Use of Authentication Mechanisms and Biometrics in Norwegian Industry

Elham Rajabian Noghondar

Master's Thesis Project Description
Master of Science in Information Security
Department of Computer Science and Media Technology
Gjøvik University College, 2009

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

This thesis will estimate use of authentication mechanism and biometric systems used in Norwegian industry. We will investigate how different factors influence the usage and application of authentication/identification systems and we will look at biometric systems requirements. The input data for this project will be collected from various types of companies/organizations in Norway by a suitable data collection method. We want to analyze correlation between answers of different respondents. Authentication technologies that will be reviewed in this thesis include: username/password, token, fingerprint, face recognition, Iris and Retina recognition, voice recognition, signature recognition, ear recognition and gait authentication, keystroke dynamics and mouse recognition. We will look at legislations and regulations to understand how they can be either helpful or a hindrance implementing biometric systems. In order to become aware of the regulations we need not only to review European countries laws but also should know about exceptions that may exist in Norwegian regulations related to biometric data. We will contact relevant organizations in order to find detail information about the biometric data laws.

Acknowledgment

At first I would like to say special thanks to my supervisor, Patrick Brous, who has been available during my thesis, answers to my questions and help to deal with problems. He presented a lot of suggestions and opinions in order to how to do this project as good as possible. Excitement about this topic causes he do so much effort to find a way in order to receive more reply from the companies/organizations. Secondly, I would like to thank the companies and organizations that contributed to reply the questionnaire with all business that they definitely have to do, without them accomplish this thesis would have been impossible. Thirdly I would like say thanks to people who sent information relevant to regulations and laws in Norway. At the end I would like to thank my family that supports me during this project.

Contents

List of figures

List of tables

1 Introduction

With advancement of technology people authenticate themselves by password, PIN-code, smart card, fingerprint, hand geometry, Iris, facial recognition, walking signature and etc. Although biometrics systems do not have long history usage in different areas, there are a lot of attention and effort to use and enhance the potential abilities of biometric systems in recent years. It might be because of traditional authentication system vulnerabilities. For instance, traditional authentication methods cannot distinguish between a legitimate user and illegal user that access to some permission. Furthermore, biometric characteristics are a sort of people assets that always are carried with them and there is no concern for forgetting and losing them. However, biometrics systems are not mature enough and they are passing their infancy period. Therefore, some efforts should be done in order to make biometrics system robust against possible fraud and attacks related to vulnerabilities of biometrics features nature.
History of biometric systems for a few human features returns to many years or several centuries ago. The first form of using biometric system was based on bony portions measurements of individuals' body in the 1800s. This was proposed by Alphonse Betillon a perisian anthropologist in order to recognize offenders. Betillon method also was based on individuals' body motions and specific signs on their body such as scars, tattoos, harms on body and so on. As this system was not accurate enough fingerprint implemented instead. Fingerprint usage can be dated back to 14th century in china as a signature. The use of fingerprint as a unique biometric characteristic is common since 1880.[1]

This paper estimates capabilities, advantages, usage and the effect of biometric technology in human daily life. In addition usability and benefits of applying biometric system at different places and organizations will be considered.

1.1 Topic covered by this thesis

This thesis includes some sections and each section refers to a specific topic related to the main title. At first we will look at traditional authentication methods. After that biometric authentication systems will be introduced which comprises some other topics such as biometric methods that usually are used in companies/organizations, biometrics requirements, biometric systems vulnerabilities, security and privacy issues, then the countries that are famous in use of biometrics will be introduced. Then we will refer to linkage between biometric and forensic science how biometrics can help experts forensic to find more useful evidence in a crime scene and recognize offenders faster. The forensic aspect of biometric will be mentioned. We will investigate legal aspects that should be considered in order to use biometric systems in companies/organizations with special concentration in Norway laws. Then the possibility of reconstructing biometric raw data from template will reviewed which can be related to security and privacy issues. Data analyzing will be done at the latest section. Designing questionnaire in order to estimate popularity of biometric and which factors effect on companies/organizations to select or deny using of biometrics and traditional method. Then email the questionnaire to companies and collect data, analyze them and make a conclusion.

[1] http://www.globalsecurity.org/security/systems/biometrics-history.htm

1.2 Keyword

Keywords: Traditional authentication, Biometric authentication, Privacy, Legal Aspect.

1.3 Problem description

Individuals authentication can be done through some special information you have such as a key, special information you know such as password and special information you are such as fingerprint. Authentication based on something you are is *biometric authentication* [1]. The first two authentication methods called traditional authentication methods. Traditional methods are vulnerable at the risk of stolen, forgotten or lost. Therefore, needs for deploying new authentication technology besides the former methods seem to be necessary?
By using biometric systems not only experts and administrators can identify individuals but also enhance safety of organizations asset and identify malicious activities against the target organization or company.
One crucial portion of any biometric authentication based system is capability to identify genuine users correctly and reject imposters as fast as possible. Speed in identification is one element to define biometric system performance. On the other hands, the subject is not such easy that seems. Biometric authentication systems include un-confidentiality because the systems usually do not generate same final score after matching process for the same person every time. It shows other external factors influence in the score such as environment light in face recognition, finger position on the reader device screen also pollution of finger, eye position in iris and retina recognition. Threshold is the other important element for biometric authentication systems that refer to system performance. Threshold defines who should be accepted and who should be rejected. These challenges introduce two types of error; False Match Rate (FMR) and False None Match Rate (FNMR). In order to overcome this problem, biometric authentication systems should be in a way such that to reduce the effect of external factors can be minimized. Besides, reasonable strategies should be deployed to select proper threshold relevant to application of biometric system. In addition, biometric authentication systems depend on some requirements such as reliability, user acceptance, easy to use, cost etc. These requirements should be fulfilled by employing some alternatives to increase user acceptance and decrease costs [2].

1.4 Justification, motivation and benefits

Biometric authentication systems can play important role as an element to reduce security concerns for organizations/companies. Biometric authentication systems analyze biometric data input in real-time to identify individuals willing to gain access to a benefit/service and preventing from unauthorized access. The real-time investigation for the input data is accomplished by pursuing several steps and final step would be making decision by comparing live biometric feature with a template already stored in the database [3]. There may be applied counter measurements related to security needs for target organization. The counter measurements include using combination of traditional authentication methods simultaneously with biometric characteristic, using biometric authentication systems that are flexible with alterations of environmental conditions such as light and external factors such as tiredness and hand pollution. Furthermore, using strong encryption topology and hash-function techniques to encode templates stored in a database. Encryption

methodologies can be employed for biometric data that might be transferred through the internet. There are also methods and regular considerations to enhance security and protect privacy of biometric data. However, the counter measurements and other protective methods must be used related to the company conditions and biometric authentication system requirements [2]. In addition, counter measurements should be according to the purpose of biometric system implemented and attacks that the biometric system is vulnerable against them [3].
Governments cooperation to adopt biometric systems seems essential [4] because they provide different capabilities which facilitate individuals identification. Besides, they do not pose weaknesses of traditional authentication techniques and more importantly prevent undisputable events such as loss of assets and terrorism. Use of biometrics system is huge in forensic. Although use of biometric characteristics has a long history in forensic area, use of new biometric system simultaneously with former features provide more creditability in results. In addition, utilizing new biometric features speed up offenders identification and reduce burden of forensic expert because in some cases forensic expert has to do some part of analysis of evidence. [5].
People identification by using biometric system is not only a subject for complex and huge organizations such as airline system of a country. They are usable in different areas for instance, working time registration of employees, access control to a network resources, PCs access control etc.
Implementation and usage of biometric authentication systems should be with regards to criteria and lawful provisions defined in order to ensure that the systems are performed properly to a legal aim. Most of the European countries have similar laws in use of biometric authentication/identification systems. However, some of them apply exceptions and use their own provisions such as France, Germany and Norway. Norway is one of the European country that is keen on using biometric features to identify and people authentication with respect to human rights [6]. Motorola made a contract with Norway's Ministry of Foreign Affairs and National Police Computing in order to use biometric characteristics for issuing Visa [7]

1.5 Research Question

In order to find out common situation of biometric authentication/identification systems used in Norway the following research questions are investigated in this thesis. There are some general and some technical questions about authentication methods, about the devices and equipments are used for performing biometric authentication.

1.5.1General Questions

- Do organizations/companies applied authentication mechanism such as card, PIN-code, Biometric characteristics, combination of them or they utilize other methods for physical access to buildings, critical rooms, PCs, servers, printers?
- If they use biometric characteristics for some areas, which biometric feature they applied. Why they think that the selected biometric feature can be secured enough for their purposes.
- Are there any special factors that compelled the organization to choose the specific biometric feature?
- We are keen on to know if organizations are aware of types of biometric systems in use.

- How the organizations' employees react to the first usage of the biometric system installed. This question in somewhat can evaluate user acceptance factor.
- Are there any changes in user acceptance rate over time?
- If the company or organization does not use any kind of biometric authentication system, are they willing to use biometrics in the future? Which of the biometric systems they think appropriate for using.
- Which factor influence the decision for performing a biometric system?

1.5.2 Technical Questions

Most of the questions in this part are based on more common and well-known biometrics system. The questions concentrate on technical issues.

- We are interested in understanding whether organizations or companies believe that username and password mechanism are safer than keystroke dynamics?
- According to organization's experience whether biometric systems safer than username and password mechanism?
- Did they employ any kind of policy in order to make password? Is there any restriction is use of special characters for instance?
- We ask about their opinion on the security level of some authentication methods such as Token, keystroke and iris.
- What is their idea about implementation costs of various authentication methods?

1.6 planned contributions

Research directly related to authentication method by special focus on use of biometric authentication system in Norway. There is rather limited in number of available articles and related work, so any type of research in the field can be mentioned a contribution on some level. Our effort is based on questionnaire and analysis the inputs. The questions will be sent to some organizations and companies in Norway. The main challenge is to have enough participants. In the analysis part we come up with different answers that will inform us how various factors and conditions effect on implementation of a biometric authentication system or a traditional method. In addition, results analysis highlights which factors have significant influence in respondents' decision and we will find out their opinions in use of biometric system. The results are presented in form of a chapter that can be used as guidelines and reference for future research in this field.

2 State of Art

2.1 Introduction to authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. It helps identify the individuals. One of the benefits of a reliable identification is to improve the general safety of the individuals in a society by identifying the criminals. In addition, reliable identification has another benefit. It helps financial and business trade to be safer and effective by making the parties attention to their actions [8].Authentication is necessary to restrict individuals from unauthorized access to physical location or network resources, and allow only to those with permission. This is accomplished by giving passwords, tokens or using biometrics characteristics [9].

2.2 Authentication methods

There are three basic authentication methods presented by Miller [10]. These methodologies have been used long ago before extensive requirements for automated, electronic authentication:

- Knowledge/ what you know: users with particular knowledge are qualified to gain access the service. Hence, authentication is performed according to secret knowledge, for example password or answers to questions [1].
  Passwords are the most common computer security tool around the world today and have central role in security. For instance, a lot of companies and organizations usually use password in order to protect their sensitive secret data, such as health care information, private data in business, critical financial data, etc. The drawback of using passwords is that they are easy to guess, since users normally choose passwords that are easy to remember. As most of the users have to keep and remember different passwords for logging into the network, applications, gaining access to various websites, logging into E-mail and so on. Most of the systems put the burden of selecting passwords on users and who typically either know nothing about security issues or may not take it serious. Therefore, passwords and tokens may easily be forgotten, stolen and can be fooled. Password and PIN code can be shared among users of a company. Besides, password and PIN code can be illegally obtained by direct observation. Generally the common attacks against password are brute force attack and dictionary attack when user has selected common words as a password [11,9]. Although there are technical procedures in order to decrease risk of password guessing, accidental disclosure to an adversary, subversion, there is no easy way to stop users from sharing their passwords. For instance colleagues will share passwords with a temporary person in case of emergency when somebody is sick, or in such case when they want to leave the company sooner and ask others to finish their tasks. For such cases, the solution is to create a temporary account. However, most people are not interested to make an effort. [8].
  The question is that why organizations, companies and institutes continue to rely on password and PIN code so much. It might be because password authentication mechanisms are easy to implement. In addition, huge number of operating system and applications are using password authentication mechanism for security purpose; therefore their users and administrators suffer the smallest cost and sometimes it means smallest secure tool in location [11].

