you to create a password which is difficult to guess.

The users to build their password, the length of it also can affect its creation by selecting different characters, such as digits, special symbols, and uppercase letters.

To know whether the password is stronger different computational techniques are used like password guessing to measure password strength for password meters.

By applying Lightweight password-strength estimation for password meters to design a competitive password strength evaluation method, which calculates password strength by calculating how much a given password is closer to the standard strong password in many ways, the false-negative evaluation says that this method is significant and suitable than other methods.

The given password is already stronger if the number of operations required to transform it into a stronger password are less. However, **a study probabilistic password model shows** that it allocates likelihood esteem to each string. Such models are valuable for inquiring about into understanding what makes clients select more (or less) secure passwords, and for developing secret word strength meters and secret word splitting utilities. Guess number graph created from password models are a broadly utilized strategy in secret word investigate. (Ma *et al.*, 2014)

### **2.2.2 Standard strong-password vector**

Two conditions that have to be satisfied by secure password generated by probability distribution are:

1. The password is randomly generated
2. The password is sufficiently long (e.g. at least characters in length)

We trust that if a secret word is adequately long and the diverse kinds of characters that make up the secret phrase string what's more, of equivalent likelihood then we view the secret word as solid. For instance, for an arbitrarily produced secret phrase with a length of  $L$ , and drawn from a letter in order of  $C$  characters, every secret phrase is of equivalent likelihood  $(C-L)$ . An assailant can't look the secret word space in plummeting request of likelihood, and would have no preferable methodology over to figure passwords at arbitrary, so the hunt cost is  $CL$ , in view of this proof,

we accept that a solid secret key ought to be arbitrarily created, and the secret word length ought to be more noteworthy than 16 characters.(Guo and Zhang, 2018)

## **2.3 Cryptography**

Cryptography is secret composing: secure correspondence that might be comprehended by the expected beneficiary as it were. While the way that information is being transmitted may be known, the substance of that information ought to stay obscure to outsiders. Information in movement (proceeding onward a network) and very still (put away on a device, for example, a disk or any other storing device) might be encrypted. (Sagar and Waghmare, 2016)

### **Encryption**

Encryption is a procedure that changes information into a secret code. It is one conceivable method for concealing information so that apart from approved clients none can peruse it. secret key or password is required to empower the unscrambling process. Encryption is the most dominant technique to decode information(Purnomo, Gondokaryono and Kim, 2017).

Encryption is commonly classified in two principal types.

- Symmetric: same key
- Asymmetric: different key

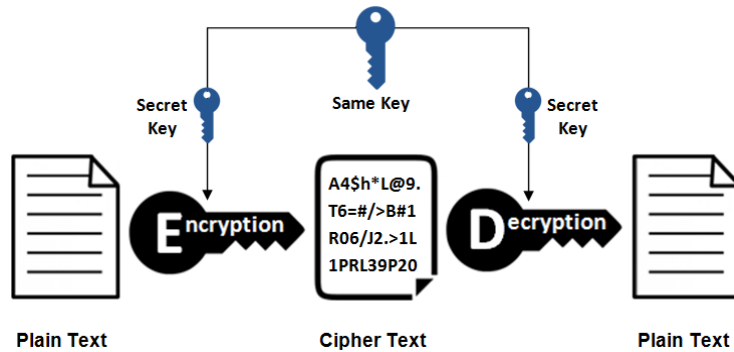
#### **2.3.1 Symmetric key cryptography**

Symmetric implies that opposite sides are in equalization or equivalent. Symmetric key cryptography is the utilization of one key to both encrypt and decrypt, and the encryption algorithm is in some cases the equivalent as the decoding algorithm (Dubrawsky, 2010).

It utilizes a secret key that can be a number, word, or arbitrary letters. All the parties, the sender, and the receiver need the key in their ownership. There is an issue with the idea of a secret key. Having the apprehension of this secret key can decrypt the message (Lozupone, 2018).

The huge issue that faces any symmetric key cipher is that their least complex utilize necessitates that the key is shared a "common key has to be shared"— between the two gatherings in the cipher. In a few detects, that will be normal, in light of the fact that the encrypted content is

itself a secret that is shared between the sender and recipients. however, if the sender has various recipients, he/she should create different keys to make certain that every recipient sees just those messages implied for him (Dubrawsky, 2010).



**Figure 1: Symmetric Encryption (Lozupone, 2018)**

### 2.3.2 Asymmetric key cryptography

A sender can encode a message utilizing the receiver's public key, and make sure that it must be decoded utilizing the related private key, which implies that the encrypted message can then just be perused by the holder of the private key. For whatever length of time that people in public key is trusted to be related with the proposed recipients, and the private key has not been uncovered, just the planned recipient will have the capacity to decrypt the message (Dalglish *et al.*, 2007) (Dubrawsky, 2010).

The trouble level of asymmetric encryption lies in the challenges of mathematical figuring in solving modulus for an extraordinary number. Because of the complexity of calculation of two different keys (public and private key), asymmetric encryption takes a considerable amount of time. In the other hand, symmetric encryption is less time expending since it uses the same key. symmetric encryption additionally has less complex calculation than asymmetric encryption. Lamentably, the secret key of symmetric encryption is less secure than asymmetric for the reason that the secret key is shared by the recipient and the sender. So it is vital to disperse the secret key of symmetric encryption safely. Most of the encryption framework utilizes the symmetric method since its calculation is single, straightforward and well acknowledged. The most imperative thing is that the generation of the secret key is basic and simple since it utilizes a similar key for encryption and unscrambling. The disadvantage happens when the interloper or intruder succeeds

stole the secret key so they can without much of a stretch open the message. Thus, the key dispersion ways.

ought to be finished with a protected strategy to make symmetric encryption secure(Purnomo, Gondokaryono and Kim, 2017) (Dey, 2012).

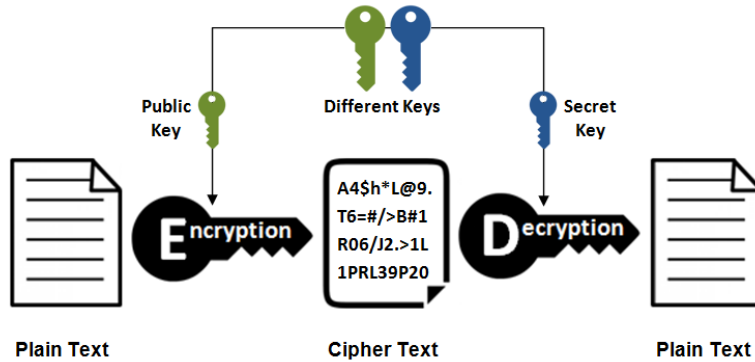


Figure 2:Asymmetric encryption (Lozupone, 2018)

### 2.3.3 Hashes and applications

Hash algorithms depend on scientific or mathematical “one-way function” these are functions that are moderately simple to ascertain going ahead, yet the reverse of the function is such a mind complex method, to the point that it is altogether harder to reverse the function than it is just attempting each and every conceivable input against the function to attempt and match its outcome.

To use them, we Care ought to be taken when utilizing a hash for calculating a digest of little pieces of information for passwords or credit cards, for example A third party with access to the hash codes might have the capacity to mount a bulk attack against the whole database at the same time, except if proper consideration is taken. Regularly, the addition of an arbitrary part, which is called "salt," to each bit of information being hashed will ensure against this sort of bulk attack that way, two users with a similar password won't have a similar hash. Putting away the salt with the hashed value is vital to guarantee that the hash can be recovered while checking the hash.

Regular more seasoned hash function incorporates Secure Hash Algorithm 1 (SHA-1), which makes a 160-bit hash and Message Digest 5 (MD5), which makes a 128-bit hash.

Shortcomings have been realized in both two MD5 and SHA-1; more current options such SHA2 are suggested (Dubrawsky, 2010).

### **2.3.4 MD5**

MD5 is the Message Digest Algorithm 5, made by Ronald Rivest. It is the most generally utilized of the MD group of the hash algorithm. MD5 makes a value of a 128-bit hash in view of any input length. MD5 has been very mainstream throughout the years, however, shortcomings have been found where impacts or collision could be found in a practical sum of time. MD6 is the most up to date form of the MD group of Hash Algorithm, first distributed in 2008.

### **2.3.5 Digital signatures**

It symbolizes a mix of cryptographic hashes and asymmetric encryption. Encrypting information with a private key does not ensure it against capture attempt, a public key should be open, thus it must be expected that your third party has a duplicate of it. So any information encrypted with a private key must be either public as of now, or secured in some other way. By encrypting data with a private key, in any case, plainly the record was encrypted by the proprietor of the private key. (Oh, Kim and Shin, 2018)

A digital signature is made by making a cryptographic hash of the record to be marked or signed and after that encrypting the hash with the private key of the signer. This has a few advantages like a solitary report (document) can be marked or signed by different gatherings; signature of any document is quick; a signature can be sent or held independently from a record or alongside it. (Zhou *et al.*, 2019)

A believed electronic signature is basic, as paper reports, for example, purchase request, checks, and contracts are progressively by electronic partners. Computerized signature is an essential part of numerous applications, for example, online business, home- banking, character, medicinal services, and physical access control administrations. programming frameworks are delicate to different assaults like Trojan horses and viruses which can be enacted remotely (M'Rahi and Yung, 2001).

The digital signature can be applied in many aspects of current proof in authentication, the protection of computerized signature (counting ID based ones) depends on the presumption that the private key is protected. The private key presentation refutes all signatures expressed by the

private key since a verifier can't notify whether a signature has been expressed previously or after the key introduction (means forged or produced). To realize the harm from the key exposure, forward security has been received to an identity-based signature (IBS). (Oh, Kim and Shin, 2018)

As of late, there have been a few explore on building forward secure ID-based signature where user private keys develop every single day (Al Ebri *et al.*, 2013).

A more particular application of Forward-secure ID-based digital signature situations is utilizing IoT and devices that use wireless technology for surveillance systems. nowadays, the internet of Things (IoT) innovation and technology of wireless communication permit large- scale surveillance systems. (Alsmirat *et al.*, 2017)

Devices used in IoT, advanced cells phones, remote or wireless CCTV, and remote cameras give recordings and pictures to a cloud server which are controlling data to that system of surveillance. (Oh, Kim and Shin, 2018)

The following is a figure explaining how it works

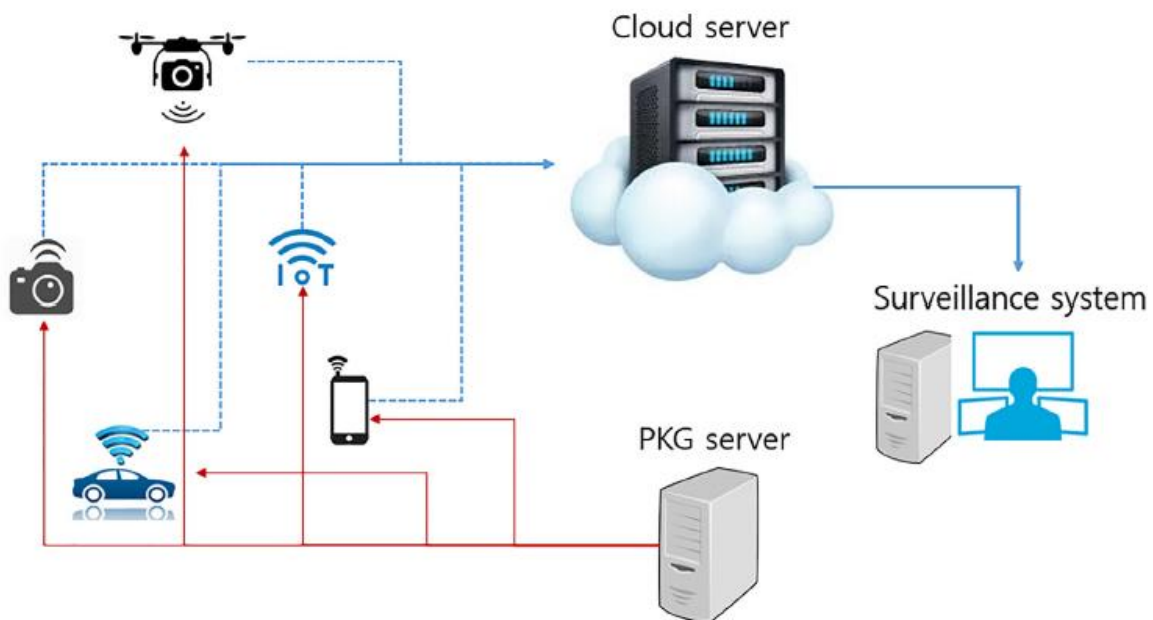


Figure 3:Implement Forward-secure ID-based digital signature (FSIBS) with forwarding secure PKG into a surveillance system. (Oh, Kim and Shin, 2018).

Even if the digital signature is considered as secure means of authentication, it has also many attacks, the certainty of vulnerabilities in innovation or technology and the non-negligible

likelihood of an event of security threats would make non-repudiation of proof hard to accomplish. by thinking about that it is of the most extreme significance to create fitting apparatuses and strategies to help with structuring and executing secure frameworks in a way that solidly advanced signature can be delivered by covering all the signature generation and verification stage(Hernandez-Ardieta *et al.*, 2013).