- Possession /what you have: everybody who is owner of particular physical object such as keys or magnetic strip card or smart card is capable to access the service. For instance, when somebody has a house key, he has permission to enter the house [1]. Authentication with physical equipments e.g. magnetic card, smart card and tokens, were boosted to remove the burden and weak links of passwords. In other word, as the token carries the secret, nobody needs to memorize anything. The other advantage of smart cards and tokens is that the people cannot share them with others; otherwise they will not be able to log in to the system themselves.
  Security has been increased in smart cards, as one cannot intercept or capture and reuse an authentication value used by somebody else. Because the procedures have been implemented on the servers and it will not accept same authentication value twice [8].
- Biometrics/what you are: Biometric authentication includes human personal traits or assessable physical characteristics that distinguish individuals and recognize them from the rest of the individual. These human attributes naturally refer to genetics, phenotypes or inheritable features. These inherent properties are hard to share, steal, copy or forge and as a comparison with possession and knowledge they cannot be changed at all or alter very slowly over time [1].

2.3 Introduction into Biometric

Biometric systems utilize human characteristics which are usually permanent to authenticate a person. Changing and using human characteristics are not easy. Furthermore, individuals cannot pass their biometric features to others as simple as cards and passwords. Biometrics features cannot be stolen easily like traditional methods such tokens, keys, cards etc. However, they could be stolen through computer systems and networks. Another advantage of biometric system is that they work based on methods which cannot be lost or forgotten. This advantage not only reduces administrative tasks but also decrease cost to reissue tokens, cards and password. Biometrics systems' speed can be considered as another their advantages. For instance, using iris-based identification system may take two or three second while finding keys, inserting the key properly and using it may take five or ten second [54]. Businesses, schools, and government organizations have found that the return on investment from biometric solutions is high when they are utilized to recognize identity theft and protect assets at the same time. There are many examples of how biometrics can enhance efficiency. Until recently, network security could only be protected by passwords; now, biometric peripherals can be used to automatically to authenticate the user. Financial transactions, specially those conducted at ATMs, are preserved by PIN-code; biometric technology can replace this vulnerable system with a process that provides acceptability from customers. [1002]

Although biometric systems provide multiple advantages, we cannot replace them instead of passwords or tokens completely. Biometrics purposes are to identify people and decrease human fallibility in identification process by using computer, but it is still based on likelihood, there will be left probability to generate wrong answers. Wrong answers can be two famous errors [54]. Biometric systems with False Rejection Rate less than 1% simultaneously with low False Acceptance Rate is still rare. Most of the current biometric systems are suitable for verification not identification as False Acceptance Rate is high. It implies biometric systems need to

be improved in sense of speed and accuracy. In contrast with traditional authentication methods that final result will be “Yes” or “No” and nothing in between , there is no an extreme result in biometric systems [19].
people without hand are not able to use hand and finger print-based biometric systems. Visually impaired people also cannot utilize iris or retina-based methods. Thus, biometric systems need to be improved for cases cause fail to enroll. One of the phases over biometric system process is data acquisition. Data acquisition phase should be repeated when input quality is not proper enough to process which will irritate users.
Input device should be supervised by a person or should be *tamper-resistant*. Biometric characteristics are not secret and may provide issues that traditional authentication systems do not have to deal with them. Most of the available biometric systems are not implemented based on this matter; therefore they present limited security level.
There is also limitation in time life of biometric sensors specially those have contact with users such as finger print reader. While a magnetic card reader could work for years.
As biometric data includes sensitive and personal information, biometric systems can put individuals’ privacy at risk. For example, body odor could reveal information about user’s recent activities.
Loss of anonymity can be another biometric systems problem. As comparison with a person can have several identities when authentication methods are based on something you have or you know. Furthermore, some individuals think biometric systems are intrusive. People usually feel fear about something that do not have enough information bout it. For instance, in some countries people are not willing to touch a place already touches several times. While some countries people are not interested to be photographed or a device get close to their face.
Lack of standards or refusing to use standards bring critical problem for biometric systems. For instance, two alike biometric systems from two vendors do not work similarly [54].

2.4 Statistics in use of biometric in different countries

Studies show that biometric identification/authentication systems are used in various countries in different fields. We will provide a list of applications that biometrics is implemented for them. For instance, public services, law enforcement, financial applications, controlling physical access to areas and controlling access to equipments and resources. We provide examples for the applications include:

- Public services :
    - Immigration application: Implemented in North America, Africa, Middle East, Eastern Europe(use for recognizing criminals), Asia, Pacific by fingerprint recognition technology.
    - Welfare services: implemented in North America, Africa, Middle East, Asia, and Pacific by fingerprint recognition. Europe utilizes fingerprint and signature recognition equally for this application.
- Law Enforcement:

Biometric systems are utilized for this application includes: fingerprint recognition, hand recognition, iris recognition, signature recognition and voice recognition. Fingerprint technology is usually employed in Middle East, Asia and Pacific, Hand geometry is normally utilized in North America and Europe. Hand and signature are equally implemented in South America. Hand geometry presents most usage in the law and order area. Examples involve:

  - Controlling prison visitors: performed in Middle East, Asia and Pacific by fingerprint recognition. Insuring the person is leaving jail is a permitted person
  - Voting: in order to prevent twice voting by a person.
  - Controlling drug trafficking: this issues is controlled by fingerprint recognition in the Californian Department of Justice.
- Financial Applications: the biometric feature is used in this field is fingerprint authentication system by North America, Africa, Middle East, Europe, Asia and Pacific. While hand recognition is used in Eastern Europe in this field. Fingerprint is the biometric method that presents most usage for financial application. There are some examples in this functionality :
  - Home Banking*:* The aim is safety of financial transaction via telephone using voice authentication methodologies.
  - Credit card: confirming security of people credit card by fingerprint method.
  - Access control: authentication of bank staff and customers.
- Controlling physical access: obtaining access to physical area is controlled by hand geometry in America and Eastern Europe. In contrast with Europe, Asia and Pacific the most preferable biometric technology is fingerprint. Hand geometry is the most common biometric technology in this application area. Examples of implemented biometric systems to obtain access to physical places involve:
  - Access to limited place of the airport.
  - Controlling presence of personnel.
  - Providing security for medical information in hospital.
  - Olympic games.
  - Controlling access to buildings and inside room.
- Controlling access to resources: for confirming that only privileged users have access to PCs, Printers, databases and network voice analysis is usually used in Europe. Fingerprint authentication technology is implemented in Asia and Pacific. Signature and voice recognition methodologies are employed in North America. Voice recognition technology is the most common method to control access to computers and networks. Examples encompasses:
  - Connecting to modem pool
  - Using voice mail technology
  - Gaining access to a conference [67, p31].

3. Biometrics

3.1 Biometric System Requirements

Biometric system requirements and the necessary characteristics define how biometric systems are appropriate for a special application and target company. As matter of fact, their requirement area is quite vast includes functional, technical, fabrication features, find utilization and financial feasibilities. Crucial elements for a biometric system in order to be efficient comprises performance, reliability, acceptance by user, easy to use, easy to implement, uniqueness, enrollment time, cost, resistance to forgery, data storage necessity, etc [18,2].

3.1.1 Performance of Biometric System

Performance of a biometric system depends on two factors: accuracy and speed beside output correctness. Important factors to distinguish whether a biometric system is accurate or not are False Rejection Rate, False Acceptance Rate, Equal Error Rate [18]. Before explaining about the mentioned factors, we are going to discuss a little about threshold and matching value. As we expressed earlier, the result of comparing extracted features with already stored template would be a matching score. This score will be compared with the system threshold that is already determined. In order to have positive authentication of a person matching score should be lower that threshold. Instead of matching value, biometric system might use distance between two templates. If distance value between two templates is high, then we are sure that they belong to two different users and whenever the distance value between two samples is lower, it shows that they probably belong to one user. Two other expressions might be used in systems. “Inter person” distance shows distance between two samples of various users which should be big enough since it determines *uniqueness* of a biometric characteristics. “Intra person” distance presents difference between two samples of the same person which should be as small value as possible to satisfy biometric system *performance* [19].

False Acceptance Rate: or False Match Rate (FMR) is kind of error that an illegal user or an imposter can gain access to a system by getting a lower matching score than the system threshold. False Acceptance Rate is called error typeI

False Reject Rate: or False None Match Rate (FNMR) or error typeII. In this error a genuine user authenticate as an imposter, then the user access to the system will be denied. It this case legal user got higher matching score than the system threshold. This error type makes unsatisfied legal users. On the other hand, if the aim is keeping imposter far from gaining access to a system, error typeII should not be mentioned as an important factor of performance. But if the system is going to be used at an airport to access control applications, FNMR will be irritating error for passengers [20]. Therefore, there should be particular consideration to the target purposes in order to select proper threshold.

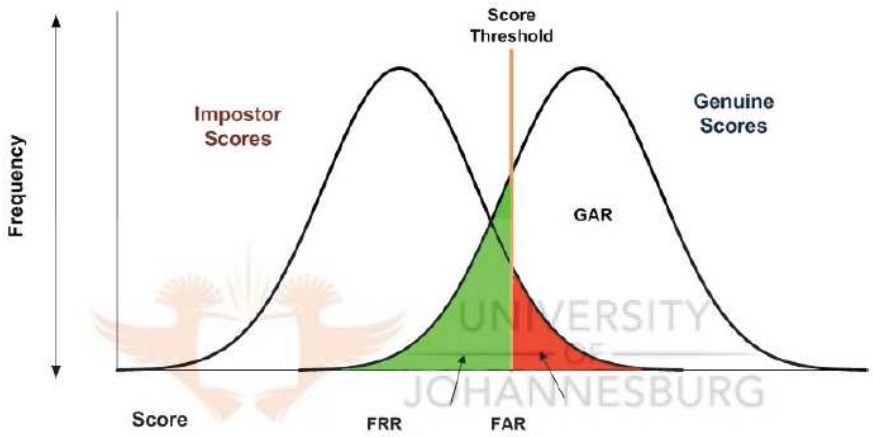

Figure 1. The relationship between FRR & FAR [14].

GAR: Genuine Acceptance Rate

In order to be realistic, although both of the mentioned errors depend on threshold value, balancing between error typeI and typeII practically is difficult. When we want to minimize False Match Rate by altering threshold False None Match Rate will rise considerably and vice versa. See figure2.

Individuals' "psychology" is another important factor should be considered by administrators because of its effect on the False None Match Rate. Biometric systems have two groups of users. First group includes experts and specialist users who utilize/adopt these systems as a part of their profession. The second group includes public users who have to work with the systems because it is either part of their job or social activities. Users not only should learn how to use biometric systems but also they have to act with the system in a particular order. Otherwise the system will not recognize them and will reject them.
Individuals are not interested to reject when willing to get a profit. There is sort of "fear of rejection" among human, as they feel shame due to lack of knowledge about something. However, the rejection might be related to something else. For instance, they may not insert card to automated teller machine properly or they may put their finger in incorrect place on the reader device screen. Rejection not only causes people aversion for biometric systems procedures but also influent in False None Match Rate or False Rejection Rate which directly affects the system performance. Therefore, system administrator should be serious about "training and communication" as a solution to solve the mentioned issue when they perform any kinds of biometric system [20].
Equal Error Rate: It uses to find a point where FMR error and FNMR error are equal i.e. where X=Y at the curve. See figure3. Equal Error Rate has been known as a crucial measure for biometric system accuracy [18, 19].

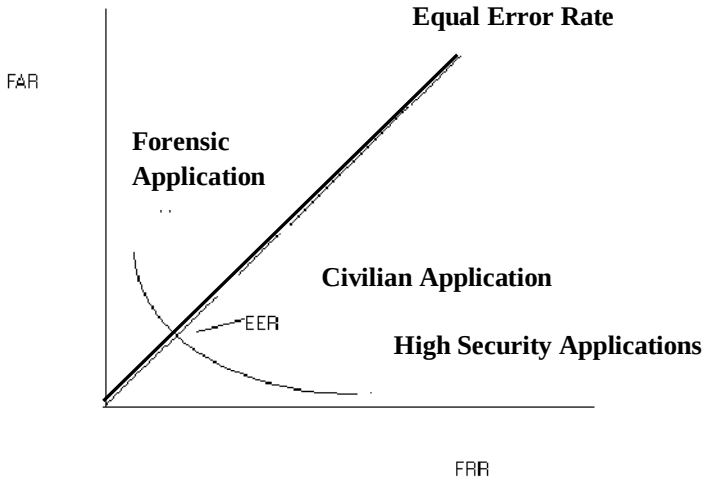

Figure 2. A Decision Error Tradeoff curve

Showing tradeoff between FAR and FRR [18] with adoption.