### 2.3.6 A digital certificate

Public key cryptography utilizes two keys and a progression of a scientific equation to scramble and unscramble advanced information of any sort. in general, one of these keys scrambles, the other one can unscramble. Practically speaking, the public key is made promptly accessible whereas the private key is secure and available just to the legitimate proprietor of the keys. Somebody wishing to communicate something specific that must be perused by the expected beneficiary will scramble the message utilizing the beneficiary's public key. Whenever gotten, just the proposed beneficiary can unscramble the message utilizing the comparing or identical private key. In extra, could digitally sign the message scrambling it with his very own private key, an activity which the beneficiary can affirm utilizing the sender's public key. This demonstrates the message really started with the expressed sender, while in the meantime guaranteeing that the message has not been altered, Digital certificate as a piece of PKI figure out the issues of criminals to present and claim public key as it belongs to them by validating the official of a public key to the personality of an individual or element. They permit check that public key does, in point of fact, relate to a particular person(M'Rahi and Yung, 2001).

Digital certificate records an arrangement of asserted characteristics about the individual, association, or PC distinguished in the certificate, and affirms those cases by the nearness of a computerized signature of a trustworthy body. It binds those cases to a public/private key match, with the goal that the user of the private key can be checked as the subject of the cases in the certificate. The subject of a certificate, the individual, association, or PC about which the certificate holds points of interest, is known as the **Subject**. The legitimate body that signs the certificate is known as the **Issuer**.



The standard for the computerized certificate is ITU-T X.509. X.509 is a standard for Public Key Infrastructure when all is said in done and covers different subjects, for example, **certificate revocation lists, and certificate path validation rules** (Dubrawsky, 2010).

Before a certificate can be broadly acknowledged as an exceptionally confided in verification of character, a way should be found to ensure them. Smart card offers this assurance by safely securing the digital certificate in a safe, removable medium, and making them difficult to reach to anybody however their legitimate proprietor, Without information of this certificate data, would be hackers and cheats are incapable to wrest or steal the legitimate owner's personality and utilization of it to access secure data or lead exchanges (M'Rahi and Yung, 2001).

### **2.3.6.1 Single and dual sided certificate**

**Single certificate:** single within the sense that they are free of any certificates other than their Issuer's, the terms **single** does not suggest single utilize, these certificates may be utilized for a single reason, or numerous reason, demonstrated by values known as "Key Usage" and "Enhanced Key Usage" values. The "Key Usage" value could be a set of bits that can be on or off.

**Dual-sided certificate:** it makes two key pairs and two certificates, the more regular term for this is **a dual key pair or dual key certificates**. One certificate and its associated key pair are utilized for encryption, the other is utilized for information signing (and non-repudiation) reasons. The key pair utilized for signing is created and kept by the user and isn't put away in any sort of key management system outside of the user's control. The key pair utilized for encryption might be supported up in a key management system for some other time recuperation(Hernandez-Ardieta *et al.*, 2013).

### **2.3.7 The weakness of the digital certificate**

The problem of using a digital certificate is because anybody with access to the private key Is accepted to have legitimate responsibility for authentication. Along these lines, while digital certificate can connect a character with the public key, the computerized certificate alone can't affirm that the individual exhibiting the certificate as evidence of personality, is really the legitimate proprietor(M'Rahi and Yung, 2001).

### 2.3.8 Security services (CIA)

Experts of data security depend on various diverse scientific classifications with the end goal to guarantee that they cover their system's security needs completely. One of the least complex such groupings accessible is CIA (confidentiality, integrity, and availability). The solution in security, for the most part, be evaluated with respect to how well it fits each, and all, of the following three classifications.

- ***Confidentiality***

Confidentiality delivers a system's capacity to keep data covered up from those individuals, systems, and procedures that are not intended to see it. Encryption is the way toward taking a document that is readable and delivering from it a document that is unreadable except if you have an appropriate key to decrypt it.

- ***Integrity***

Integrity delivers a system's capacity to guarantee and to demonstrate that data being handled is the after effect of the use of approved procedures to the first or original information. This means information can't be modified without agreement, or where it is modified (altered), in such situation, data modification will be detected, you have to care about an affirmation that information got are actually as sent by an approved element (no alteration, inclusion, deletion, or replay).

- ***Availability***

Availability talks about a system's capacity to exist and to give information to its affirmed users. Usually viewed as the inverted side of confidentiality if a document is encrypted and after that, the key is discarded, the document is unquestionably secret, however, it isn't accessible any longer.

- ***Non-repudiation***

It is a segment of data security that attempts to evaluate the likelihood that somebody could play out an activity and after that later claim that was not really them, but rather somebody utilizing their name without consent (it is a security against the refusal by one of the gatherings in a communication). A computerized signature can be utilized as evidence that the proprietor of the key related with the signature endorsed of, or if nothing else knew about, a document or an activity.

- *Key management*

To keep up availability it is vital to think about how to deal with the accidental loss of a key, or how to avoid it, and how to deal with a key's life cycle. Key management incorporates deciding if it is worthy for anybody other than the key holder to have the capacity to access the key. While the underlying response is to state "no," this disregards the likelihood that the key holder may intentionally or coincidentally crush the key. On the off chance that a key's purpose is to recognize the user, indicating utilization of the key is verification of the user's inclusion, at that point the appropriate response is certainly that nobody other than the user ought to access that key. Such a key ought to be put away just in the users' private certificate store, perfectly world on a smart card or other hardware device subject to anti-tampering security. The life cycle of such a key succeeds from creation utilize, renew, lastly to either revocation or lapse. It is the least complex of key life cycles (Dubrawsky, 2010).

### **2.3.9 Cryptographic attacks**

They are utilized by cryptanalysts to recuperate the plaintext without the key. please don't forget that recouping the key or steal the key is typically simpler than breaking present-day encryption. This is the thing that law requirement normally does when looked with a speculate utilizing cryptography: they get a look warrant and endeavor or try to recuperate the key.

#### **2.3.8.1 Brute force**

It creates the whole key space, which is each conceivable or likely key. Given enough time, the plaintext will be recouped or regain.

#### **2.3.8.2 Known plaintext**

A known plaintext assault depends on recouping and examine a matching plaintext and cipher text pair, the objective is to determine the key that was utilized. You might wonder why you would require the key on the off chance that you as of now have the plaintext: recuperating the key would enable you to decode different cipher texts encoded with a similar key.

#### **2.3.8.3 Meet-in-the-middle attack**

A compromise attack encrypts on one side, decrypts on the opposite side, and meet within the center. The most widely recognized attack is against **double DES** which encrypts with two keys in "**encrypt, encrypt**" arrange. The attack is a known plaintext attack, the aggressor has a

duplicate of a coordinating plaintext and cipher text and looks to recuperate the two keys used to encrypt.

#### **2.3.8.4 Known key**

The expression "known-key attack" is deceiving, in case the cryptanalyst knows the key, the attack is finished. Known key implies the cryptanalyst knows something almost the key, to lessen the power utilized to assault it. On the off chance that the cryptanalyst realizes that the key is a capitalized letter and a number just, different characters might be excluded in the assault.

#### **2.3.8.5 Differential cryptanalysis**

It looks for to discover the "difference" between relevant plaintexts that are encrypted, the plaintexts may contrast by a couple of bits. It is typically propelled like an adaptive-chosen plaintext attack, the assailant picks the plaintext to be encoded (however does not know the key) and after that encrypt associated plaintexts (Conrad, Misener and Feldman, 2014).

### **2.4 encryption algorithms**

Various encryption algorithms are accessible for utilizing, and more are made after some time, the followings are the list of some algorithms.

#### **2.4.1 Data Encryption Standard (DES)**

It utilizes a 56-bit key, and not surprisingly from something with such a little key size, it is a symmetric key encryption algorithm, asymmetric keys are typically in excess of a thousand bits long. It is called "block" encryption algorithm which is implying that it can encrypt in a block, for DES's situation, a block is 64 bits with also one block at any given moment. While square figures are not in themselves intended to scramble floods of information, it is conceivable to utilize what is known as a "method of activity" to encode a stream utilizing the square figure.

To encrypt a stream utilizing the block cipher, it is conceivable to utilize a "**method of activity**" because block ciphers are not in themselves intended to encrypt streams of information

#### **2.4.2 Triple Data Encryption Standard (3DES)**

It's an algorithm worked from three utilizations of the DES algorithm, as the name suggests, instead of the undeniable procedure of running the DES encryption three times, 3DES first encrypts utilizing DES and the first key, at that point, decrypts utilizing the second key, lastly

encrypt utilizing the third key. This strategy was picked in extensive part with the goal that a hardware usage of 3DES could be utilized to likewise actualize or implement DES by setting each of the three keys to the equivalent 56-bit value.

### **2.4.3 RSA**

*RSA*, stand for the names of its inventors Rivest, Shamir, and Adleman, it is a type of asymmetric cryptography algorithm furthermore, its quality depends on the gigantic trouble of factorizing two huge prime numbers. Appropriately, it requires much more time to prepare RSA algorithm in case the length of the key is much longer because of that a shorter key is utilized to diminish the handling time of RSA algorithm and double encryption to ensure the security of the cryptosystem (Hernandez-Ardieta *et al.*, 2013).

Since the RSA algorithm depends on scientific task especially exponentiation, it is conceivable to apply it to any size of the input. The RSA algorithm can be very moderate and, in similar, the RSA algorithm and most asymmetric key cryptographic algorithm will, for the most part, be utilized just to encrypt an interrelation of an appropriate symmetric key for a stream or a block cipher to be utilized for bulk encryption (Zhou *et al.*,).

### **2.4.4 The Advanced Encryption Standard (AES)**

AES can scramble and unscramble 128 bits of the block with 128, 192, or 256 bits of key(Quisquater, 2015).

It indicates a FIPS (Federal Information Processing Standards)-affirmed cryptographic algorithm that can be utilized to secure electronic information. The AES algorithm is a symmetric block cipher that can encode(encipher) and decode (decipher) data (NIST, 2001).

## **2.5 Practical application of encrypting data**

Data protection is accomplished in the present day cryptography by utilizing encryption. Symmetric key cryptography is basically capable of genuine user information assurance in different network protocols such as SSL/TLS and so on. The plan of such encryption algorithms has dependably been a standout amongst the most imperative research targets, where overwhelming cryptanalysis works have been performed to assess the security edge. Accordingly, investigate community is occupied with settling the security imperfections dependent on the cryptanalysis results. As of late, the thought of building the automatic security insurance plot

dependent on the neural system has been proposed. The encryption algorithm, which may be a neural organize is instep developed by machine amid the learning stage in an antagonistic environment (Zhou *et al.*, 2019).

### 2.5.1 symmetric key encryption by using automatic security

It begins by building an encryption scheme automatically without manually planning any concrete algorithms. In this new direction, all parties joining the computation are well prepared neural networks. In arrange to attain the security goal, the center thought of this modern innovation is to present the adversarial neural networks, and let it compete with the legitimate users.

all the members in this convention are neural networks including the adversary Eve. Each neural network has it possess purpose, which is anticipated to be accomplished after the training stage.

For example, a wants to send information to B through the communication channel and also there is the existence of third-party P who don't need to know the content of message, by introducing adversarial neural network information will propagate safely. the presenting of it is the key portion to create the communication secure from the spy or eves.

**Access control encryption with efficient verifiable sanitized decryption:** it empowers controlling both the composing users and the reading users.

Compared with other public key encryption systems like attribute-based encryption, which as it implemented access control on recipients (specifically it as it were empowers controlling what clients are allowed to decode), access control moreover executes get to control on senders (specifically it empowers controlling what users are permitted to encrypt). Generally talking, ACE is characterized related with not as it were a set of sender  $S$  and a set of clients  $R$ , moreover an access control policy  $P: S \times R \rightarrow \{0, 1\}$  which maps a sender-receiver combine to a Boolean output. Particularly, the arrangement  $P(I, j) = 1$  is utilized to demonstrate that sender  $I \in S$  should communicate with recipient  $j \in R$ , but  $P(I, j) = 0$  implies that sender  $I \in S$  is not permitted to communicate with recipient  $j$ . Additionally, in this algorithms, expect that all communications may be controlled by an intervention, named as the sanitizer, who is competent of changing a cipher text  $c$  scrambled by a sender to a cipher text  $c'$  of the same message by employing a sanitized key (or so-called change key). Uncommonly, other than taking after the protocol in the framework, the sanitizer may endeavor to get extra data by means of debasing other clients within the framework (Wang *et al.*, 2018).

## 2.6 Practical application of user authentication

### 2.6.1 Eyes free, the two-factor authentication method for smartwatches.

Tap-based User Authentication for Smartwatches by using this technology, the user will be permitted to tap a noteworthy or vital song (top-secret key) of their decision anyplace on the touchscreen to open their watch. A user will be confirmed depending on the top-secret word and in addition her physiological and social qualities when tapping.

Nowadays, smartwatches are ending up progressively well known to all because of their practical application in many daily lives to detect different perspectives like tracking health and fitness, as of late, smartwatches are being utilized to advantageously open PCs and also cars, at the other hand, the protection of the privacy is still doubtful. Indeed, the Pin and Pattern Lock strategies, in the case at all utilized, have numerous shortcomings. They can be defenseless to shoulder surfing, guessing attacks. From an ease of use perspective, authentication by using a Pattern or PIN may experience the ill effects of **the fat finger** issue because of the restricted size of the smartwatch screen. In addition, using biometric sensors mostly used like fingerprint scanners and camera for face acknowledgment or recognition on smartwatches might be troublesome given their little shape factors.

This technology gives a few attractive highlights. Initially, as far as security, its two-factor nature makes speculating, smudge and shoulder surfing attacks less applicable. Indeed, even for the situation where an enemy realizes and can rehash or repeat the song of an owner, regardless he needs to pass a behavioral and physiological check or verification which is altogether more troublesome. This security likewise applies to video attack, Second, as far as ease of use, it's without eyes highlight, enables the owner to tap anyplace on the screen, and thus takes care of the **fat-finger** issue as well as empowers owners to login attentively and profits owners or users with a visual disability. In various conditions like sitting and walking, this technology accomplishes execution like that of PIN and preterm lock techniques. It is imagined that this technology can be used as a lock and unlock technique or to protect matching between a watch and a telephone. It can likewise be shown as an alternative along the PIN or pattern for the user to pick dependent on the setting of usage or environment. For instance, clients can pick this technology to open or unlock their watch in an open place where the danger of being seen by somebody is high. What's more,

when they are at home or alone, they can open or unlock their watch with normal PIN lock and pattern strategy. (Nguyen and Memon, 2018)

### **2.6.2 StarSign Mobility Token as the next generation of USB security tokens**

USB tokens are getting to be progressively omnipresent or found everywhere within the computerized world. Obviously, smart card technology produced nowadays is presently sending their innovation in this frame factor for IT security-based applications. Utilizing USB tokens empowers helpful, secure access to corporate network and internet benefits by giving solid validation to security basic applications.

There's a developing number of USB smart tokens on the advertising, in this example, we are going to be using the offer from Giesecke & Devrient (G&D) as it is a company that gives security printing and other relevant activities like smart card, ...

**1. The StarSign mobility Token** is one of the up and coming age of USB security tokens, equipped for conveying most extreme versatility, adaptability, and security. Since applications and information stay on the token consistently, they leave no trace on the host PC and also there is no footprint.

**2. This technology has many advantages in the digital economy** like numerous employees spend a noteworthy sum of time on the move, going to clients and accomplice firms or attending traditions. this expanded mobility has a number of benefits as it can move forward their work/life adjust and can also offer assistance those who have to make a trip much of the time for work to keep in contact with the workplace. This has generally been encouraged by present day technology that is applied in communication, which enables individuals to remain in contact with their organization nonstop from any area. They can get emails, keep working while they are on the move utilizing their note pad PC, and remotely get to all information and applications on the corporate network. However, this extent of opportunity can cause some challenges with regards to the security of information interchanges, corporate information is frequently secret or have to be confidential what's more, should in this way be kept from getting into the wrong hands. Information likewise needs to be ensured against malicious control, regardless of whether it is on an organization note pad or another PC. USB security tokens give a helpful what's the more, secure arrangement. Much of the time, clients can abstain from conveying overwhelming notebook as tokens offer secure access to corporate systems or network kindness of strong authentication



techniques and take into consideration the use of programming applications straight, from the tokens.

### 3. The flexibility of the new version of the token

The new token has a measured plan as this is considered the most ideal approach to convey adaptability to clients in the advanced world. It uses four components:

**A smart card:** handles key organization furthermore, stores computerized personalities

**Flash memory** in the form of a standard: can be utilized to store applications what's more, both decoded and coded information.

**MicroSD card:** Swapping the MicroSD card is a speedy and simple way to evacuate all put away information, maintaining a strategic distance from the time-consuming require to erase data.

**A flash controller:** empowers the memory on the MicroSD card to be separated into multiple segments.

**A powerful processor** goes about as a stage for programming applications and for correspondence with a host PC.

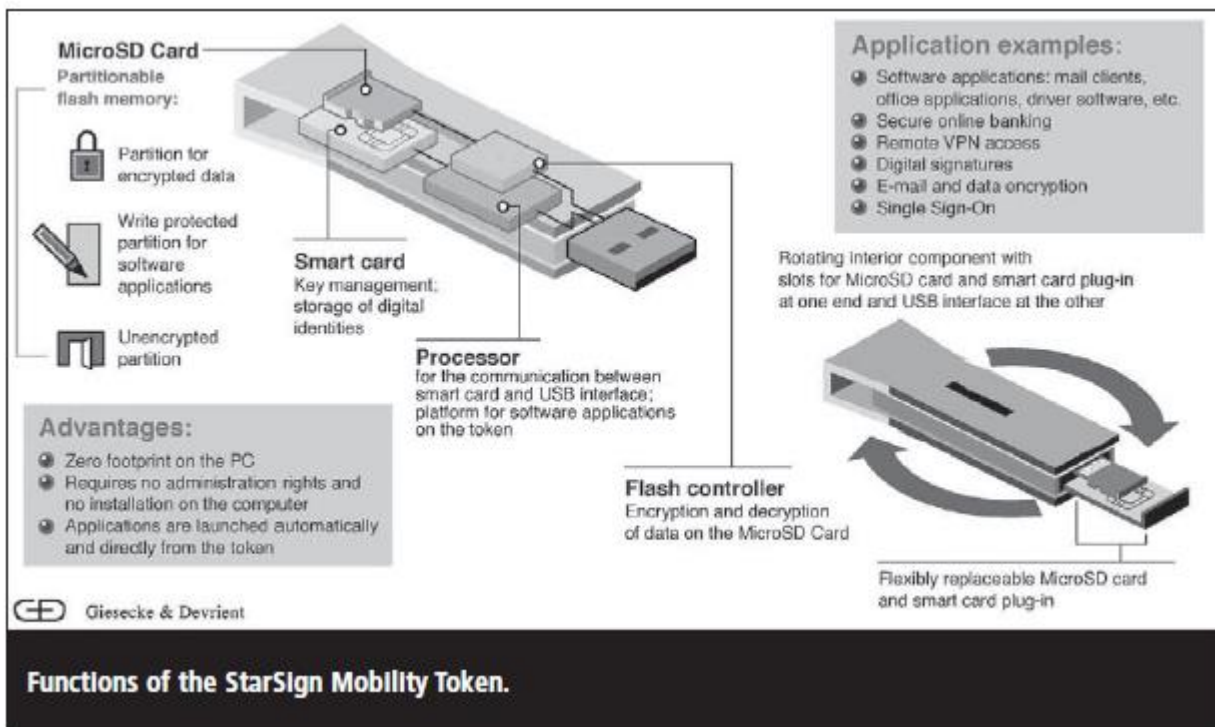


Figure 4: The StarSign Mobility Token (Frischat, 2008)

## **4.Application**

Regularly, frameworks integrators execute the USB token for two-factor authentication as some portion of their security arrangements. On the other hand, partnerships, especially bigger ones, do the usage themselves at home.

The USB token grants staff to take a shot at the move utilizing recognizable applications and screens consistently even without them possess note pad. By utilizing StarSign Mobility Token, it is likewise conceivable to utilize a solidified browser that dispatches straight from the token and incorporates a mechanism for secure authentication by implies of one-time passwords. This gives strong assurance against Trojans also, malware.

Correspondence over the Web/ internet by means of the host PC happens solely through with completely secured VPN channel. This guarantees indeed, even outside of the token there aren't any vulnerabilities.

### **4.1 The way in which this technology works**

The token is perfect with any Windows-based host framework. Up to this point, applications for portable sending depended on the host computer having the fundamental programming also, space to store information and execute programs. That has presently changed. The tall execution of the processor and the limit of the coordinates flash memory card (ordinarily somewhere in the range of 0.5 and 8 GB) imply that every single wanted application can run straightforwardly on the token. The token is perceived and initiated by the host PC utilizing direct attachment and plug-and-play functionality There is no have to be compelled to install any drivers. This moreover allocates with administrator rights; which staff frequently don't have for their system. Along these lines, a key prerequisite of IT divisions is satisfied especially inside bigger undertakings or enterprise, which are the essential focus for this sort of solution. Once expelled or eliminated, the token takes off no evidence on the host PC. This no footprint is a fundamental component in conveying information security. The token gives secure remote access to the connection indeed, even inconceivably non-secure conditions, for example, PCs possessed by partners in business, home PCs, pads utilized on an apartment WLAN or even open terminals in the Internet café. (Frischat, 2008)

### 2.6.3 Strong mobile signature service

It is used as an example of security services, the drivers request forgets to open systems or network and administrations within the data society, requesting the importance of solid client identification and authentication, non- repudiation of exchanges and certainty in and integrity of the information and administrations. the benefits supplier needs an official understanding just with one administrator. At that point, all administrations within the Circle of Believe or trust may ask authentication and digital signing from client indeed on the off chance that a benefit supplier has made an understanding with another competing administrator than the domestic administrator of the user. The signature benefit stage is greatly secure utilizing solid two-factor and two-channel demonstrate. (Kerttula, 2015)

#### 1.Mobile identity and signing tool

A cell phone is a perfect device to give confirmations or authentications and computerized signature in everyone's day by day lifestyle. The portable phone is personal, raising the feeling approximately my digital, or my portable identity, and as a **marking instrument**, the sentiment of electronic comparable of a pen. Mobile operators are trusted parties society having more than twenty a long time of encounter of the productive and financially savvy SIM card, logistics in GSM/UMTS networks (Initiatives, 2017)(Kerttula, 2015).

#### 2.Mobile signature services architecture

A federated digital model includes a little number of specialists issuing identity accreditations that are shared by interest groups, or organizations and clients. These permit businesses to reuse qualifications issued for other company offline and online situations (Focardi and Gorrieri, 2001) (Kerttula, 2015).

Finnish mobile signature scheme is PKI based federated identity framework with believed, solid and tall quality enrollment preparation and guaranteeing low chance for depending services. By the computerized signature in a certificate, the mobile operator(CA) ensures that it has checked, concurring to its approaches, that the subject personality said interior the certificate is, in fact, the proprietor of the public key that's interior the same certificate, which this public key additionally is in control of the comparing private key. The signature within the certificate can be confirmed by anyone, by utilizing the issuing CA's public key. Below is the graph that it will be describing

The Finnish mobile signature benefit fulfills the solid identification within the Finnish Act on Solid Electronic Identification and Electronic Signatures. all processes that

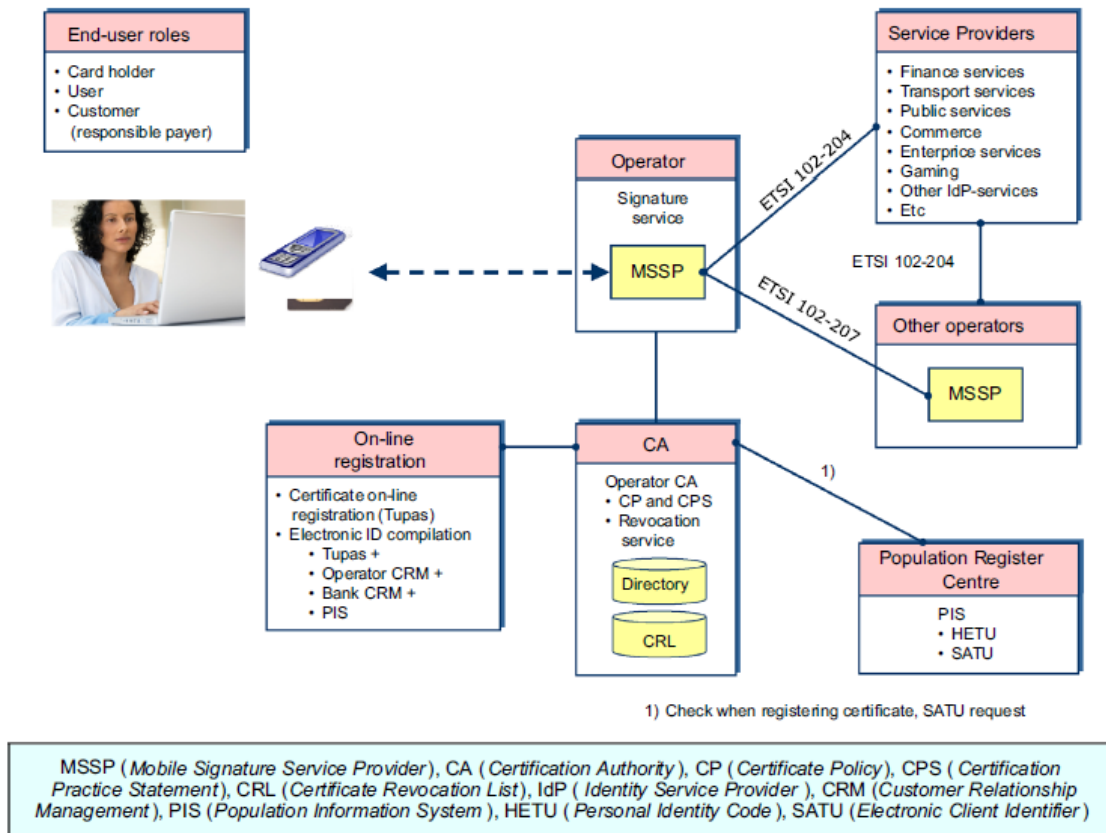


Figure 5: System components of Finnish mobile signature service, only the basic Internet-based service channels are shown (Kerttula, 2015)

## 2.6 Multifactor authentication

Whenever you verify yourself to a framework, you utilize at least one techniques or components of authentication. The more you use, the more secure and progressively dependable the validation or authentication (Burnett, 2006). In general, the advancement of authentication of the frameworks towards Multi-factor authentication beginning from Single-Factor authentication and through Two-Factor authentication. Especially, MFA is relied upon to be used for human-to-everything connections by empowering quick, easy to use, and solid authentication while getting to a service.