Speed is the second factor effects on biometric system performance. As a matter of fact, speed depends on the whole authentication process, includes walking to the biometric device, presenting biometric feature or inserting smart card or entering PIN code and waiting for making decision [18]. There is a technique called filtering that is very useful to use for instance in fingerprint biometric system. Filtering technique provides a "quick pattern-based comparison" by checking unique and distinctive signs of live feature with available template on database and eliminate uncertain nominate from the search list. In this manner, the number of matching decrease while accuracy and generating output of the entire system increase very fast. You can find more information in this topic in [21].

3.1.2 Reliability

Biometric identification systems have not been presented proper authentication up to now. It might be due to the errors explained in previous section; it could also be related to manufacturing features such as sensor noise, process techniques restrictions and changeability in individuals' biometric characteristics. In order to implement an accurate biometric system for a specific application, estimating and finding out the number of users who are going to use the identification application is essential. It influences in accuracy and reliability of the biometric system, particularly if it has been implemented in a large scale biometric system, for instance border access control. Furthermore, we should consider a perfect and complete accuracy proper for a system might not be adequate for a large scale biometric system [2].

3.1.3 Easy to Implement

Easy implementation of a biometric system means it should be simple to use. Controlling and emerging current biometric techniques is not possible easily. First reason is lack of "industry-wide" standards. More information is in [22]. Second reason is market willingness is escalating to use low-priced and economical authentication systems.

3.1.4Easy to Use

Providing easy to use factor, there need to be a tradeoff between ease of usage and security level. In addition, ease of use and how users should work with the specific biometric system, shall be trained in simple ways, depending upon individuals training needs also the target application requirements. However, training has some costs for authorities. Usage complexity should be relevant with the target application since even we assume that individuals will accept system difficulties which is really rare, it might not be proportional for the target application purpose. Proportionality between usage complexity and the target purpose is very important issue. We will discuss it at legislation and privacy part. On the other hand, a complex biometric identification system with all its inconvenient may not be a barrier for target application that needs high security [2]. Three fundamental elements define easy to use factor for the biometric systems include: "Ergonomics" , False Rejection Rate and biometric software [71].

3.1.5 Acceptance by User

As we mentioned above, a complex biometric system will be ignored by people. Privacy is the other item affecting individual's acceptance. Some people have negative opinion about biometric application, more information is in [23], because they think biometric data could be used to trace and investigate them. They believe biometric systems are privacy invasive. However, this opinion is not true for all biometric features and some of them are robust against privacy issues because of the techniques the biometric systems apply for extracting templates. After raw biometric data transformed to template, that data cannot be reversed to achieve the primary information about a person. For instance, Iris image is used for extracting a feature vector which will be compared to feature vector already store on the database. In fact, feature vector is obtained/extracted from raw image but retrieving person's Iris image from the feature vector is impossible. Therefore, in spite of biometric system shortcoming they can provide good enough privacy in comparison with the other type of identification methodologies like smart card and password [2].

3.1.6 Cost

Cost is an important element for implementation and employing a biometric system for an application. Cost includes installation costs, configuration, maintenance, individuals training, purchasing software package, buying requirement devices etc [2].

In addition to the biometric systems requirements biometrics should be presented some other attributes. Biometric characteristics were compared with each other against seven classifications. Biometric futures encompass: Universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention. We will look at these properties in details in chapter three.

3.2 Biometric System

There are two types of commercial biometric systems that provide link between a person and his identity. These systems work based on either verification or identification. Verification/authentication system is used when we want to know whom we claim. The system may accept or deny our claim. Shopping by a card, gaining access to a critical room, building or resource, boarding control are examples of authentication technology. Biometric authentication includes a "one to one" or (1:1) search to the sample recently presented by a user, which is then compared with the template provided for the user previously. While biometric identification includes a wider search in a large central database in order to recognize a user through (1:N) or one-to-many search [6]. Identity identification or search system will be used when we want to know who we are without any primary claim for identification. Without regard to which types of biometric systems are used, they work based on individuals' characteristics that might be physiological or behavioral features. Biometric characteristics that are utilized in authentication or identification systems regardless to whether they belong to physiological or behavioral characteristics must offer some properties comprise: [10]

- Universality : everyone should have the feature
- Uniqueness : two persons should not have the same biometric feature
- Permanence: the feature should be permanent over time.
- Collectability: the features must be measured quantitatively and simple to achieve.
- Performance: accuracy of the features defines their performance.
- Acceptability: the features should be acceptable by people to use them.
- Circumvention: the biometric characteristic should be hard to fake and cheat.

However, none of human characteristics presents all the above properties. For instance, users without hand or finger cannot utilize fingerprint biometric system. Also palm with scar cannot be useable in palm print based system. Therefore, universality is not guaranteed in these cases. Uniqueness property will not provide for example for DNA since identical twins can have same DNA feature. Furthermore, finding people with same hand geometry is possible. Permanence property is not presented for biometric features such as face that change over time slowly. Measuring and feature acquisition is not easy in DNA recognition. Depending on analysis method used for extracting DNA attitudes, different results may be achieved. Moreover, factors such as cure shampoo, dyed hair, etc change the laboratory results for DNA. Hence, collectability property is in low level for DNA recognition. Performance attribute will not suitable for biometric characteristics that environment and individuals conditions influence on them. Environment noise

deeply effect on voice recognition and keystroke dynamics performance depends on tiredness and mental situation of the person at working time. Some biometric characteristics will not be accepted by users because people believe either they are intrusive like face recognition or they are not hygienic to touch a public screen like palm print or fingerprint based systems. Circumvention feature is not guaranteed by for instance finger print feature that remains in surfaces and it is collectable from the surfaces.

As these properties have direct influence in biometric system performance, therefore, available biometric systems should be improved to have better recognition. In this manner governments and commercial companies will have challenges to produce more strong and resistant identity tools and extend the tools smartly to provide internal and external requirements for different countries. There should be cooperation between government, industry and academic experts to overcome these challenges reasonably and quickly.

Physiological characteristics normally are more stable and permanent than behavioral characteristics. Therefore, physical characteristics seem more suitable as a parameter and feature to identify individuals. Physical characteristics include fingerprint, palm print, hand geometry, hand vessels, iris, retina, facial, DNA, blood pattern, ear shape, body odor. Behavioral characteristics include voice, key stroke, signature and handwriting model and mouse movements which are affected by person's psychology. These human characteristics will improve by learning over time. Thus they change as human ability improves. Hence, dynamic biometric systems are required in order to accept human characteristics changeability. But behavioral biometric characteristics present least invasive system which causes individual can deal better with them [12]. For example, in iris and retina recognition a device must be very close to user's eye which might not be acceptable by some participants. One the other hand, with a careful look at society we can find out biometric concepts in different portions of the society. Although biometric techniques not mature enough and passing its infancy period, they currently are used in medicine, access control to restricted areas, forensic, internet, boarding control, customs and so on. Besides, this modern and new identity management tools have been applied in variety of areas. Passwords, PIN code, Token, Smart cards and magnetic cards are samples of the traditional management tools that are being used for personal verification, permission to park a car, entering to an organization rooms after a specific time, control user access to PDs, automated teller machine etc [13].

Biometric systems might be more secure and safer than traditional methods. The old methods either can be completely replaced by biometrics techniques or combination of traditional and biometric can be recommended. Since biometric and traditional authentication can conceal each other drawbacks. Some may prefer to use traditional authentication methods. In that way they could deal with traditional methods disadvantages by employing some limitations and safeguard for them such as forcing staff to use special characters and consider specific length for their passwords. We will discuss whether the idea of replacing former methods with modern techniques is a reasonable decision or simultaneously use of the methods

provide more security according for today industrial and commercial needs or continuing use of traditional methods lonely is a good idea.

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palm print	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1. Comparison of Biometric characteristics [14].

3.2.1 Biometric systems uses in organizations

Biometric systems are appropriate for those applications that want to create identity for a specific purpose. Biometric systems can be used in three fundamental modes, which include: identification, authentication/verification and negative identification. Negative identification is especially effective and cannot be found in the other available systems. The system gathers people biometric characteristic and defines which of the individuals have already enrolled or registered within the biometric system. Negative identification prevents several enrolments of a similar individual. Thus it should be considered as a constituent part of each biometric system particularly for large scale biometric system [15].
Although biometric systems are different in many attributes, they work based on specific layering model. The layered model includes two modules:

1. **Enrollment Unit**: This phase includes three subsets, acquiring samples, producing template, saving final templates. The outcome of these steps generates digital samples of the people. In acquiring sample, individuals

biometrics characteristic will be collected by a reader device when individuals encounter with the biometric system for the first time. Biometric properties that mentioned earlier are important in this phase, otherwise enrollment phase will fail, for instance when required feature is iris, and some participants have damaged eyes. As working with new technology might be unfamiliar for many users. In order to achieve better quality samples, a skilled person should present the sample collecting method.

The second subset of enrollment unit is producing templates; individuals biometric sample collected previously will be processed by adding some extra samples and parameters, depending on the type of methodology is used. Since the purpose is preventing to store biometric samples in raw format and extracting template from raw data.

The last part of enrollment phase is saving advance templates. Extracted templates in previous steps should be stored and kept in an adequate condition. Strategies for storing templates could be used in order to make future database search easy. Templates save in a smartcard, a server, a client station or an authentication terminal. Making decision about where template data should be stored depends on the organization purpose [16].

2. **Verifying individuals**: verifying process in biometric systems includes several steps: acquisition, creation, matching, making decision. Person should present required biometric characteristics via an input device similar to acquisition module in enrollment unit. Template produces based on raw biometric data from acquisition module in creation module. It might be necessary to repeat acquisition module for the person due to low quality or not enough extracted data during enrollment phase. In matching module current template compares with template stored on the database. The database involves either many other templates in case of user identification or one template for specific person in case of user authentication. The output of this process would be a score or match value.

   Decision making process will be accomplished by comparing the achieved score with the biometric system threshold. Its output is either to accept the user because the system identifies him as a genuine user or reject the user since the system has been recognized the user as an imposter [16].

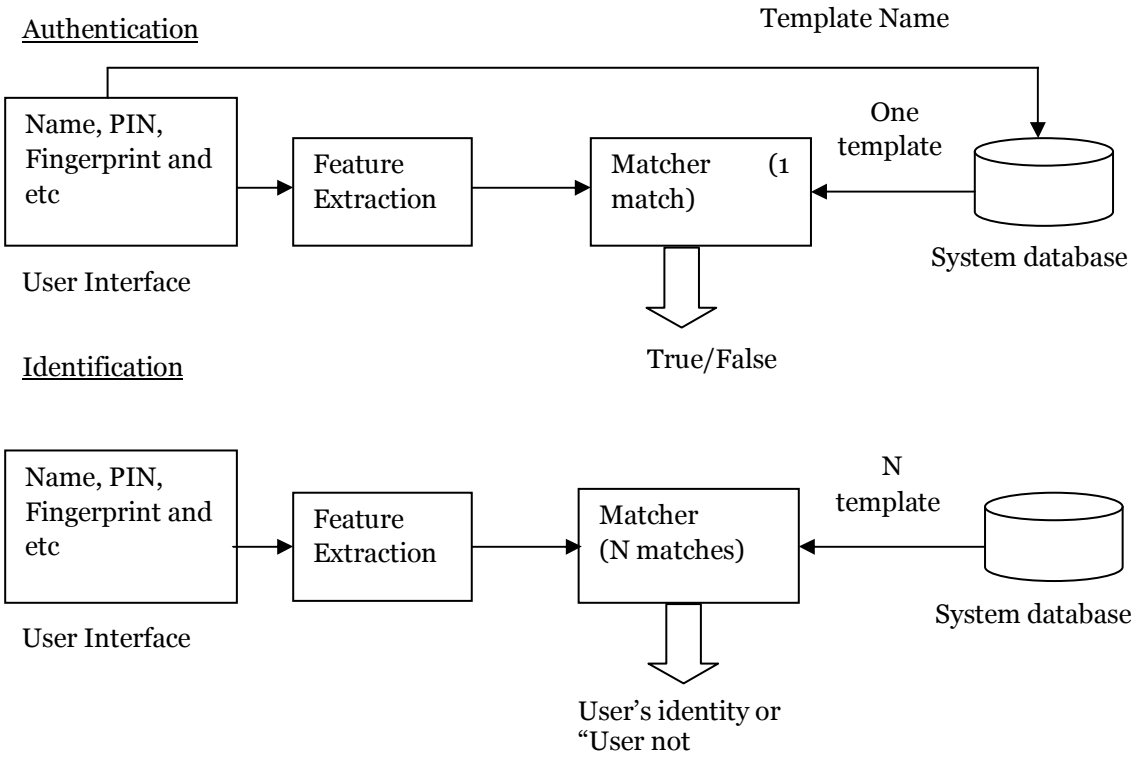

Figure 3. Authentication and identification mechanism [16].