### 2.7.1 Three elements of authentication

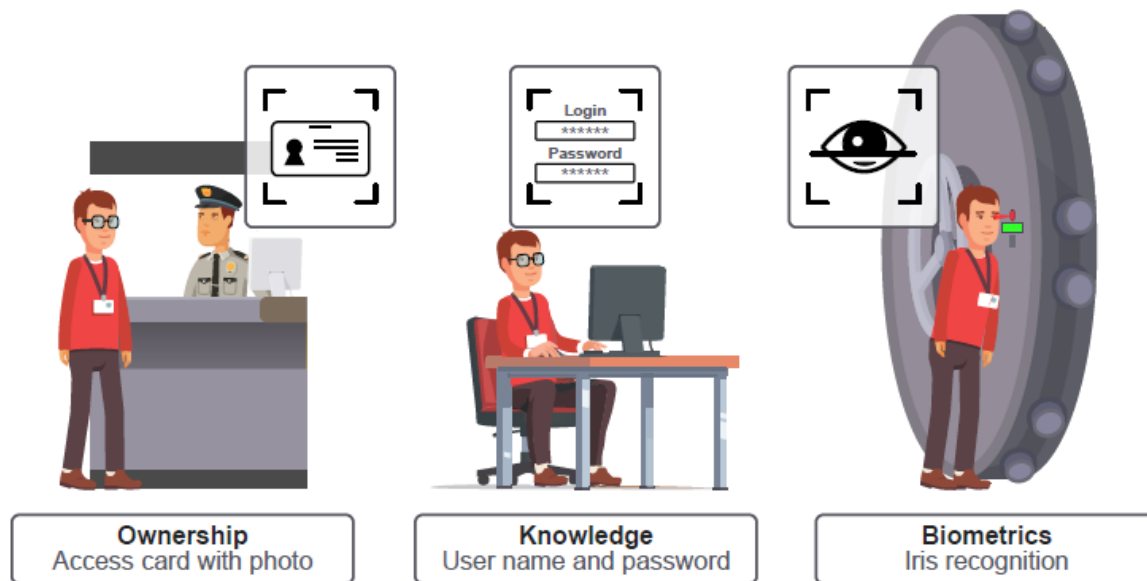


Figure 6: Conceptual authentication examples (Ometov et al., 2018)

At first, just a single factor was used to authenticate message. At that point, Single-Factor authentication was generally accepted by the network because of its effortlessness and easy to be used by the clients. For instance, the utilization of a secret word (or a PIN) to affirm the ownership of the client ID could be considered. Clearly, this is the weakest dimension of authentication. By sharing the secret phrase, one can attack the account quickly. In addition, an unapproved client can also try to get entrance by using different ways of attack like rainbow table etc., Usually, password complexity has to be considered while using this kind of authentication. Further, it was understood that authentication with only one factor isn't solid to give sufficient insurance because of various security dangers. As a natural advance forward, Two-Factor authentication was recommended that couples the delegate information (username/secret phrase mix) with the factor of individual possession, for example, a smart card or a telephone. Today, three kinds of factor bunches are accessible to associate a person with the setup credentials (Ometov *et al.*, 2018):

#### 2.7.1.1 Something You Know

It is an unknown, for example, a secret phrase, that you can create at whenever for the verifying framework. A secret word is a basic component for any security framework and can't be dismissed. In spite of the fact that motion pictures and promoting efforts would have you think something else, none of the other validation techniques dependably supplant or change a secret key. The other two techniques for validation are extremely successful when utilized in blending

with a secret key, however, these different strategies are not dependable enough to take a shot at their own. The entire idea of multifaceted validation is to give different layers of security that cooperate (Burnett, 2006).

### **2.7.1.2 Something You Have**

It is any physical gadget that can be in just a single place at a time.

**This could incorporate any of the accompanying:**

#### **1. Magnetic stripe card**

A plastic card, for example, a credit card, with a dark attractive strip on the back that contains fundamental record data. The new technologies are using Integrated Circuit (IC) card its chip contains both two processors and memory within the body of the card, this will help on card process and data encryption (Madan and Reid, 1992).

The card also includes code which is printed on it. In case the card is going to be stolen the owner will keep his code, as this code makes a difference anticipate a few sorts of fraud, such as stealing a credit card number from a carbon credit card slip, the code can also provide support in confirming of ownership of the card for phone or Internet orders.

#### **2 Smart card**

It is a plastic card with an implanted microprocessor chip fit for putting away a lot of information and performing essential computing tasks (Madan and Reid, 1992). They regularly give cryptographic token, what's more, their structure and improvement over the most recent couple of years have been affected by the advancement of the web-based business. Then again, improvements in web-based business and related advanced technologies (for example java programming language) additionally influenced patterns in smart card models or designs, guaranteeing that card designs depend on the developing requests and needs of online business clients.

It is also commonly progressively solid, and give to some degree preferable verification and also they have the capacity to carry out cryptographic calculations locally in the inside circuitry over magnetic cards. This implies the client's PIN codes or keys never need to leave the limits of the tamper-resistant silicon chip, in this manner conveying most extreme protection to the general subsystem in which the cards take an interest.

Smart cards contain extraordinary-purpose smaller scale controllers with build-in self-programmable memory and temper-resistant highlights proposed to make the expense or cost of a malicious assault on them far better than their advantages.

Over a couple of years there has been an expanding interest for public key smart cards from government organizations and huge companies, for example, phones administrators, banks and protection companies till now where e-commerce and other relevant technologies are used (M'Rahi and Yung, 2001).

### **2.1 Inside the smart card**

The motivation behind why the smart card is brilliant is because smart cards have the remarkable capacity to store moderately huge sums of information, do their own on-card capacities (for example encryption also, mutual authentication) and connect fast with a smart card reader, with the assistance of an installed microcontroller(Leng, 2009).

### **3.USB key**

It is a little gadget that connects to a USB port of a computer. It gives extra confirmation, what's more, regularly has a lot of storage room for keeping private documents or information (Burnett, 2006).

Dongle: A dongle is a little gadget that connects to the printer, or other gadget ports on a PC. It is also held confirmation or authentication data and some of the time contain encrypted duplicate insurance schedules (Burnett, 2006).

#### **2.7.1.3 Something You Are**

It is the estimation of a few physical or behavioral feature about yourself that regularly will never show signs of alter. Common examples are biometrics like fingerprint and retina checking but nowadays the tricks of utilizing different techniques for recognizing or identifying a person is most popular and trusted (Look at the figure below). These are like typing behavior, measurement of hands and so on. biometrics should dependably be joined by a secret word (Burnett, 2006). Bio-data is a solid strategy with regards to validation. For instance, passwords (something you know) or equipment tokens (something you have) is effectively speculated or stolen, yet bio-data

(something you are) isn't. The likelihood of discovering two people with indistinguishable bio-data is low. Accordingly, it is generally held that bio-data can secure a framework against produced validation, and numerous associations or big companies that require high-security levels have embraced bio information in their systems. In spite of the fact that verification utilizing biometric systems is advantageous, security issues, for example, the loss of individual bio-data are not kidding issues, it is really difficult to regain (Kang, Nyang, and Lee, 2014).

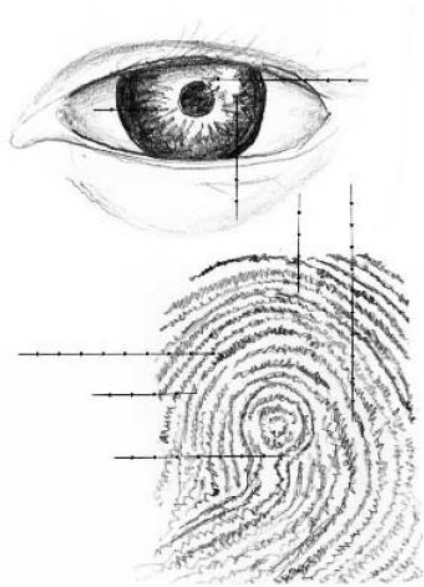


Figure 7:Biometrics has retina and Fingerprint checking (Burnett, 2006).

### **Multiple Layers**

Utilizing any of these three techniques is uncertain, yet joining at least two of them should have great affect security (Burnett, 2006).

### **2.7 Mutual authentication technique**

It is a procedure in which client character is validated and the objective Site is validated to the client (Singhal and Tapaswi, 2012).

In order to secure mobile payment ways like using a passcode, PIN number, identification of serial numbers when it is stolen by the criminal and also when your smartphone is stolen, when someone else knows your username and password it will be easy to act on your behalf. To fix that problem of utilizing only single authentication techniques, another layer of mutual authentication techniques will be adopted.



## 2.8.1 Quick Response Code

QR Codes: are for the most part used to pass on or store messages since they have higher or substantial capacity limit than some other normal conventional 'bar codes'(Dey, 2012)

QR Code is a variety of bits that can be utilized to store data. Data embedded or implanted in QR Code can be protected utilizing different strategies, for example, hash function, reversible data hiding, histogram, symmetric encryption, asymmetric encryption etc.

QR Code has its center structure (appeared in Fig). Position pattern is utilized to distinguish QR Code position, the alignment pattern is utilized to address its distortion, timing pattern is utilized to distinguish focus or middle coordinates for each QR Code cell. The quiet zone is the separation edge for perusing QR Code. Data area is where the information put away.

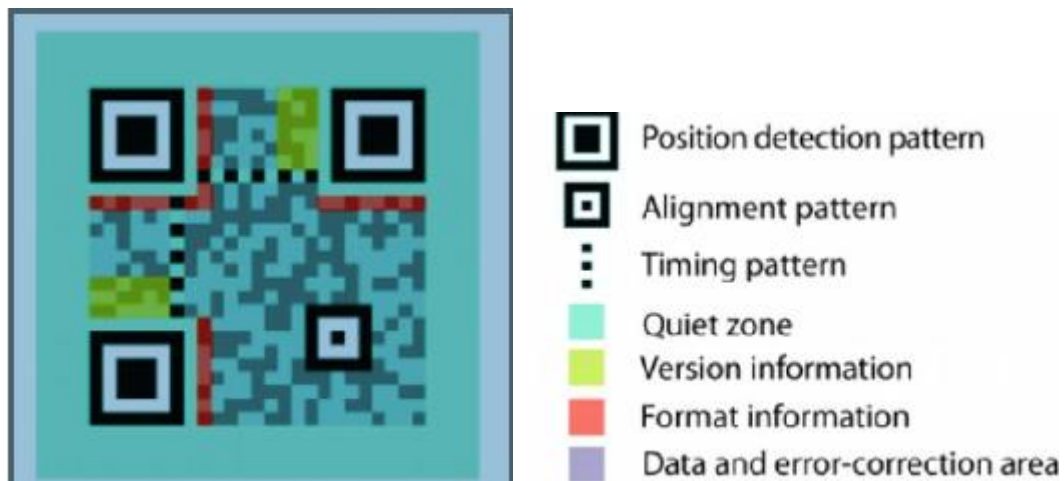


Figure 8:QR Code architecture (Purnomo, Gondokaryono, and Kim, 2017).

QR Code can keep a few hundred times more data. Various kinds of data that can be taken care of by QR Code, for example, numeric, alphabetic characters, binary, control codes, and so on. Up to 7089 characters can be contained at the same time, that is why the QR Code has a high limit information encoding. In the event that QR Code is filthy (unclean) or harm, it doesn't make a difference since the QR Code has error correction capacity. Information can be reestablished regardless of whether the image is in part unclear or harmed. Other than that, the QR Code is likewise discernible or clear from every direction due to pattern detection. This pattern detection is situated at the three edges of the QR Code. QR Code additionally has the ability in

structures appending highlight. It implies that the QR Code can be partitioned into a few information areas then it very well may be structured as a single information image. One information image can be divided into up to 16 images. So it is permitting QR Code to be imprinted in a restricted region. Amid imperative or essential information exchanges in the portable payment framework, the security system of QR Code ought to be considered to guarantee confidentiality, legibility and trustworthiness or integrity of unique information(Purnomo, Gondokaryono, and Kim, 2017).

There are some numbers of the technics that use already encrypted message to add another layer of QR Code. Since QR Codes are greatly sequestered from everything the message, that is the reason it can be utilized to hide the encoded message in the QR Code. This will help us to ensure the security of our information and bring too much complexity to the criminals(Dey, 2012).

## **2.8 One Time Password**

OTP - one-time password, can be utilized just once, and the secret word is invalid after utilize. The single special case can happen if an aggressor utilizes a one-time secret phrase before an approved client.

It can give total assurance of the login time authentication component against replay attacks, it is also able to act in increase existing client IDs and passwords with an additional layer of authentication to improve security for every single authentication application (Huang, Huang, *et al.*, 2013).

The reason is that in case a secret key is bargained, the OTP would at present be broken too to obtain access. This sort of authentication is called two-factor authentication, a more grounded sort of authentication (Huang, Xue, *et al.*, 2013).

The technique for conveying the OTP might be an exclusive token, by means of a cell phone, on paper or an online methodology (Burnett, 2006), By using OTP reply attacks like shoulder surfing will become useless and also timestamps will permitted the location of constrained delay attacks. In any case, utilizing a cell phone as the OTP generator has vulnerabilities keyboard monitor attacks sine cell phone's restricted assets (Huang, Xue, *et al.*, 2013).

Advantages of a one-time password are because the server will never let you use the same password two times like the name proposes, passwords that are utilized just once. By always adjusting the secret word, it turns out to be generously harder to mount an assault(Moloney, 2009).

## 2.9 Security Token

A security token might be a physical device (something the person has) that an approved client of PC administrations is given to facilitate confirmation as a part of a multifactor authentication scheme. they are utilized to demonstrate one's character electronically(Singhal and Tapaswi, 2012).

The token is utilized in augmentation or instead of a secret key to demonstrating that the client is who they guarantee/ claim to be.

From the above, OTP is utilized and built. The client will be confirmed dependent on something he possesses like code scratch cards. To improve security by including one more factor, we can require the client to know something like PIN-code. This two- factor authentication makes it harder to access a record, as a potential assailant would need to take the card and extract the PIN from the client. Such plans are executed by utilizing a security token which requires a PIN code with the end goal to work. A security token generally has a cryptographic processor with a tamper-proof smart card (Moloney, 2009).

A few models of security tokens can be found in the following figure



Figure 9:RSA security tokens(Moloney, 2009)

### **2.10.1 Software token**

Software tokens take a place of the physical hardware token with a product application that can keep running on an assortment or diversity of devices. They offer a progressively adaptable, dynamic, protected and simple to oversee alternative in the present progressively versatile and cloud-based situations. The mobile phone is more suitable for this technology of using software token as a two-factor authentication scheme (Singhal and Tapaswi, 2012).

## **2.11 Different types of two-factor authentication which are most used in networks**

### **2.11.1. Challenge Response Authentication**

In this strategy, there are five stages characterized in which the client confirms himself and demonstrates his character.

- Start where the client enters his username and a secret phrase.
- The Server sends an 8-digit challenge.
- Now the client enters the 8-digit challenge.
- The 8-digit answer is shown on the token.
- Then the client enters the 8 digit answers and accordingly approved to get to the information.

This Technique continues through a hard five stages procedure and it is much inclined to client mistake (Singhal and Tapaswi, 2012).

### **2.11.2. Event Synchronous Authentication**

In this strategy, there are just three stages in which the token code depends on the following number in the arrangement, not the arbitrary number generation scheme which makes it much inclined to the hacking.

- The client initiates the following or the next token code by pushing the button of the token.
- The client enters the username and password (the password is an event delivered token code and the client's PIN).
- Then the server validates by coordinating or corresponding the client password with the server password (Server Password is in depends on the following occasion in the succession).

### **2.11.3. Time Synchronous Authentication**

In this strategy likewise, we have three stages for the verification however here the thing that matters is that both the client also, the server has the internal timekeepers that are synchronized henceforth they are known for time synchronous. Furthermore, they likewise have indistinguishable seeds. A seed is the beginning qualities utilized by the arbitrary number age to make a pseudo-random generated number.

- ✓ The client enters the username and Password (the password is a 4 to 8-digit irregular token code and the Client's PIN).
- ✓ The Server and the token make the token code by joining seed record and current Greenwich Mean Time.
- ✓ The Server validates the client password with the server password and therefore approved whenever found right.

As we discussed above Time Synchronous Authentication is much better than the others two because for instance from the security aspect, the Time Synchronous depends on the token's secret seed which we can say that it is not clear for hacker evidence. The other two are less advanced and inclined to assaults, it also has few steps that make it be easier to use and its portability is based on the way the time synchronous hardware token is not attached to the client's desktop(Singhal and Tapaswi, 2012).

### **2.12 Google Authenticator**

The Google Authenticator application on your cell phone or any other device will produce or create time depends on one-time authentication codes, each of them is authentic just for 30 seconds. These confirmation codes are utilized to sign in to the Barracuda SSL VPN (is a perfect apparatus for providing distant clients secure access to the network assets, just needs a browser to support distant clients access from any PC).

it is recommended that before you can utilize Google Authenticator to sign in, you have to set up an account on your cell phone to create the confirmation codes. On the off chance that you need to utilize numerous cell phones, you should design or configure them at the same time, as it is impossible to expect to include extra gadgets later once the setup has been confirmed. It is

conceivable to make Google Authenticator represents more than one client on a solitary cell phone(Singhal and Tapaswi, 2012).

## CHAPTER THREE

### Practical parts –Methods and selecting solution

#### 3.1 Bank of Kigali

Bank of Kigali was consolidated in the Republic of Rwanda on December 22<sup>nd</sup>, 1966 as a joint endeavor between the Administration of Rwanda and Belgolaise, the auxiliary of Fortis Bank. The open private organization included the proprietorship of 50% of the standard share capital. The bank started its operations in 1967, acting to serve as one of the market pioneers in managing an accounting sector. Following Fortis Bank technique of pulling back its activities in Africa in 2005, the Legislature of Rwanda gained the Belgolaise share in 2007, along these lines expanding its immediate and roundabout shareholding in the Bank to 100%. In consistence with amended laws identifying with privately owned businesses in Rwanda, in 2011 the Bank changed its name from Bank of Kigali S.A to Bank of Kigali Limited and to BK Gathering PLC in 2017 with 3 auxiliary organizations to be specific BK General insurance, BK TecHouse and BK Capital (*personal @ www.bk.rw*, 2018).

In this research, the data was collected using questionnaires where 807 BK customers participated in answering the questionnaire about the use of internet banking in their daily transactions.

As the main aim of this study is to improve the authentication of **BK** internet banking users by adding the second factor of authentication to existing website login to the clients' accounts after comparing the current one by using customers' satisfaction level.

To improve the authentication for BK internet banking customers, an application that helps them to create an account by using an email which linked to the bank account was made. The username and password need to be filled first. Immediately, Application sends you an instant message with a second password. Basically, reply to the instant message with the code to authenticate. The customer will react by typing in the code that he received via email.

## **3.2 Web-based application**

This Web application will be a website created to give access to the database, empowering registration and allowing users to manage their transaction safely. First, our users will need to be with the email and its corresponding password. they will need to open their favorite browser and write the domain name of our web-based application, then from the home page, there is sign up where they will be asked to use already emails that they have and create the first password.

These data will be saved and then users will go to the sign in to put email and the first password h/she already knows then after the second password will be the one-time password that will be sent to the email. Whenever they want to do or to check the transactions, the users will go to the web and finish it safely without being afraid to the hackers and any other bad guys to the internet.

## **3.3 Design**

The "BK website application" project is made of a client-server application where the client side consists of a web application - communicating with the server side made of PHP and MYSQL for the database.

### **3.3.1 Use case diagram**

The use case diagrams for BK online application System will help us to present a graphical functionality overview of the system in terms of actors, their goals as shown in the below diagram we have two actors which are the following:

**User:** is a person, who has an Access to the Application using BK website

**Server:** enable the app to store some necessary information that can help the user to use the website.



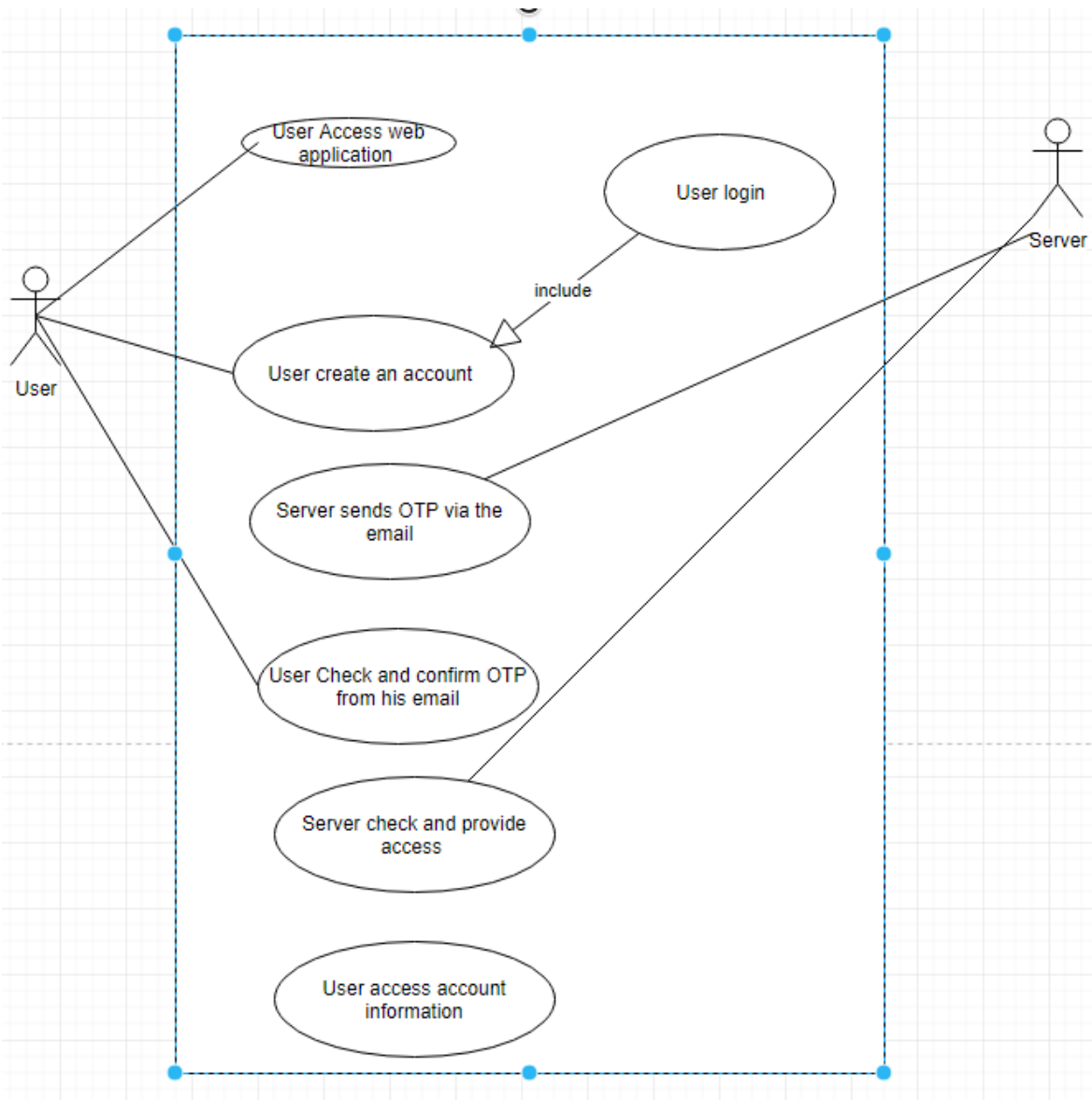


Figure 10: use case diagram (Source my own processing)

The roles of the actors and respective use cases in the BK online banking system is depicted in the above figure as the shown user will access the web application, register himself, login and confirm one-time password send to the email then server will provide the user full access for the user to the application

### 3.3.2 Activity diagram

An activity diagram will be graphical portrayals of work processes of stepwise activities and actions with help for the decision, iteration and simultaneous. In this application we will be using it to show the process to the user side, activity diagrams will be utilized to depict the business

and operational well-ordered work processes of parts in a framework. An activity diagram will also demonstrate the general flow of control.