3.2.2 Ethical Issue

Some groups of people hurt by use of biometric systems in society. These groups of people encompasses: individuals with physical/learning inabilities, individuals with mental problems, old people, individuals of specific ethnic, individuals of specific religions and homeless people.

People with physical/learning inabilities have trouble in enrolling their biometrics. Their biometric samples are not accurate enough and enrollment time and authentication is long. For instance, in fingerprint, face recognition and iris recognition.

People with mental deceases will not accept to utilize biometric systems. They have negative opinion about biometrics. For example, they might think that biometric systems alter their life conditions negatively. However, there has not been published any study in this subject.

Elder maybe ignore to use biometrics. Enrolling phase will take long time for this group of people specially those are above 60 years.

Individuals of specific ethnic such as black people will be more in trouble in enrolling face, iris and fingerprint feature than other ethnic.

Individual of specific religion that cover their face or use veil probably ignore use of facial recognition systems. They might be irritated or shying in use of biometrics.

There is not specific address for homeless people to set up an enrollment time for them. Homeless people will be in disadvantaged in usage of biometric. Their biometric information will not be confidential even in case of getting a card because of health situation, losing weight, untidy skin etc.
These social members will be excluded when implementing biometric systems in society. Elder members will be more disadvantaged than other social members. They need to gain access to health and social services more than others. Social exclusion is considered as ethical issues because some social groups should be sacrificed in the benefits of other groups and possible hurt is neglected for the individuals. In other words, public benefits and right will be considered more than the individuals' rights. However, there should be a balance between public right with right of few group of people in society. For example, if a biometric system is implementing to obtain access to health care and social welfare services, there will be lack of proportionality on people who are chronically sick or unable to work because of age, health issues etc. Disproportionately factor results individuals who have right to access to health care and social services miss their right. In addition, some social members might be victim of identity forgery and terrorism. Hence, the approach that biometric systems prevent identity forgery is not guaranteed [68].

3.3 Biometric system vulnerabilities

Although biometric systems present many benefits versus traditional authentication technologies that may not distinguish between legitimate user and illegal user. They prone to some attacks. As figure 4 shows there can be attacks in various portions of a biometric system process. First attack could occur via presenting a counterfeit biometric feature to the device sensor. Biometric systems are vulnerable to replay attack. In this case attacker captures biometric data on place two. For instance, in voice recognition somebody can record somebody else voice or in fingerprint authentication that unintentionally fingerprint remains on surfaces. This attack called "*contamination*". "*Coercion*" is another attack that may happen on this step when an attacker obliges the legal user to use his biometric feature to gain access to the system. The attack could happen in place three; the attacker using procedures on feature extraction phase to generate feature score desired by the attacker. In place four attacker substitute original feature score with the generated score on place3. Attacker tries to exploit matching unit by editing the final matching value in place5 in order to achieve a value that match to the system threshold. Furthermore, there could be attack against templates database in place six. For example, adding desired templates, manipulating, removing available template which refers to Denial of Service attack and capturing personal data that put individuals privacy at risk of using in illegal purposes, this attack called "*circumvention*". Possible attack between template database and matching unit could be modifying and changing template when data is transferred in order to find a match. The last place that could be at risk of attack is place eight. Attacker tries to change system decision for identifying positively by the system [3].

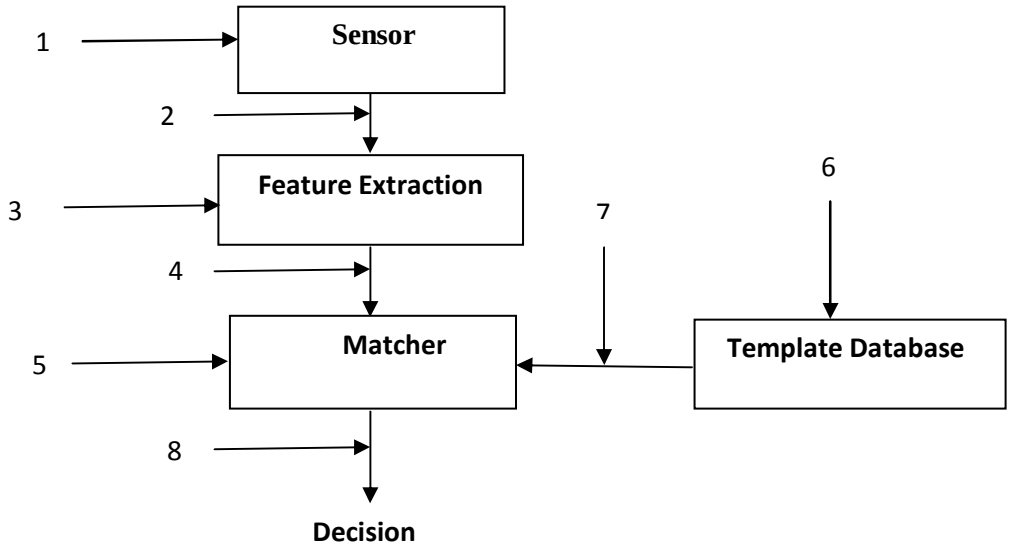

Figure 4. Attack against Biometric Authentication System [3].

You can find more information in [3] about number of attacks against biometric systems.
Most of the attack against biometric systems is because of the biometric characteristics nature. Individuals cannot prevent their fingerprint that remains at surfaces and equipments. Schneier emphasizes in [24] a compromised biometric characteristic cannot be replaced with a secure one when it is misused by an adversary, but it is possible to use another encoding structure to create a new encoded biometric characteristic.

3.3.1 Reconstruction Biometric Raw Data from Template

Each biometric authentication system embraces as follows:

- Sensor: use for acquisition of biometric raw data.
- Feature extraction: use for create template.
- Matcher: compare presented sample in enrollment phase with stored sample.
- Reference archive: keeping all the biometric stored templates.

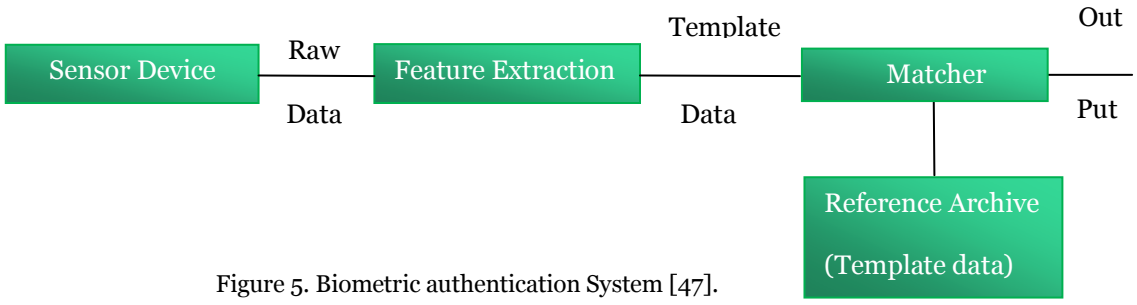

Figure 5. Biometric authentication System [47].

The unchanged output of sensor would be raw data, which might be fingerprint, face image, iris or a voice captured via microphone. Raw data type clarifies possible ways to abuse individuals' privacy. Generally, raw data involves as follows depends on what kind of biometric characteristics are studied:

1. Useful information for authentication such as chronic disease. In fact, this information is a subset of numbers three to six.
2. Information that is not useful for authentication e.g. acute disease. Other type of raw information related to origin of biometrics characteristics.
3. "Genotype information which is defined by genetics".
4. Randotypic information or "phenotypic" without genetic pants will be defined completely random.
5. Behavioral information is obtained by training and rehearsal.
6. Information about "unchanging marks". For example, scars. Tattoos and chronic disease [47].

3.3.2 How possible Reconstructing Raw Data from Template

- First example: This sample is quite rare in biometric systems, but is not a completely hypothetical thought. It will occur when raw data equals templates; therefore, reconstruction process is minor.

- Second example: This example could be same with example1 if the raw information only includes information mentioned above in number1, which is suitable for authentication purpose. But if some changes are applied mathematically in feature extraction phase that do not decrease available raw information, some believe that raw data will always re-build from template feature [2][47].

- Third example: Raw data includes both information suitable for authentication and not suitable information for authentication. Feature extraction phase eliminates the information that is not proper entirely which might contain acute disease; therefore, the template data equal information suitable for authentication. Hence, eliminated data cannot be re-built from template data unless one tries to guess them.

3.3.3 How Template can refer to re-building Raw Data

As fingure5 shows both raw data and output of the matcher unit are available. An adversary is going to apply "*hill-climbing*" attack in order to re-build raw data by repetitious processing. The attack begins with a primary guess for the raw image and the attacker tries to perform authentication. Then a score will be appeared at matcher result. The first data is changed a little and again offer to authentication if there is a deployment in new matcher result derived from repetitious raw data,

[2] http://www.bromba.com/knowhow/temppriv.htm

template data and reference archive. If changes to the raw data were not enough new changes is required. This process might be repeated hundreds times until the adequate score value accepted by the biometric system. For more information about *hill-climbing* attack see [47].

Generally, part of raw data which is suitable for authentication can be re-built. While suitable information for authentication and were eliminated from template data cannot be re-fabricate. As mentioned before unsuitable information for authentication such as acute disease that put people privacy at risk should be omitted from raw data. Furthermore, the effect of re-constructible authentication data such as genotypic and behavioral data should not be neglected on privacy. Genotypic information is crucial because they disclose racial or origin, diseases etc [47].

3.4 Biometric Security Issues

There are two types of weakness with biometrics authentication/identification. Either users do not authenticate/identify erroneously or users authenticate/identify wrongly. In this cases difficulty of identification pattern should be considered. Users do not authenticate or identify erroneously when resemblance examination is rough. While resemblance examination almost is easy when users authenticate or identify wrongly [25]. In the other words, there must be an acceptable balance between the first issue which is False Negative and the second one which is False Positive error that is a challenge for biometric systems [26]. According to previous experiences one of the errors can have a small scale while the other error type has a high scale. Using biometric technologies can be safe for a specific domain if both error types happen very infrequently. Another common challenge related to performing of authentication/identification biometric technology. The data collected from the user should be kept confidentially. Therefore, the data will be secured enough for the certain biometric system. It is obvious data collection from users should be at the current time and any repetition of the data collection for verification purposes is not expected [25, 27]

Biometrics brings other security problems beside security issues mentioned above. First problem is reduction in use of classic forensic methods. In the other words, as usage of biometrics is increased, there will be a decreasing in usage of classic techniques like fingerprints. This is important because fingerprint databases facilitate finger copy that could be exploited against somebody else at the crime scene. Another example is border control system cannot being up to date quickly like a standalone machines to build fingers copy. The second biometric security issue is stealing body part which put at risk physical integrity of people. However; kidnapping and blackmailing can take place of the body parts stealing. The last issue is “wanted multiple identities could be uncovered as well”. For instance, some countries might define a person for their biometric databases at least for foreign citizens or asylums which uncover representative for secret services [25].

There must be special consideration and attention on choosing a biometric characteristic to use in a certain place or for a defined objective not only because of the needs and necessities of the target organization but also due to biometrics technologies weaknesses such as forgery and cheat. For instance, *hill-climbing* attack is a famous threat for biometrics that will happen when an attacker or unauthorized user has gain access to a biometric system template or database including people digital signature and try to change threshold even add new template or alter available templates. Digital signature could be compromised when signing key extracted from digital signature completely depends on the number of biometrics enrolled by the people [28]. Solution for eliminating the attack against

digital signature which can be utilized for electronic mail, withdraw from account, contracts etc is using encryption techniques. In order to make it more secure, secret key for the digital signature can be stored onto a smartcard [29].
Fingerprint could be tricked by call uses by remaining points and stamp ink on the reader device, hand cream or greasy hand. Facial recognition is another example that can be compromised by impersonates and disguise when environment light is not suitable. However; some biometrics companies struggle to perform statistical methodologies in order to neutralize the changes in biometric devices output because of various environmental conditions such as lighting at the time of taking sample. Iris recognition can have reduction on quality or even increasing risk of fraud when people use lenses and because of "*watery eyes*" [30].