### 3.3.2.1 User activity diagram

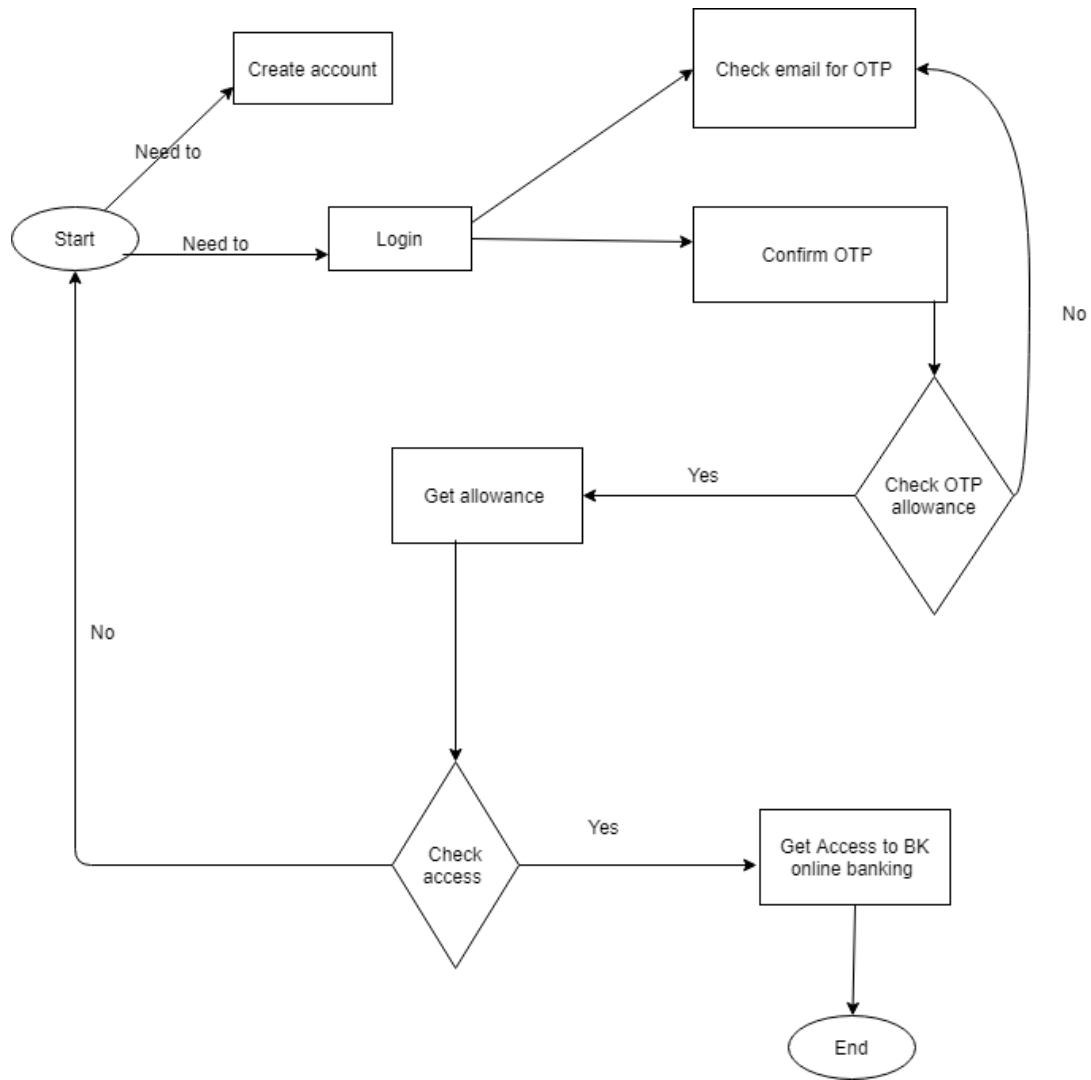


Figure 11: User side activity diagram (Source my own processing).

## User activity

Diagram shows how the users register on the web and how they access information online when access is in Process of realized. From above diagram user Access app on his device and Creates an account and then login into account by using the already known password, after that he will need to check his email and also complete the whole secure login. system check the credentials allowance if no, start again, if yes, receive the access for doing online banking, finally the purpose is to provide the full access and secure control of an account to take place.

### 3.3.2.2 Activity diagram for a server

Server activity diagram showing how application knows registers data if the accepted user starts to use and fill information and send it. From the start, point server recognizes the registered user and check its saved data.

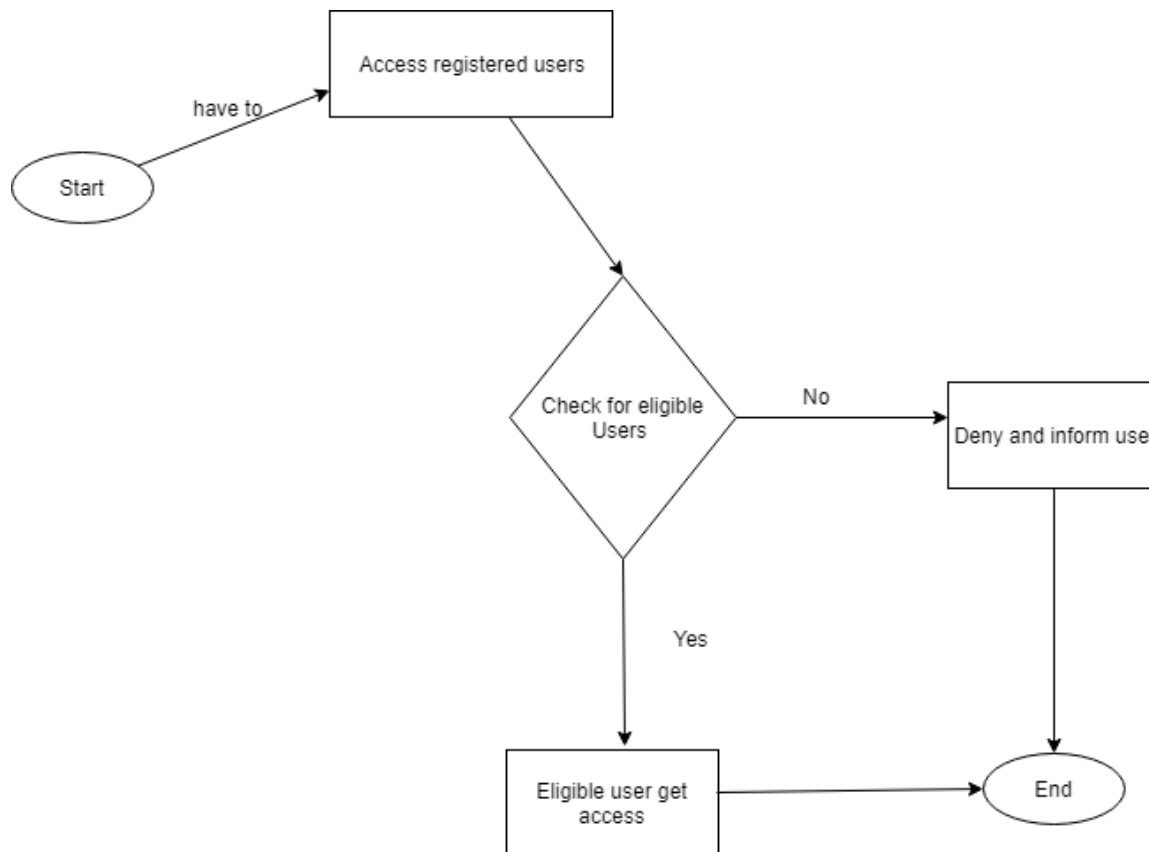


Figure 12:Server activity diagram (Source: my own processing )

### 3.4 Study area.

Data were gathered in four provinces of Rwanda and Kigali City.

<b>Province</b>	<b>District</b>	<b>No of participants</b>
Kigali	Nyarugenge	220
	Gasabo	306
Southern	Huye	70
	Nyamagabe	33
Eastern	Kayonza	10
	Kirehe	12
Northern	Gicumbii	60
	Musanze	67
Western	Rusizi	10
	Rubavu	19



Above is the map showing the province where the data was collected (Google maps).

### 3.5 Technologies used

#### 1. Sign up

Function `NewUser()` will be used for the first time user of the system where s/he will have to input all the data required and then submit to the server to process it .

All data entered through the form, will also be inserted into the database table called `User_tbl` by using insert query.

Here bellow is the description of how Function `NewUser()` and insert into `users_tbl` (names, gender, `user_email`, password) communicate together till where the information is saved into the database.

In terms of security some approaches to anticipate SQL injection attacks were used as shown in the following screenshot where `trim()` and `strip_tags()` will be filtering input information. In general, `trim()` and `strip_tags()` will be the ordinary approaches to separating your information entered. `trim()` will be utilized for expelling or take away whitespaces from the earliest starting point and end of a string. `strip_tags()` for stripping HTML and PHP labels or tags.

The two together can help in expelling extra codes and spaces commonly utilized by unauthorized programmers or hackers.

When we will need to save the clients' password in a database, we will never store them in plain content for security safeguards and protection. In the event that we do hashing the passwords before keeping them to the database, we will have a security system for not uncovering them to the attacker.

```
function NewUser(){
$con = mysql_connect("localhost","root","");
$db = mysql_select_db("project_registration_db");
$first = strip_tags(trim($_POST['fname']));
$last = strip_tags(trim($_POST['lname']));
$full = $first." ".$last;
$em = strip_tags(trim($_POST['email']));
$pass =strip_tags(trim( $_POST['passwrld']));
@Sge = strip_tags(trim($_POST['gender']));
if($em != "" && $pass != "" && $ge != "" && $last != "" && $first != ""){
    // plain text password
    $pass = 'secretcode';
    // add random characters - the salt
    $salt = 'k*jJlrsH:cY]O^Z^/J2)Pz{}qz:+yCa)^+V0898Zf$eV[c@hKKG07Q{utg%0lODS';
    // hash salt and password together
    $md5 = md5($salt . $pass);
    //$pass = md5($_POST['passwrld'] );
    $sql = "INSERT INTO users_tbl (Names,Gender,User_email,Passwrld) values ('$full','$ge','$em','$pass)";
    $query=mysql_query($sql);
    if($query){
        echo "<script>
        alert ('You are registered successfully...!');
        </script>";
    }else if (!$query) {
        echo "<script>
        alert ('Not registered...!');
        </script>";
    }
}
}
```

The below function SignUp () will be used to check or as a condition of already registered users who want to register again, user email will be the Identity to every user, there are not more than one user that can share the same email. This means that one email to each users of the system to ensure the identity of our customers.

```

function SignUp() {
$dbname = "project_registration_db";
$con = mysql_connect("localhost", "root", "");
$db = mysql_select_db("project_registration_db");
$em = strip_tags(trim($_POST['email']));
$sql = "SELECT * FROM users_tbl WHERE User_email='$em'";
$result = mysql_query($sql);
$row = mysql_fetch_array($result);
if (!$row) {
    NewUser();
} else {
    echo "<script>
        alert ('The Email is already used...!');
    </script>";
}
}
if(isset($_POST['submit'])) {
    SignUp();
    mysql_close();
    $boolen = true;
}

```

## 2.Sign in

Below is the PHP script of the sign in after sign up where it checks if the form has been submitted successfully or not and the output are the secure access to the resource.

```

<?php
$seerr= $perr= "";
$email = $passwd= "";
$boolen = false;

if($_SERVER["REQUEST_METHOD"] == "POST" && $_POST['submit']){
    function validate_input($data) {
        $data = trim($data);
        // $data = stripslashes($data);
        $data = htmlspecialchars($data);
        return $data;
    }
    if(empty($_POST['email'])){
        $seerr = "Email required...!";
        $boolen = false;
    } else if (!filter_var($_POST['email'], FILTER_VALIDATE_EMAIL)) {
        $seerr = "Invalid email...";
        $boolen = false;
    }
    else{
        $email = validate_input($_POST['email']);
        $boolen = true;
    }
    if(empty($_POST['passwd'])){
        $perr = "Password field required...!";
        $boolen = false;
    }
}
}

```

### 3. Authenticating user by providing a one-time password

OTP sent via email has to be expired in 120 seconds, this means that the user has to use it within time as it is mentioned.

```
session_start();
@$signed_passw=$_POST['token'];
$t=time();
@$t2=$_SESSION['last_password_generated_time'];
//echo $t."<br />";
//echo $t2."<br />";
//echo $t-$t2."<br />";
mysql_connect("localhost","root","");
mysql_select_db("project_registration_db");
$select="SELECT * FROM authentication_tbl where Generated_pass='$signed_passw'";
$query=mysql_query($select);
$row=mysql_fetch_array($query);
//echo $row['Pwd_genertd_time']."<br />";
if(isset($signed_passw))
{
    if((time()-$row['Pwd_genertd_time']) > 120)
    {
        header("location:authenticate_account.php");
        echo "invalid";
    }else if((time()-$row['Pwd_genertd_time']) < 120)
    {
        echo "Stil valid";
    }
}
```

#### 3.5.1 PHP

It is a generally utilized, open source scripting language with scripts executed on the server to associate and control databases where results come back to the browser. PHP records can contain content, HTML, CSS and PHP code while having ".php" while you saving its file an extension. Within this project, PHP will mainly be used in the process of connecting to the server and from the email that it'll be used to generate a one-time password to the users. It is the one responsible to connect to SQL database data of our users in order to access their accounts and database manipulation.

#### 3.5.2 MySQL

MYSQL as the database framework that will keep running on a server and backings standard SQL. MySQL will store information in tables and will be perfect for both few or many numbers of users. It very well may be downloaded for nothing to pay from the following



recommended website <http://www.mysql.com/>, and at present, it is notwithstanding being utilized by huge names like Yahoo and Google as their database framework that can prove its usability and safety for it. For this project, MySQL is mainly utilized to store clients' data.

### **3.6 Security side of the application**

This is the adjusted verification convention includes some performing ways: the users of the application, the services that the users are looking for from the authenticated server to a database containing information. The users of the application should get services on the off chance that he gives its own legitimate OTP produced by the security PHP mailer, the authenticity is confirmed by the confirmation server.

#### **3.6. 1.One-time password**

To ensure better security of the system, the calculation of one –time password must be with the end goal that it can't be speculated or tried to figure out and ought to be sheltered or secure from all kind of hacking assaults.

#### **3.6. 2.Users side blueprint**

Our web-based program will be produced and introduced on the user's personal computers and also it will be responsive to all device to create the One Time Password. The program will have a friendly interface with the goal that the client can use it without much of a complexity. The application has been produced utilizing PHP, HTML forms and JavaScript where it can run in all browsers. The client is permitted to enter just his password. in case he attempts to enter some other password, an error message would be shown giving unapproved access. At the point when the client enters the password, the framework links the password, with the already saved password. Consequently, the programmers need to have a knowledge for both the password for the client side and also the one time generated password in order to get access. What's more, the One Time password created from this application would be substantial for 120 seconds after which it terminates. That is, soon after providing of the secret key, the client has to login in 120 seconds generally that secret word would lapse and would be of no utilization. At that point, he needs to provide again the secret key.