3.4.1 Biometrics Privacy Issues

In reviewing legal aspect of using biometric technology, we should consider data security beside people privacy. In the other words, data authorities must apply all possible methodologies in order to prevent accidental event and organized fraud and attacks to protect private and personal information. Sudden event includes loss and destruction of data due to human mistake or mechanical problems and crash, also natural crisis. The examples of organized attack are misused of data for a special framework, data disclosure, and corruption etc. We must think about security issue particularly when biometric data is executing. This process typically involves several steps: storing data, transferring, extracting pattern and evaluating similarities. In addition, there must be special safeguard for example by applying strong encryption algorithms when biometric data should be passed over an unsafe universal network like the internet or networks with poor security. Proper considerations should be taken to account in use of biometric data because data security is an unavoidable portion of privacy protection law. Other solutions should be recommended to escalate biometric data security. Data must get nameless, anonymous or using assumed names and deleting unnecessary information after enrolment process finished, biometric data transformed to templates and storing data. In addition, False Rejection Error, error typeI and False Acceptance Error or error typeII must be at the lowest scale. These two present biometrics system accuracy which obviously effects on security. The final results of these types of error are critical and vital for data owner. For example, one may gain access to a secured building or a database who should not be allowed to access to the areas. Even worth one could pass border of a country wrongly due to improper identifying passengers.
Biometric data has a key role to make connection between various databases including people private information. Moreover, some biometric data reveals more data than essential for authentication/verification and identification such as health and racial data. Therefore, challenges will be raised because both mentioned cases refer to sensitive information. Hence, there must be not only a compliance with legislation principles but also there should be strong security applications for the data controllers to use people sensitive biometric data [31].
Recently, biometrics information has been stored into large computers include scanner, digital camera etc that are known ICT system. This digital database can be searched from anywhere around the world to find a match for possible samples. Therefore, database includes biometric information can be threatened by manipulation, destruction, corruption, theft and disclose.
Privacy refers to preserve integrity, autonomy and individual private life. Factors such as mobility, efficiency, security in society cause keeping privacy become tough. For instance, individuals are interested in carrying an RFID token in their car

instead of cash in order to pay toll road. This put their anonymity in danger. Researches show some people are not worried about breaking their privacy since they believe that they have nothing to keep secret. Critics think there is no enough work for preventing terrorism when discussion comes to security and surveillance identification. Some countries prohibit anonymous calling cards while some criticize this prohibition only stops typical people who would like to be anonymous [25]. The United States breaks people privacy in some ways to do anti terror projects by for instance, eavesdropping telephone, monitoring electronic communication, and analyzing individual data which may collected from various databases without notifying them [26].

Biometrics technologies can be a threat for people privacy in some ways because it includes crucial private information. For instance, retina scan exposes consumption of alcohol; from the previous two days. Another example that is under discussion yet is investigating whether asymmetric fingerprints display information on homosexuality life. More information is in [12,32]. Some biometric methodologies may collect data without knowledge of persons which called passive biometrics recognition such as face recognition and gait authentication. That is another example against individuals privacy. In addition, using two or more biometrics features simultaneously to increase security of a system, make the privacy issues double [25]

A crucial subject is how biometric should be utilized and how it should not be utilized at all. First of all we explain how biometrics should be used. Biometrics metrologies can be used in equipment that has been shared only by one person since there is no shared database between large numbers of users to occur fraud. Furthermore, biometrics can be used with possession authentication like key, magnetic card and smart card and authentication by knowledge like password in order to increase security of authentication method. In addition, it can be utilized when there is no reduction in use of classic forensic technologies such as fingerprint. The biometric features have been saved on the database could be disclosed to unknown devices by the person who has access to the biometric database. Furthermore, biometric technologies can be used when there is no privacy issues derived from biometrics because each person control their own equipments. If possible turning biometric system off when authentication has been completed. Therefore, the safety and physical integrity of users will not be at risk even if the user be interested in working with the attacker together. Cases that biometrics should not to be used at all include passive usage of biometrics by devices helpful for face recognition at public places since person does not aware of the recording. While person on active biometrics capturing aware of the process such as passports control and can ignore active biometrics. Hence, using passive biometric methods in secret should be prevented by law [25].

3.4.2 Security and Privacy Enhancement in Biometric Databases

Some techniques have deployed to enhance security and protecting biometric databases privacy by considering verification or authentication as a key point. Traditional method to control privacy and security called *zero-sum paradigm* emphasizes somewhere privacy must be deal for security and somewhere security for privacy. While *positive-sum model* “Untraceable Biometric” approach includes two methods: *Biometric Encryption* and *Cancelable Biometric.* Positive-sum model escalates privacy and security simultaneously. Biometric Encryption, there is no database including samples for example for fingerprint in order to use in Biometric Encryption. Instead of storing biometric data in a database, Biometric Encryption

makes a digital key from the biometric data, then use it to encrypt or encode other information such as PIN code, account number, social number etc. Not only the key but also the biometric feature cannot be recovered from the saved information. Finally, Biometric Encryption technique encodes the code and store it not biometric feature. Result of Biometric Encryption authentication would be either a digital key or an error message because the key will be produced again if proper biometric feature has been presented by user. While the second technique, Cancelable Biometric, apply some changes to the primary biometric feature and storing the new template. The similar changes will be applied to biometric feature at the time of authentication, and if correct matching done between the biometric feature and the template, reply will be "Yes" otherwise "No" [33].

Biometric Encryption increases privacy in three ways. First, there is no need to preserve biometric templates then the probability of missing, corruption and misusing decrease. Second, People can control and limit the use of their biometric information for specific intent. Third, Security will rise because authentication method and data broadcasting have been improved [33].

Multimodal biometric system, multi biometric or biometric fusion is another technique to provide security, privacy and better comfort. See figure6. As a matter of fact, multimodal biometric increases accuracy and availability of a biometric system. Multimodal biometric system can be deployed in five fashions:

- Multiple sensors, it means using various sensors to extract variety of recognition features as outputs for one specific biometric feature. For example, using combination of movements in two- dimensional such as movement to forward and sides and three dimensional movements in gait authentication. Motions to forwards and sides plus vertical motions can be used to improve total recognition accuracy.
- Employing multiple biometrics features to extract set of recognition outputs to increase accuracy in authentication/verification cases and speed in identification situation. For example, gait authentication and facial recognition are two fast authentication methods while fingerprint and iris recognition are slow but more accurate.
- Applying multiple units of specific kind of biometric characteristic. For example, collecting biometric data for more than one finger, or checking the retina of both eyes.
- Using multiple snapshots of a specific biometric characteristic. It means collecting For instance iris biometric data for several times or several image of ear or face.
- Using multiple algorithms or extraction techniques for a specific biometric characteristic in order to find a match. In other words, different algorithms or feature extraction methods must provide same results [34].

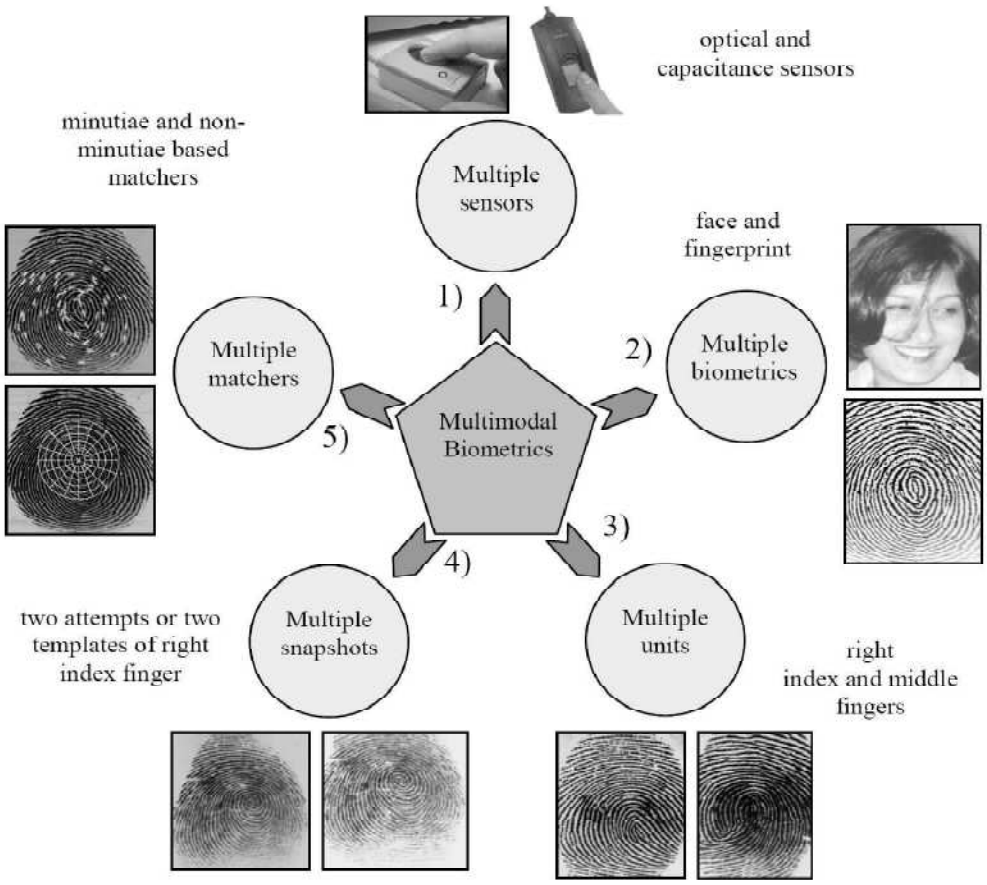

Figure 6. Scenarios in a multimodal biometric system [51].

3.5 Biometrics In Forensic

The reasons why we look at use of biometrics in forensic is that history of biometric features in forensic is longer than history of commercial usage of biometrics in organizations for authentication purposes. Beside most of the biometric features, we are going to investigate in Norwegian industry are common in forensic science as well. Then, there is a clear linkage between forensic and biometric authentication/identification systems. Today, many biometrics systems are introduced by scientists. Each of them works based on a specific identification and recognition methodology which defines whether they are suitable for a special aim or not. There are some requirements for installing and using biometric characteristics to receive reliable throughput involve: [35]

1. Captured data should present the least needs on resolution, quality, size and enough permanency.

2. There should be sufficient data for the extraction algorithm to categorize identities. Moreover, there must be an proper database as well.

3. There should be tradeoff between False Match Rate and False None Match Rate by accurate and adequate adjustment for threshold related to necessary security level for the organization/company or place.

4. Each biometric feature should be analyzed by a specific algorithm. The algorithm should be able to generate strong and resistant templates and storing template data as much as possible in small size.

There is a link between forensic and biometric. Some of the forensic evidences will be investigated and analyzed by biometric methods if they fulfill the above mentioned needs. Otherwise, improvement and re-fabrication methods will be applied to original evidence and image. Improvement methods are useful to help specialist person to make his decision. However, enhancement methods decrease reliability of the analysis results. Sometimes improved evidence is not applicable and useful even after applying improvement methodologies, then the evidence is not efficient to analyze by biometric procedures [35].
Different reconstruction and fabrication methodologies will be used depending on the type of biometric evidence. "*Super resolution*" techniques [3] employ in several steps to biometric evidence recorded such as face, fingerprint and Iris etc that has low resolution and quality to make a suitable image for verification purpose. Forensic artists might draw a preliminary image according to witnesses expressions. In such cases other vision methods will be used to create an adequate image for biometric verification aim. If the primary image for example is a face, than "*low resolution eigenfaces*[4]" will be used for the low resolution image to extract their coordinates. Later, the coordinates will be applied to high resolution "*eignface*" to re-build and achieve an image with high resolution [35].

[3] Super resolution methodologies are used to increase an image resolution either by breaking the "diffraction-limit" of the system or breaking the restriction of the "imaging-sensor". More information is in http://en.wikipedia.org/wiki/super-resolution

[4] Eignfaces technique use some eigevector to calculate vision and imaginary perception issues of individuals' faces resolution. Eigenface idea was recommended and improved by Matthew Turk and Alex pentland in 1987 as an initial face recognition method. More information is in http://en.wikipedia.org/wiki/Eigenface

4 Legal aspects in use of biometrics

Biometrics characteristics include a lot of sensitive and private data that could compromise people privacy, civil liberties and it can be at risk of function creep action[5] [70]. For instance, DNA presents person diseases that are interesting subject for insurance companies. Furthermore, loss of anonymity when authentication technology regards to something you know or have is the other issue that should be considered over biometric implementation [53]. There are lots of discussion in applications of biometric technology comply with legal issues. The biometric data involves personal information more or less depends on its type and possibly identifying people regards to their biometric data. Hence, people should think about all probabilities whether a person can be identified directly or indirectly by using biometric system. According to privacy protection legislation nameless data can be executed and processed by biometric systems.

Law enforcement authorities have been utilizing biometric features extensively. For instance, huge fingerprint databases are used in investigation of forensic missions to identify criminal. People are aware of these types of databases and they are not worried about the crucial data of databases. When usage of biometric features comes for people authentication in daily life, then databases will be center of attention for third parties. For example, one of the third parties might be law enforcement authority who wants to take advantage of the information for their purposes, which is known as function creep attack [31]. An example of function creep is a Norwegian database for asylum seekers. This database includes asylum biometric features such as fingerprints that were disclosed to police in criminal inspection [26].

4.1Norwegian Legislation in Use of Biometric

In this part, we will express the legal principals and guidelines that must be considered before installing and during use of biometric system at places to provide necessary components, privacy and security over people identification and authentication.

Some of the core principals of data protection law refer to data collection and the others focus on data processing. Second core principal of data protection laws called minimality emphasizes the personal data collected must be restricted to necessities to reach the aims of data collection. This principal is called proportionality or frugality principle as well. In other words, proportionality in personnel data collection states personal data must be non excessiveness, relevant, necessity with the certain purpose (55, p59). Minimality or proportionality principle expresses personnel data need to be erased, nameless or pseudonyms when they are not more require for the collected goal [6]. See also [55, p346]. Proportionality in data processing refers to the first principal of data protection law is that personnel data ought to be processed fairly and lawfully. Notion of fairness emphasizes the interests and logical exceptions of data subjects shall be realized by data controllers. To state difficulty, data controllers in data collection and further processing should not break data subject privacy, autonomy and integrity. Beside data processing aim should be transparent for data subject. However, make decision about what is fair certainly alter over time. [55, P58]. To achieve fairness and lawful principal in data

[5] Data collected use for other purpose differ the original aim [70].

[6] See Art6(1)(e) of the EC Directive and Art 5(e) of the COE Convention.

processing, the aim of processing collected personnel data should be a legitimate and lawful purpose. Moreover, purpose of further processing should be compatible with the aims that personnel data are collected at first [55].
Two principals, proportionality and purpose are fundamental needs to argue whether a biometric system satisfies the legal and legitimate agreements. Although use of biometric system should be done by informing the data protection authorizes because of privacy concerns, sometime the authorities allow to set up a biometric system by providing two main mentioned principals because biometric system can increase privacy if apply minimality principle in personnel data. In contrast with methods work based on possession and knowledge attributes. Biometric systems have capabilities to make anonymous and re- identification of a person infeasible in biometric systems that provide more privacy. Privacy friendly biometric system typically store a summary of templates processed during enrolment and acquisition phase. To secure the summarized templates, biometric system employs either one-way hash or encryption algorithms. However, as biometric templates collected from people in various times are not same using one-way hash and encryption techniques implementing a privacy friend biometric system is impossible [31].
Proportionality and Purpose identification Principals in Biometric in European Countries:
Some expresses have carried out about use of biometric related to minimality principal by the European data protection manager or Data Protection Working Party. DPWP committee emphasizes some factors in performing biometric authentication systems in companies/organizations and places. First factor states using biometric template which includes less crucial information instead of raw biometric data that typically presents sensitive information about data subject. Second factor stresses templates must not subject to sensitive information. This issue is unavoidable as we argued before about reconstructing original biometric information and authentication/ identification processes for biometric features. The Data Protection Working Party expresses biometric data shall be comply with purpose and proportionality like other data. The committee illustrates to have more privacy for authentication/verification purpose; biometric data should not be stored on centralized databases because a biometric sample presented at enrollment time by a user will be compared with already collected sample of the same user. Authentication process follow (1:1) search pattern and there is no need to find a match in a central database. Biometric identification follow (1: N) search pattern which refers to identify a user between huge number of collected samples. Hence, establishing a central database includes all users templates suppose is unavoidable [52].
Prior checking will be required by data protection authorities if biometric data is going to use for high security cases. Prior checking for identification and authentication aims depends on DPWP decision which is not clear on this context. In other words, DPWP emphasizes proportionality and purpose principles are two important elements in law for biometric system. The committee does not provide any definition and guidance for proportionality principle in details such as non-excessiveness, necessity and relevant [6]. Retention time of biometric data is another important criterion by data protection committee. It means biometric data shall not be kept more than requirement time and shall be removed when biometric system is no longer operational[7] . Original biometric data should be deleted,

[7] Article29. See appendix B

nameless and useless[8]for facial image, fingerprint and voice features for identification purpose[46].
There argue is choosing biometric type to increase security. For example, using hand geometry, hand vessels instead of fingerprint that remains accidentally on surfaces. The European data protection law committee believes biometric data ought to be processed and employed after risk assessment, apply human rights respect to European provisions [6].
The data protection authorities and court make decision with respect to fair and lawful processing principle and purpose specification principle in use of biometrics feature in authentication and identification systems. Fair and lawful and purpose principles are known proportionality [6]. However, there might be different decision for using biometrics characteristics for a specific case in various countries. The UK data protection authority has allowed to students use of fingerprint in order to gain access to schools restaurant if suitable protection has been applying at the schools. Use of fingerprint for the same aim has been prohibited by law in France. In Germany the data protection authorities emphasized that fingerprint image should be saved at the cards microchip instead of database. Many samples exist about various decisions about use of biometrics characteristics for same circumstances in different countries. It seems proportionality area and purpose identification principle are very vast, then making final decision to apply these two fundamental principles to cases depends on the target country court system. Final decision for use of biometrics technology in companies/organizations in Norway is made by both the Data Protection Inspectorate and the Data Protection Tribunal or PVN. PVN accept the Data Protection decision and sometimes revoking decision of the Data protection Inspectorate for some cases. The Data Protection Inspectorate makes decision about acceptance or denying use of biometrics with respect to some factors as below:

- Article 12 [9] of the Norwegian personal information emphasizes for employing unique identification feature such as fingerprint, iris, retina, hand vessels blood pattern, hand, etc there must be actual reason for use of identification system. In addition, the method should be necessary for that kind of identification.
- Legal base processing that biometrics data comply with it should be according to needs of articles 8,9,11[10] of the Data Protection law[11].
- Raw biometrics image and biometrics template created from it, should be considered the same as personal data. Because according to legal definition in the data protection law personal data is something can identify an individual directly and indirectly.
- Implementation encryption methods are not enough to allow a biometrics system to be implemented. Utilizing encryption techniques increase security and it will have meaning when the primary purpose provides the law needs [48].
- Data Inspectorate stress biometrics can be used for authentication purposes when essential. In general, the Norwegian Data Protection authority is same as the policy declaration by European Union/Data Protection Working Party and the consultative committee of the 108 convention:
- There must be special consideration if unique and singular biometrics feature

[8] http://www.bioprivacy.org
[9] Article12: Any type of identification includes national identity number can be used only if there is an objective requirement to perform the identification [6].
[10] See Appendix B
[11] See Appendix B

is going to use for identification purpose.
•Biometric techniques should not be used when other types of non-invasive alternatives are accessible to obtain the interest security purpose.
•DPWP behaves with biometrics images and templates such personal data since both are identifiable and partially unique.
•Data Protection authority know the proper level of encryption for providing suitable security.
•Data Protection authority have knowledge of difference between biometric identification and authentication [6].

4.2Case study

We will review some cases to find out how the Data Protection authority made decision to implement biometrics systems in some places in Norway.

REMA1000 is a famous chain store in Norway. Needed a method in order to control work time registration of their employees. Personnel entered their personal ID number for authentication on the system. REMA1000 decided to use fingerprint instead of the previous authentication method in order to prevent the employees to share their personal ID number together and register for each other. According to Article12 of Data Protection law REMA1000 had an actual objective need for authentication. Whether the objective need can comply legal and "necessity" needs for this intrusive authentication technique. This subject refers to proportionality principle then balancing test seems is an essential requirement to make decision. Data Protection Tribunal or PVN declared there can be alternatives for REMA1000 because using fingerprint to register daily working time has deeper meaning than a simple registration. It distrusts and subverts relationship between employees and employer. However, biometrics technology is an accurate authentication technology. In such cases risks and results derived from biometrics usage will be reviewed versus advantages present and security needs. For instance, library school and shops require less security than servers at a governmental organization. Moreover, Data Inspectorate believes REMA1000 can use less intrusive methods.[12] Proportionality principle includes subjects should take to account when discussion and concerns is about security levels, spoofing attack, effect of human factors, social, cultural, legal, economic and technical issues. In addition, Inspectorate has different ideas about security and obscure balancing factor for various positions. These allow to Data Protection authorities to have important, special and elastic role in inspecting balancing need in making decision for use of biometric systems which is logical and unavoidable [6].
Second case that we want to review argues about security level between biometrics and smartcard.
Tysyaer Municipality applied biometrics to access control of all new laptops and some desktop PCs at their organization. Data Inspectorate pointed using smartcard with password can present similar security level with biometrics. On the other hands, PVN mentioned smartcard might have risks that using fingerprint for authentication for instance does not present them. In the other words, PVN believed that combination of smartcard and password cannot provide higher security level than biometrics. It is clear main concentration for making decision is according to security not balancing factor. It means "necessity" element is an

[12] http://www.personvernnemnda.no/vedtak/2006.htm

alternative because it makes easy understanding of objective need for security.
Biometric systems are not robust against identity theft. Besides, 0.1% False Positive error rate is a high error rate than people can think because it clearly poses biometrics systems are not resistant against adversaries [49, p19]. On the other hands, smartcards are suitable solution for "Website ghosting, phishing and spam" [49,p11].
There is a discussion about identification issues when focus and priority is on convenience use of biometric identification versus traditional methodologies. A person is going to be identified should present at the time of identification. Furthermore, user does not require to memories a password with biometric identification. However, the probability of cheating should not be neglected. Some people think that biometric identification is the best and the last way to keep safe assets of a company or organization. A mixture of smartcard and password poses more accuracy, hard to spoofing and they do not reveal any information related to health care situation and genetic. Biometric technology adds some attributes to security protocols. Hence, its weakness should be mentioned as a portion of the protocols with special attention in its implementing process. Therefore, comparing smartcard with biometrics indicates none of them is better than the other and we cannot think about biometrics system as a replacement for keys, Token, smartcards or passwords [6]. Some specialists believe only combination of traditional technologies such as smartcard with biometrics features provide a higher security level than the two mentioned solutions [49].
Smartcards refer to an accurate identification technique which was neglected by the Data Protection Tribunal/PVN for Tysyaer Municipality case because the PVN stressed on difference between smartcard and biometrics technology. Therefore, the PVN decision will be rational if "simple, secure and robust" were logical requirements for final purpose. Biometrics provides comfortable and simplicity needs besides robustness and security at the same time as comparison with the other authentication methods [6].
The Data Protection Working Party and consultative committee emphasize avoiding unnecessary and central storage of biometrics data because it is related to proportionality principle of biometrics data. As mentioned before, central data base include personal data is at the risk of misusing, function creep, cyber attack and terrorist attacks. Making decision about implementation of biometrics system in an organization/company according to proportionality principle refer to another critical element that is well-known to consent factor which is primary principle in provisions data protection law in connection with fair and lawful principle for processing individuals private data. Consent implies personal data processing is possible with agreement of the data subject, unless there should be a specific conditions mentioned in law. In addition, if personal data involves sensitive information additional agreement is necessary. Norwegian opinion about consent determines complete alteration of collected biometrics data is forbidden even with considering consent principle [6].