### **3.6. 3 Database blueprint**

A database configuration is required at the server side so as to store the data, for example, the Username and first password comparing to every client. The database won't be utilized to store the second secret key as it would not be secure but rather it would be utilized by the Server to create the secret key as the demand goes to the server. Subsequently, the OTP calculation would not be detected.

### **3.6. 4. Server blueprint**

A server will be applied in the Bank of Kigali so as to produce the One Time Password (OTP). The server comprises the database as depicted in the above paragraphs. The Server is applied utilizing PHP script technology that oversees, refresh, and retrieve information from and to the MySQL database.

### **3.7 Statistical analysis**

Descriptive statistic with Graphs analysis will be used to specify the satisfaction of respondents based on their cities, genders. The pie chart will also be used to know the proportion that will help us to design the solutions to the proposed system.

All Descriptive statistical analysis was performed using Microsoft excel 365 program (<https://www.microsoft.com/cs-cz/>).

## CHAPTER FOUR

### Practical part ---Results and implementation of the proposed system

#### 4.1 Statistical analysis based Results

With this method, the data was collected and processed by analyzing the satisfaction of how current BK online banking system is working by using a one-step authentication system. From the observations, it is remarked that people about **89%** need a solution not only access their accounts but also the security of them. Therefore, the focus was to find the right content sources for building a new way of accessing their accounts by adding a new layer to the current way of authentication.

##### 1.Participation based on the responses

The following bar chart illustrates the number of participants for each response where No answered by 697 respondents.

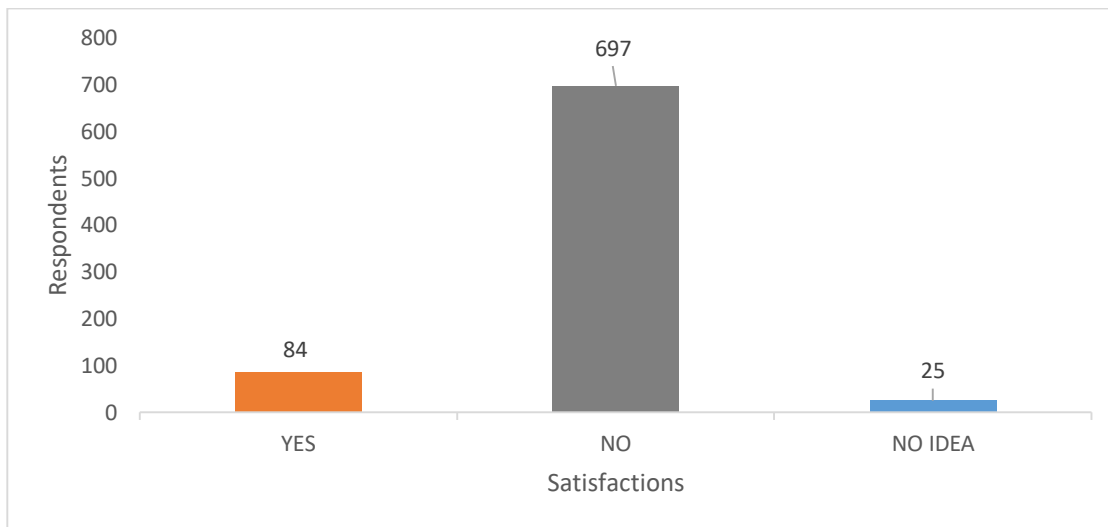


Figure 13:Frequency of respondents respond Yes, No and No idea (source: my own processing)

##### 2.Participation based on the different provinces

Many interviewees were located where branches of University of Rwanda are located, the following graph shows that Kigali City that has many interviewees as also host headquarter of the university.

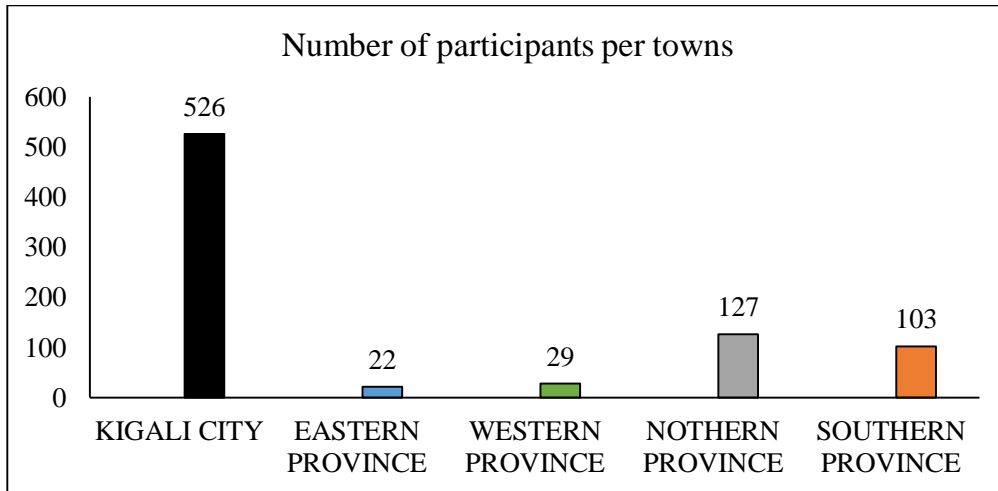


Figure 14: Number of participants per towns (source: my own processing)

### 3. Participation based on gender

During the research, female and male were participated where the number males are much more than female as shown in the following bar chart.

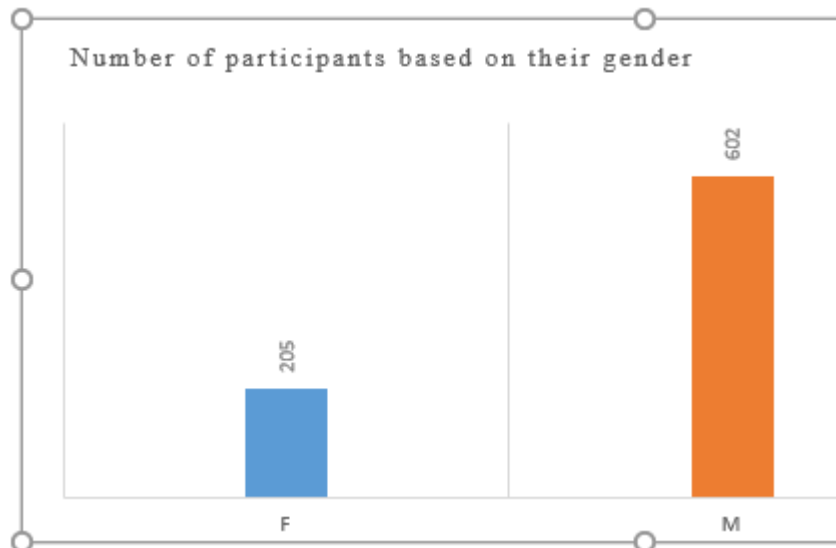


Figure 15: number of participants based on their gender (source: my own processing)

### 4. Pie chart of respondents

The following pie chart shows the proportion of satisfaction level at BK online users. The respondents whose No as response is larger in proportion while Yes respondents are the smallest.

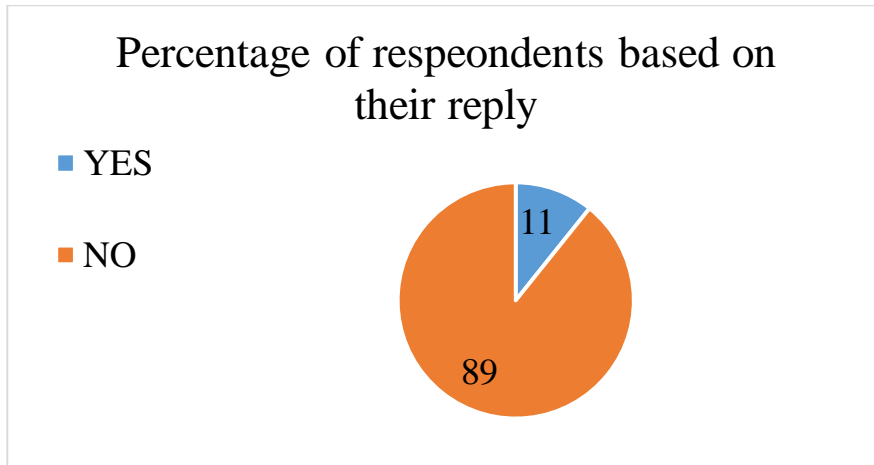


Figure 16: Proportion of the satisfactions (source: my own processing)

## 4.2 PROPOSED SYSTEM

The proposed system provides solutions to BK administration and customers to effectively communicate and share the information, digitalize the output data of the work done at BK after checking the data and easily show up the data that are not allowed by it because of missing of some requirements. It aims to do the following:

To digitalize the way of providing authenticated credential based on data provided by the customers.

To stabilize secure registration and increase the reliability of services.

To ensure reliability and time delivery of sign in to the customers.

To respond correctly to all kinds of inputs.

## 4.3 PROPOSED SYSTEM REQUIREMENTS

System requirements are categorized into two main classes: Software and hardware specifications requirements.

### 4.3.1 Software Specifications requirements

- PHP
- HTML
- MYSQL

### **4.3.2 Hardware specification requirement**

Development and testing machine: Laptop with at least CPU - Dual Core 2.2 GHz, RAM -2GB.

### **4.4 proposed system analysis**

Web application for authentication of the online system through the web is comprised of one main part; That part is described below:

#### **3.4.1 Web application**

The web application will be a site created which gives access to the backend database, empowering registration and refreshing login services. Clients will get to the application online by utilizing their PCs or advanced mobile phones and register to the service

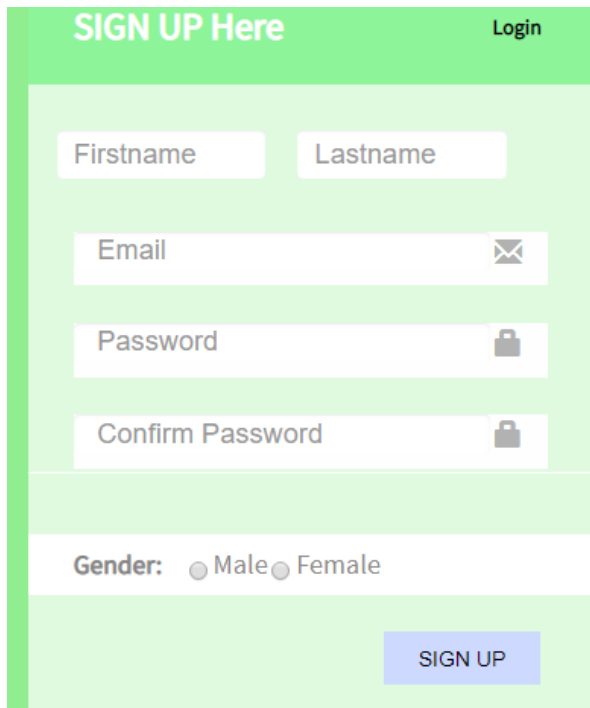
### **4.5 System implementation**

For doing an online exchange, the clients need first to give his registered email and password for confirmation. A one-time password will be produced passed on to the client's registered email. So as to verify OTP from attackers or assaults the proposed arrangement is to create an exchange where OTP will be received via email and also it has to be changed and generated randomly after 120 seconds.

This web based application will have made available to the clients who will be using smart phones or desktop machines which require to access internet connection.

All graphical interfaces that we proposed to include or to integrate in a current web application, the following are the samples screenshots taken from "proposed BK authentication" web-based application. And a summary on design concept as given under each interface highlights the meaning and the role that it plays in the system.

### 4.5.1 Sign Up



The screenshot shows a sign-up form with a green header. The header contains the text "SIGN UP Here" on the left and "Login" on the right. Below the header, there are several input fields: "Firstname" and "Lastname" (two separate boxes), "Email" (with an envelope icon), "Password" (with a lock icon), and "Confirm Password" (with a lock icon). Below these fields is a "Gender:" label with two radio buttons labeled "Male" and "Female". At the bottom right of the form is a blue "SIGN UP" button.

Figure 17: sign up screenshot (source: own processing )

#### How it works:

The first time customers will open an account by filling their names, an email, and gender as they appear on their bank accounts then after they will be asked to set a password to validate them.

### 4.5.2 Login

Logging in can be done after creating an account and confirming the password. As it is described above our application will be two ways authentication, in order to access their accounts, the user will first present email and password as he click ok, the next step will be to present the second temporally code sent to email that have to changes every 120 seconds (appointed to a unique credential ID for client registration). The user has to use those codes before it's expired in 120 seconds.