4.3Legislation outside Norway

There are not much study and related work in use of biometric in Norway. Therefore, in this part we will introduce countries that are well known in employing biometric systems in different areas inside their region.
Biometrics technologies have been improved during the past years. Although it is not completely mature now, it can be implemented with admissible and considerable success and fair price. Robustness and drawbacks a biometrics technology will determine the specific biometrics is good enough for certain

applications. As mentioned before utilizing biometrics together and by possession or knowledge based techniques decrease the number of fraud [37].
A set of factors caused a growth in use of biometric on government and commercial places. Countries concern about their citizens security and safety particularly against terrorism. In addition, escalation various type of fraud such as identity theft. Besides, user acceptance has increased in general. Furthermore, accuracy of biometric solution has been increased and effort against illegal immigration is the other reason for rising use of biometric. The United States recently has spent $1billion budget in order to create very huge database includes biometrics characteristics such as DNA, fingerprints, signature, etc in relation to terrorism concern. Collecting, sharing, storage, usage and analysis of people biometric features have been escalated among departments that are portion of the United States federal government ordered by bush in 2008. Moreover, the united States were planned to deploy facial biometric for its citizens in 2005. Facial recognition system deploys ability to recognize people at up to 500 ft. These applications are against national privacy, civil liberties and increasing danger of identity theft derived from criminal aims remotely [38,4]. The system *El Camino Hospital* in California is implementing palm vein biometric authentication system in order to register and identifying new patient. It is a non- invasive and accurate technology for identify patients in opinion of responsible people [66].
Government cooperation has been improved biometrics technology excellently in Germany until 2009. For instance, issuing E-passport for all Germen nationals. E-password includes a chip that keeps a digital photograph and usually four fingerprints from each hand. There are also new rules related to work visa involve fingerprint, iris scanning and digital photos. These improvements in use of biometrics technologies in Germany not only because of government desire holding German borders safe but also because of the deadline established by U.S.A for "visa-waiver" countries. Moreover, Germany is one of the first countries that use biometrics authentication to preserve German athletes at the Olympic games against terrorist activities. The visitors get an ID card involves visitors' fingerprint then they gain access to the places [4].
UNITED KINGDOM is one of the countries with a lot of discussion in use of biometrics in industry and access control applications. Although there are many debate against use of national biometric ID card include individuals' fingerprint, the British parliament skipped relevant laws and made decision to use it in 2007. You can see more information in [37].UK citizens had to apply for an ID card with their biometric data from 2008 when they want to renew their passport. The biometric characteristics are used comprise: face recognition, fingerprint and iris scanning. The crucial personal data will keep at National Identity Register as databases. Criticisms about implementing this project are because some believe databases are at risk of security attack [39]. For instance, in some school at UK fingerprint scanner systems uses for making easy the process of withdraw of parents account for their children meal. The responsible person for this job can provide a report of student food habit for their parents. Critics believe it damages choice liberties of young persons. Furthermore, information about student habit might be leaked by meals provider for schools to health services such as insurance companies.
Biometrics technologies are performed by Citizenship and Immigration Canada and the Canada Border Services Agency particularly in border security and immigration [4].
"Australia is the first country to introduce a biometric privacy code." Australia uses face recognition as biometric data for passport and border control [39]. In addition, visitors planning to visit Australia very soon have to present their biometric data for authentication [4]. National Australia Bank is the first Australian bank to

implement a biometric-based system for customer authentication and employing a voice-based system for telephone banking customers [66].
In 2006 Sweden airline, SAS, deployed use of passengers fingerprint once when handing in their baggage and next time at the gate in order to automatic matching the passengers with their luggage. Passengers fingerprint is removed from the system automatically at the end of the passenger trip. This facilitates check in procedure and shows excellent escalation in security. Furthermore, authentication method related to fingerprint identification instead of presenting photographic ID. However; the use of fingerprint ID is optional for passengers and they can utilize an identity card or passport [40, 39].
Norway is one of 36 participating countries have been signed the Visa Waiver Program in order to travel to the United States for tourist or business aims to settle for 90 days without need to apply for visa. More information in[41]. Norway already issued biometric passport in 2005 [50]. On the other hand, the participating countries must present some requirements such as increasing law enforcement, being strict on border control, reporting of lost and robbed passports include blank and issued, working against terrorism, sharing security- depended information at the proper time with the United States and use biometric characteristics at their national passports with discretion of every country [42]. The use of biometrics features is increasing in Norway governmental activities such as asylum process, residence permit and passport control. Norwegian passport would involve a biometric data that already define by authorities. Besides, they are making schemes to use a citizens ID card encompasses biometrics feature. Furthermore, some rules and obligations have been deployed in Norway by authorities for cases that biometric characteristics can be used such as visa issuance and ID cards. Fingerprint is the biometric characteristic that Norwegian Data Inspectorate selected to control in SAS airline application. It is not a mandatory task for passengers to use fingerprint. Passengers are not willing to utilize fingerprint can do baggage check in manually. As a matter of fact, using biometric data in airline application of Norway guarantees the same passenger at baggage check in time boarding the plane, in order to prevent terrorist activities [43].Data Inspectorate emphasizes that the passengers must be informed before the registration process begins. They should know who is the controller, the aim of the behavior, the data will be revealed to whom, inform them that is a voluntary task to present fingerprints, they must know about how long template will be stored, passenger should know what kind of information will be stored about them and ability to correct or remove information [43].Another biometric application uses in Norway is camera surveillance for forensic purposes [53].

5 Data Collection

In this research we will utilize questionnaire method for data collection. The questionnaire for data collection should fulfill our purposes in this research project. Data collection is an important factor to accomplish the project because the analysis part depends on the amount of information and input data we will receive in the data collection phase. The amount of data will collect is one factor to determine the reliability of the derived results.
There could be other methods for data collection such as using web site, interview by phone, face to face interview, etc. Both web site and interview by phone methods will not provide sufficient information because of the expected low cooperation by the respondents. People will not trust a person that is asking different types of questions through the telephone without a former connection. Although face to face interview will be effective on respondents and provide more collaboration, this data collection method seems not suitable for this thesis as the companies/organizations are in different cities in Norway. Utilizing face to face interview is time consuming which might result in a reduction in the amount of data in contrast with questionnaire for this thesis.

5.1 Introduction

In Chapter 1 we provided two types of questions, including general questions and technical questions. We pursued the aims of this thesis via the questions. We want to know if Norwegian industry and organizations are using of traditional authentication technologies or biometric authentication technologies. We asked about authentication methods they are using or want to utilize to control access to areas and assets. We struggle to check if choices for the authentication method are based on knowledge or a set of factors and elements impress implementation of the biometric systems. Do they have any specific strategy in use of an authentication technology? Which factors need to be improved to deal better with security and privacy issues? In other words, the other goal of this study is recognizing factors that could make shorter passing period to utilize new and modern authentication technologies with/without traditional methods in Norway. The respondent opinion was asked about factors such as awareness, security, operational cost, user acceptance, Norwegian regulations and companies' size and type. Statistics give us some information whether Norwegian industry has sufficient knowledge on this topic. Although we have received only a few or no answers for some of the questions, acceptable numbers of responses are available for the rest of the questions. Hence, in Chapter 6 a comparison will be presented between existing scientific information about authentication mechanisms and the Norwegian companies/organizations opinion relevant to the studied authentication mechanisms. The comparison is with respect to factors such as awareness, security, privacy, etc. Moreover, familiarity and proper knowledge about modern technologies were estimated. For instance, fingerprint recognition, face recognition in the new laptops, keystroke dynamics and mouse dynamics. Norwegian industry awareness about traditional mechanisms is a subject that studies in this study. We emphasize that most of the companies are aware of security breaches in traditional methods. Then, they determined specific policies to reduce risk in use of them. Finding out Norwegian companies' willingness to implement the biometric system in the future is the other aim of this thesis. Relevant information can be found from questions eighteen and twenty four. From the data we can conclude which factors influence a future decision on the use of biometrics. However, there is not sufficient

information about the biometric systems Norwegian companies/organizations utilize to control gaining access to properties or resources. The amount of information the companies provide for the users about personal data that will be stored in use of authentication methods is not enough. Nevertheless, we have not received good enough data about users satisfaction in use of biometric authentication technologies.
We designed the questionnaire with respect to what we want to discover and learn from this research project. This helped us to pursue specific strategy for making questions to receive clear and relevant answers from the respondents.
Questionnaire includes both general and technical authentication questions in order to estimate the use of authentication methods in Norway properly. We used simple and understandable terms when writing the questions because we wanted the questions to be understandable for participants. Moreover, we wanted they spend less time to answer. Most of the questions were multiple chose and we tried to keep the number of open questions very low because we believe that respondents are not interested in replying open questions may be because they are time consuming to answer.
The questionnaire scheme has such a style that the number of questions participants will answer depends on their choice and answers in some questions. In other words, participants do not see some questions according their primary answers. We mentioned at the beginning of the questionnaire that the replying time is between 15-20 minutes. This was evaluated before sending out the questionnaire by filling in the questionnaire ourselves.
We ensure the name of the companies/organizations will be anonymited and we do not use the names in the research.

5.2 Questionnaire

We will look at the questionnaire content in general and highlight noticeable results for each question in this part. The questionnaire used for this thesis includes 34 questions.
The first nine questions ask if the companies/organizations utilize any types of authentication and biometric mechanisms, and what types of authentication and biometric methods have been applied in order to gain access to physical buildings and critical areas inside buildings, PCs, servers, printers, etc. We asked about special policy applied in creating username/password as an authentication method in place. The policy that might be existed for creating password is asked in Question ten. Questions eleven to fourteen investigate companies/organizations awareness, opinion about security and privacy that the authentication methods provide. Beside cost of operation is queried for the authentication methods study in this thesis.
Questions fifteen and sixteen inquire if participants know new laptops have fingerprint system and webcam to face recognition instead of the username/password authentication method.
Question seventeen asks if respondents are aware of that username/password can be more secured by employing biometric keystroke dynamics.
Question eighteen to twenty one inquire if companies/organizations we interested in using biometrics and if so, what type of biometrics are they prefer to utilize. Are operational costs and security of biometric mechanism comparable to username/password method or they are higher/lower that username/password method?
We are interested to know user reactions at the first contact with biometric systems through question twenty two to twenty five. Does user acceptance alter over time?

Do companies give information about what kind of information will be stored during usage of biometric system?
Question twenty six specifies what type of biometrics respondents prefer to use in the future.
Question twenty seven and twenty eight ask opinions about operational cost and biometric systems security versus username/password.
In Questions twenty nine and thirty we again ask for user reaction when understand they have to use biometric systems and if companies provide information for biometric system users about what kind of data will be stored in databases.
In question thirty one we are looking to find out factors why companies are not keen on using biometric systems in the future. Therefore, in question thirty two we ask how more knowledge will alter their ideas on utilizing biometrics.
Question thirty three investigates if Norwegian legislation hinders implementation of biometric authentication techniques in Norway.
Size and type of companies/organizations participated in this thesis is asked in question thirty four and thirty five.
In question36, we ask for further cooperation related to this thesis from the participated companies. At the last question, question thirty seven, we offer final results of this thesis for companies/organizations that interested in. Thus, we ask their contact information in order to send the results for them.

5.3 Distribution

We sent the questionnaire to 260 companies/organizations. We did not restrict ourselves to a specific industrial field when sending the questions. We desire to know about biometric systems present in various industrial fields. We have received fifty answers.
The Quest- back website was the system we used to send the questionnaire because it does not only send email in more economical way but it is also a quick method. In addition, most of the companies and organizations have email address and internet access. Some companies utilize a message link in their website instead of email address, we sent a message if they are interested to contribute in this research project inform us. We set reminder time one week after first sending which considerably effected on receiving new answers. We also asked face to face from some individuals or sending email to some people and familiar persons if they would like to contribute to participate in this thesis by answering the questionnaire.
Some of the companies/organizations sent an email that they have a policy inside companies and cannot participate in your survey.

6 Analysis and Results

In this chapter two purposes will be pursued. First we will explain how collected data has been analyzed. Second we will look at the results obtained in this thesis.
We will look at the each question, analysis their data and make a conclusion. Next, we will find relationships between different questions and answers in order to reach and compare their effects on each other.
We will use quest back and Excel software to analysis the data. Then results will be presented by various types of chart or table.

6.1 General statistics on responses

In this section we will investigate responses to the questions in sequence. The number of response differ from question to question because of the relation exist between questions. We will write our comment and conclusion for each question.

1. Is your organization/company using an authentication mechanism for physical access to the building?

Alternatives	percent	Value
1.Yes	91.7%	44
2.No	8.3%	4
Total		48

Table 2. Use of the authentication methods for the building.