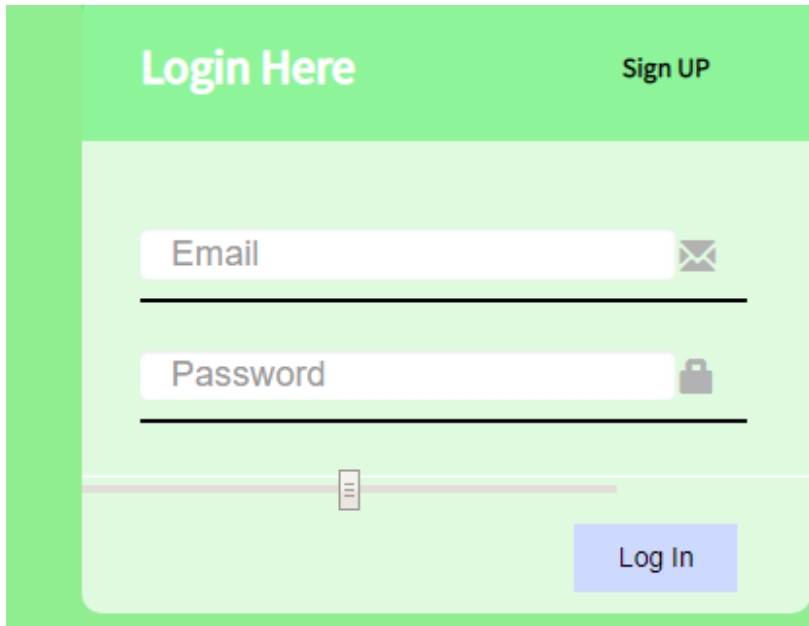


Figure 18:Login screenshot (source: own processing )

After you confirm created email and password by clicking on login, the new tab will be opened where you will be having to put these randomly provided passwords on your email

#### 4.5.3 OTP received via email



Figure 19:OTP Email Source:(My own processing)

The last step will be to prove the authenticity by filling out the random password received via email and that has to be expired after 120 seconds



## CHAPTER FIVE

### Discussion

By referring to the current or previous research done in Rwanda to look after the satisfaction of online banking, this research will be the first to be implemented, which will be highlighting the use of an email address as the second layer of authentication, many of the authentication ways have been presented in the literature review.

The present study shows only how the multifactor way of authenticating your system's account is most used by the biggest organization to ensure security even if it is somehow expensive and requires some knowledge of being familiar with these devices. From those reasons, it cannot be applicable due to the target users of the system.

Because of different reasons, in a previous couple of years, a vast number of BK online banking users have started to complain about the security of their accounts, then after the research that was conducted to figure out the satisfaction of the users where it found that second layer to authenticate the account should be the first solution, however, Ma et al., 2014 said that password that has a length of at least 8 characters and also that 8 characters have to be with a combination of the lower-case, upper-case, numeric and non-alphanumeric, all of them should make password difficult to be guessed and also he proved how to use it as static password may protect your account from hackers.

The study of Guo and Zhang, 2018 studied about secure password with at least 16 characters and generated by a probability distribution and which is also difficult to guess all 16 characters, on the other hand, once the server is compromised, all the password stored on it will be stolen and all accounts will be used by unauthorized persons.

Nguyen and Memon, 2018 conducted the study of using hardware tokens of how two steps validating and verifying of the account's system or any other authenticated user should work by implementing tap-based user authentication for smartwatches where the user will have to pray anywhere on the touch screen to open his/her watch, even if users themselves should fail to keep constant motion to tap on their screen which will bring to them not to access their account, this method is also expensive to implement in such countries on the way to a development like

Rwanda where we might need the method or technology that will facilitate the citizen not to invest in order to start to use it.

Frischat, 2008 implemented about StarSign mobility token as the next generation of USB security tokens where you will be having to install its software and also have a physical token to make it work, but, as I said above nothing better like to be protected to be at least confident of the current the technology you are using, but sometimes due to the targeted customers, sometimes is not easy to switch to the best technology, that is why some countries are still facing the problem of lagging behind in other countries in the best current technology that's why we will not implement any authentication methods which will require to buy a physical device and also some level of familiarization of the electronic device so that it can be used.

Kerttula, 2015 talked about Strong mobile signature service where you need smartphone whoever, in this application, we will implement it to be working in either desktop or any other smartphone as it will be responsive to all device.

Huang, Huang, et al., 2013, Burnett, 2006, and Huang, Xue, et al., 2013, all of them did about OTP based SMS the way the randomly generated password is substantial once and for a certain period of time, The calculation that creates every random a password isn't reversible which is difficult for hackers to breach the security, the customer status have to be confirmed for each attempt to the login by using SMS OTP and finally the clients have to receive SMS to authenticate them via their telephone, in any case, to receive OTP via email have the same steps like phone however OTP SMS in my the country should not be successful due to the shortcoming of the signal for some people who live near to the country border and also for those who like to travel abroad, they will not have a chance to access their online banking as the SMS OTP can be used only inside the country or for some country where roaming is possible.

Therefore, as we have discussed above, Email based OTP is favorable in my country based on geography and economic situation and also we cannot take away targeted customer where it is difficult to implement hard token as it requires some level of familiarizing with some advanced technological device so that you can use it.

Email OTP is cheap and also you can use it across the word that will make it being implemented successfully

## **CHAPTER SIX**

### **Conclusion**

In this project, we described how OTP via email can be the first solution to authenticate BK internet banking users as the current system is less secure as they are still using static password method to access their accounts. We reviewed different technologies that are currently used all over the world, starting from where static passwords are used till now at new world of advanced technology including the drawbacks and the advantages of these systems.

After assessing current level of customer satisfaction towards BK online banking today, which is currently utilizing static passwords, the results clearly showed that it is not viewed as protected and safe. Two Factor Authentication thus becomes the most suitable solution to this problem.

The implementation will have the advantage of simple one-time authentication message exchange, no need for a third party, low computation cost and no cost for proprietary tokens. This research also focused on Two factor authentication implementation by utilizing email. The technique has been tried and found to be secure since it includes the factors that are hard to speculated or hacked.

The findings showed that high proportion of the users need to be authenticated so that they can access their accounts. The only downside to this is that each client needs to have a token material which is still costly for the current users of BK online banking, and that is the reason sending OTP via email will be successfully. This is however worth the risk and the researcher recommends that the bank uses this system.

## CHAPTER SEVEN

### References

- Aiash, M. and Loo, J. (2015) 'An integrated authentication and authorization approach for the network of information architecture', *Journal of Network and Computer Applications*. Elsevier, 50, pp. 73–79. doi: 10.1016/j.jnca.2014.06.004.
- Alsmirat, M. A. *et al.* (2017) 'Internet of surveillance: a cloud supported large-scale wireless surveillance system', *Journal of Supercomputing*. Springer US, 73(3), pp. 973–992. doi: 10.1007/s11227-016-1857-x.
- Burnett, M. (2006) *Perfect password: Selection, protection, authentication, Perfect Passwords*. doi: 10.1016/B978-159749041-2/50012-6.
- Conrad, E., Misener, S. and Feldman, J. (2014) 'Domain 5: Cryptography', *Eleventh Hour CISSP*, pp. 77–93. doi: 10.1016/B978-0-12-417142-8.00005-4.
- Dalgleish, T. *et al.* (2007) '[ No Title ]', in *Journal of Experimental Psychology: General*, pp. 23–42.
- Dey, S. (2012) 'SD-EQR: A New Technique To Use QR Codes™ in Cryptography', *arXiv:1205.4829*, (January). Available at: <http://arxiv.org/abs/1205.4829> <http://www.arxiv.org/pdf/1205.4829.pdf>.
- Dubrawsky, I. (2010) 'General Cryptographic Concepts', in *Eleventh Hour Security+*, pp. 135–151. doi: 10.1016/B978-1-59749-427-4.00010-1.
- Al Ebri, N. *et al.* (2013) 'Forward-secure identity-based signature: New generic constructions and their applications', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 4(1), pp. 32–54.
- Focardi, R. and Gorrieri, R. (2001) 'Foundations of Security Analysis and Design', *Foundations of Security Analysis and Design*, 2171(January), pp. 331–396. doi: 10.1007/3-540-45608-2.
- Frischat, S. (2008) 'The next generation of USB security tokens', *Card Technology Today*, 20(6), pp. 10–11. doi: 10.1016/S0965-2590(08)70153-1.
- Guo, Y. and Zhang, Z. (2018) 'LPSE: Lightweight password-strength estimation for password meters', *Computers and Security*. Elsevier Ltd, 73, pp. 507–518. doi:

10.1016/j.cose.2017.07.012.

- Hamdare, S., Nagpurkar, V. and Mittal, J. (2014) 'Securing SMS Based One Time Password Technique from Man in the Middle Attack', *International Journal of Engineering Trends and Technology*, 11(3), pp. 154–158. doi: 10.14445/22315381/ijett-v11p230.
- Hernandez-Ardieta, J. L. *et al.* (2013) 'A taxonomy and survey of attacks on digital signatures', *Computers and Security*. Elsevier Ltd, 34, pp. 67–112. doi: 10.1016/j.cose.2012.11.009.
- Hiltgen, A., Kramp, T. and Weigold, T. (2006) 'Secure internet banking authentication', *IEEE Security and Privacy*, 4(2), pp. 21–29. doi: 10.1109/MSP.2006.50.
- Huang, Y., Huang, Z., *et al.* (2013) 'A new One-time Password Method', *IERI Procedia*. Elsevier B.V., 4, pp. 32–37. doi: 10.1016/j.ieri.2013.11.006.
- Huang, Y., Xue, W., *et al.* (2013) 'On the Security of Multi-Factor Authentication: Several Instructive Examples', *Cognition*, 226(August 2013), p. 42. doi: 10.2991/icacsei.2013.165.
- Initiatives, R. (2017) 'Mobile identification: implementation , challenges and opportunities'.
- Kang, J., Nyang, D. and Lee, K. (2014) 'Two-factor face authentication using matrix permutation transformation and a user password', *Information Sciences*. Elsevier Inc., 269, pp. 1–20. doi: 10.1016/j.ins.2014.02.011.
- Kerttula, E. (2015) 'A novel federated strong mobile signature service - The Finnish case', *Journal of Network and Computer Applications*. Elsevier, 56, pp. 101–114. doi: 10.1016/j.jnca.2015.06.007.
- Leng, X. (2009) 'Smart card applications and security', *Information Security Technical Report*. Elsevier Ltd, 14(2), pp. 36–45. doi: 10.1016/j.istr.2009.06.006.
- Lozupone, V. (2018) 'Analyze encryption and public key infrastructure (PKI)', *International Journal of Information Management*. Elsevier, 38(1), pp. 42–44. doi: 10.1016/j.ijinfomgt.2017.08.004.
- M'Rahi, D. and Yung, M. (2001) 'E-commerce applications of smart cards', *Computer Networks*, 36(4), pp. 453–472. doi: 10.1016/S1389-1286(01)00166-9.
- Ma, J. *et al.* (2014) 'A study of probabilistic password models', in *Proceedings - IEEE Symposium on Security and Privacy*, pp. 689–704. doi: 10.1109/SP.2014.50.
- Madan, M. S. and Reid, M. A. (1992) 'Data processing aspects of the integrated circuit and magnetic stripe cards', *Information and Management*, 22(1), pp. 41–52. doi:

- 10.1016/0378-7206(92)90005-Z.
- Moloney, A. (2009) 'Online Banking Security and Consumer Confidence.', *Credit Control*, 30(4/5), pp. 28–29. Available at:  
<http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=64306198&site=ehost-live>.
- Nguyen, T. and Memon, N. (2018) 'Tap-based user authentication for smartwatches', *Computers and Security*. Elsevier Ltd, 78, pp. 174–186. doi: 10.1016/j.cose.2018.07.001.
- NIST (2001) 'FIPS PUB 197: Specification for the Advanced Encryption Standard (AES)'. doi: 10.6028/NIST.FIPS.197.
- Oh, H., Kim, J. and Shin, J. S. (2018) 'Forward-secure ID based digital signature scheme with forward-secure private key generator', *Information Sciences*. Elsevier Inc., 454–455, pp. 96–109. doi: 10.1016/j.ins.2018.04.049.
- Ometov, A. *et al.* (2018) 'Multi-Factor Authentication: A Survey', *Cryptography*, 2(1), p. 1. doi: 10.3390/cryptography2010001.  
*personal @ www.bk.rw* (no date). Available at: <https://www.bk.rw/>.
- Purnomo, A. T., Gondokaryono, Y. S. and Kim, C. S. (2017) 'Mutual authentication in securing mobile payment system using encrypted QR code based on public key infrastructure', *Proceedings of the 2016 6th International Conference on System Engineering and Technology, ICSET 2016*, pp. 194–198. doi: 10.1109/FIT.2016.7857564.
- Quisquater, J. (2015) 'New Differential Fault Analysis on AES Key Schedule : New Differential Fault Analysis on AES Key Schedule : Two Faults Are Enough', (September 2008). doi: 10.1007/978-3-540-85893-5.
- Sagar, K. and Waghmare, V. (2016) 'Measuring the Security and Reliability of Authentication of Social Networking Sites', *Procedia Computer Science*. Elsevier Masson SAS, 79, pp. 668–674. doi: 10.1016/j.procs.2016.03.085.
- Singhal, M. and Tapaswi, S. (2012) 'Software Tokens Based Two Factor Authentication Scheme', *International Journal of Information and Electronics Engineering*, 2(3), pp. 383–386.
- Stübing, H. (2013) 'Multilayered Security and Privacy Protection in Car-to-X Networks'. doi: 10.1007/978-3-658-02531-1.
- Wang, H. *et al.* (2018) 'Access control encryption with efficient verifiable sanitized decryption',

*Information Sciences*. Elsevier Inc., 465, pp. 72–85. doi: 10.1016/j.ins.2018.06.068.

Zhou, L. *et al.* (2019) ‘Security analysis and new models on the intelligent symmetric key encryption’, *Computers and Security*. Elsevier Ltd, 80, pp. 14–24. doi: 10.1016/j.cose.2018.07.018.