Total number of people answered to question one is 48. High percentage of the companies employed authentication methods to gain access to the building. A few numbers of the companies/organizations have not implemented any authentication method to enter to the building. Two of the companies have fewer than five personnel. Two other companies involve people between 26-100. In general four of the companies are sort of small companies. Hence, size of the companies could be a reason that they have believed it is not necessary to implement an authentication method. However, some of the participated companies with few numbers of staff have been used an authentication method not only to control access to the buildings also for critical areas and the resources in their companies. We believe that performing risk analysis procedure to acquire sufficient comprehend refer to security requirements is the other important factor that causes the companies be anxious about lack of an safe authentication methodology in place even with small and medium size. The companies/organizations with number of personnel between 26-100 and 101+ are distributed into three categories with respect to the strategy have chosen to employ the security technologies:

- The companies/organizations neither utilize an authentication method to control access to the building nor any controlling mechanism for the critical areas inside the building and resources like PCs, servers, etc.
- The companies/organizations have implemented an authentication method for gaining access to the building but not for the critical areas and the resources.
- The companies/organizations have carried out an authentication method to control access to the building and critical areas but not for the resources.

Considerable percentage of the companies/organizations have not applied an authentication mechanism is 34% of the participated companies. It could be due to either the companies/organizations are not aware of the security issues or do not take the security requirements as a critical and serious concern. The percentage has counted with concentration on use of authentication technologies in general. In other words, it concluded regardless to focus on specific authentication/identification methods for instance biometric systems implementation.

2. What authentication mechanism is your organization/company using for physical access to the building?

Alternatives	percent	Value
1. Visual (e.g. a guard)	14.29%	9
2. Card	19.05%	12
3.Card + (PIN) code	66.65%	42
4.Biometrics	0.0%	0
5.Other, please specify	0.0%	0
-1.Don't know	0.0%	0
Total number of answers		63
Total number of respondents		44

Table 3. Authentication methods used for building.

Total number of respondents is forty four for question two. In some question the sum of total number of answers is more than the total number of respondents. The reason is that the respondents had opportunity to select more than one answer for those questions.
High numbers of the companies/organizations utilize one of the traditional authentication mechanisms such as visual, card and card with PIN-code to control access to the building. Approximately 16% of the companies/organizations with number of personnel between 1- 25 utilize card + PIN code to access to the building. Almost 25% of the companies/organizations involve number of personnel between 26- 100 use card + PIN code in order to control access to the building. Noticeable percentage of the companies comprise staff more than 101+ utilize card + PIN code

for gaining obtain to the buildings, almost 59%. Number of the large companies participated is more than the companies/organizations with population between 26-100. Suppose the number of the companies/organizations with personnel between 26-100 was double of current number, still percentage of the large companies/organizations that use an authentication method to control access to the building is higher than the medium size companies.
Approximately 20% of the large companies/organizations utilize combination of visual method; card and card + PIN code for the building. There is not usage of the biometric systems for entrance of the building. It could be because the combination of card and PIN code methodologies introduces both safety and cost effective requirements among the authentication mechanisms. Furthermore, utilizing card + PIN code might be more economical than employing a person for visual purposes and using biometric systems particularly when companies have small or medium size. In other words, there is a proportion between provided security and necessary budget for card + PIN code method. However, issuing card for huge number of staff, losing card or sharing it with others are challenges in use of card + PIN code mechanism.
We believe size of the companies/organizations could be an important factor in usage of the authentication methods. Large companies/organizations are at risk of social engineering attacks. Hence, there ought to be an efficient security fence for the building entrances.

3. What biometric authentication mechanism is your organization/ company using for physical access to the building?

Alternatives	percent	Value
1. Fingerprint	0.0%	0
2. Face recognition	0.0%	0
3. Voice recognition	0.0%	0
4. Iris scan	0.0%	0
5.Other, please specify	0.0%	0
-1.Don't know	0.0%	0
Total		0

Table 4. Biometric used for building.

According to Table 3, there is not any company/organization that utilizes biometric systems to control physical access to the building. Therefore, the values are zero in the table 4.

4. Is your organization/company using an authentication mechanism for physical access to critical areas inside the building?

Alternatives	percent	Value
1.Yes	78.3%	36
2.No	21.7%	10
Total		46

Table 5. The authentication methods used for critical areas.

High percentage of the companies/organizations exerted an authentication technology to gain access to critical areas inside the building. On the other word, some of the participants have not employed any special authentication method for crucial places inside the building. This percentage is almost double and half of the percentage of the companies that do not have any recognition methodologies for physical access to the building according to the tables 2 and 5. Six numbers of the ten companies are companies have number of the employees fewer than a hundred. Critical areas comprise places include tangible or intangible assets, properties or resources of a company. According to table 6, we have recognized exerting an authentication mechanism for the critical areas more than depending on the size of the companies/organizations related to whether the companies have utilized a recognition technology for the assets such as database, servers, PCs, etc. This could be a reason for the escalation of number of the companies/organizations has not utilized an authentication mechanism for critical region inside the building. Therefore, the companies/organizations might conclude there is no need to employ a recognition method for the critical areas when they have an authentication technology to control access to the building. However, most of the companies/organizations with population between 26-100 and more than 101+ people have been utilized an authentication technology for the three locations in Question one, Question four and Question seven. See Table 11.

Number	Company size	Company Type	Access to the critical areas	Access to the servers, PCs, etc
1	1-5	Foundation	No authentication method implemented	Username/password
2	6-25	International commercial CO towards whole world	No authentication method implemented	Password only
3	26-100	Educational	No authentication method implemented	Username/password
4	26-100	Governmental	No authentication method implemented	No authentication method implemented
5	26-100	International commercial CO towards northern Europe	No authentication method implemented	No authentication method implemented
6	26-100	National commercial CO	No authentication method implemented	Username/password
7	101+	International commercial CO towards whole world	No authentication method implemented	Username/password
8	101+	International commercial CO towards northern Europe	No authentication method implemented	No authentication method implemented
9	101+	International commercial CO towards northern Europe	No authentication method implemented	Username/password
10	101+	Governmental	No authentication method implemented	Username/password, biometric

Table 6. Implementation of the authentication methods for critical and resources

5. What authentication mechanism is your organization/company using for physical access to critical areas inside the building?

Alternatives	percent	Value
1. Visual (e.g. a guard)	2.1%	1
2. Card	17.4%	8
3.Card + (PIN) code	67.4%	31
4.Biometrics	0.0%	0
5.Other, please specify	11.0%	5
-1 Don't know	2.1%	1
Total		46

Table 7. Authentication methods used for critical areas.

Table 7 shows most of the companies/organizations use one of the traditional technologies such as guard, card, and card + PIN-code to control access to critical areas inside their company/organization. There is not any statistics in usage of biometric systems to access to the critical areas inside the building. Some numbers of the companies/organizations have been exerted the other authentication technologies to physical access to critical areas inside the building. Three companies expressed that they give the key to the person should have access to the areas. Two other companies mentioned that they utilize safe code and PIN-code.

6. What biometric authentication mechanism is your organization/company using for physical access to critical areas inside the building?

Alternatives	percent	Value
1. Fingerprint	0.0%	0
2. Face recognition	0.0%	0
3. Voice recognition	0.0%	0
4. Iris scan	0.0%	0
5.Other, please specify	0.0%	0
-1.Don't know	0.0%	0
Total		0

Table 8. Biometric recognition methods for critical areas.

There is not statistics to prove utilization of the biometric authentication systems to gain access to critical places inside the building. The reason is that there is not any data for “Biometrics” in Table 7.

7. Is your organization/company using an authentication mechanism for access to computers, servers, printers, etc.?

Alternatives	percent	Value
1.Yes	87.2%	44
2.No	12.8%	6
Total		50

Table 9. Use of the authentication methods for PCs, Printers and Servers.

Table 9 shows noticeable percentage of the companies/organizations utilize an authentication methodology to access to PCs, printers, servers, etc. while small number of them has not applied any types of authentication technologies for the devices. Two out of six companies that do not use any authentication mechanism for the resources applied an authentication mechanism for critical areas inside the building. Three other companies do not utilize any recognition methodology for both critical areas and the resources. These corporations include two companies with size between 26-100 and one company with size more than a hundred. Another corporation is the company that has not exerted an authentication methodology for control access to the building, critical areas and the resources. This corporation involves 26-100 people.

8. What authentication mechanism is your organization/company using for access to computers, servers, printers, etc?

Alternatives	percent	Value
1. Token	7.0%	4
2. User name only	0.0%	0
3.Password only	3.0%	2
4.Username/Password	67.0%	38
5.Biometrics	9.0%	5
6. Other	14.0%	8
Total number of answers		57
Total number of respondents		46

Table 10. Access methods to recourses inside company.

Table 10 illustrates high percentage of the companies/organizations utilize username/password authentication mechanism to access to PCs, printers and servers in their company/organization. It could be because of first it is a cheap authentication method. Second, username/password has been utilizing for almost long time and then it is a common and familiar methodology in the industry. Third, use of username/password does not need much administrative tasks. It is controllable by applying some policies. However, its security risks could not be

neglected. Combination use of username/password recognition method with another recognition method could provide a growth in necessary security. On the other hand, small percentage of the respondents mentioned password only is the authentication method that has been applied in order to control access to the devices. These corporations belong to small size companies. Although the respondents mentioned token mechanism is more secure than username/password in question twelve, it has been utilized less than username/password method. The reason could be because security of username/password mechanism can be improved by applying variety of policies. For instance, resetting password after a while, set the policy not allow using previous passwords, etc. Servers and databases include sensitive, crucial and valuable information for third parties and adversaries. It motivates the companies/organizations to exert an authentication methods or utilizing the methods provide more security in their opinion such as biometrics. Fourteen percentages of the companies have been implemented other traditional authentication mechanisms:

- Card + PIN
- Smartcard W/PIN, & Certs. (PKI)
- Giving key to personnel that should have access to the servers.
- For printers using access card.
- Keys (locked doors)
- Smart card +Certificate +Username/Password
- Card
- Card + PIN

Most of the companies/organizations have been preferred to use the traditional authentication technologies.

The companies/organizations have been utilized visual authentication method to control access to the building, they have been implemented an authentication methodology for the critical places inside the building and resources such as servers, PCs, printers, etc. However, there is an exception. High number of the corporations comprises large size companies/organizations. See Table 11.

Number	Company size	Company type	Access to the building	Critical areas	Access to servers, PCs, etc
1	26-100	National commercial CO	Visual, card, card+ PIN code	card, card+ PIN code	Username/password
2	26-100	National commercial CO	Visual, card, card+ PIN code	card, card+ PIN code	Username/password, smart card, PIN, CERT
3	101+	Governmental	Visual, card, card+ PIN code	card+ PIN code	Username/password
4	101+	Governmental	Visual, card+ PIN code	Yes/ He did not know which authentication method used	Yes/He did not know which authentication method used
5	101+	Governmental	Visual, card+ PIN code	Card + PIN code	Username/password, for printers: access card
6	101+	International commercial CO towards Northern Europe	Visual, card, card+ PIN code	Do not use	Do not use
7	4000	International commercial CO towards Northern Europe	Visual, card, card+ PIN code	Visual, card, card+ PIN code	Token, username/password
8	101+	International commercial CO towards whole world	Visual, card+ PIN code	Card+ PIN code	Username/password
9	101+	International commercial CO towards whole world	Visual, card+ PIN code	Card+ PIN code	Token, username/password

Table 11. Implementation of the authentication methods for access to the building and resources.

The number of companies/organizations that used visual method should be ten regard to Question two and Question five. However, the number of the companies/organizations is nine in Table 11. It is because a company utilized visual methodology for two locations according to the row seven. Almost most of the international and governmental organizations are interested in use of visual method.

9. What biometric authentication mechanism is your organization/company using for access to computers, servers, printers, etc.?

Alternatives	percent	Value
1. Fingerprint	100.0%	5
2. Face recognition	0.0%	0
3. Iris scan	0.0%	0
4. Voice recognition	0.0%	0
5. Keystroke Dynamics		
6.Other, please specify	0.0%	0
-1.Don't know	0.0%	0
Total		5

Table 12. Biometric authentication system used for PCs, printers, servers.

Finger print recognition methodology is the preferred recognition mechanism by whole number of the companies/organizations for the resources. According to the table 38 in the part 6.2.3, only six companies/organization have been implemented the biometric system. One of the companies did not respond Question 9. The company has clarified finger print recognition in the laptops is used in the corporation. The ambitious can be because fingerprint recognition has distinguished long time ago. It has been utilizing for a long period in different applications.

10. Is a policy in place for creating and using passwords?

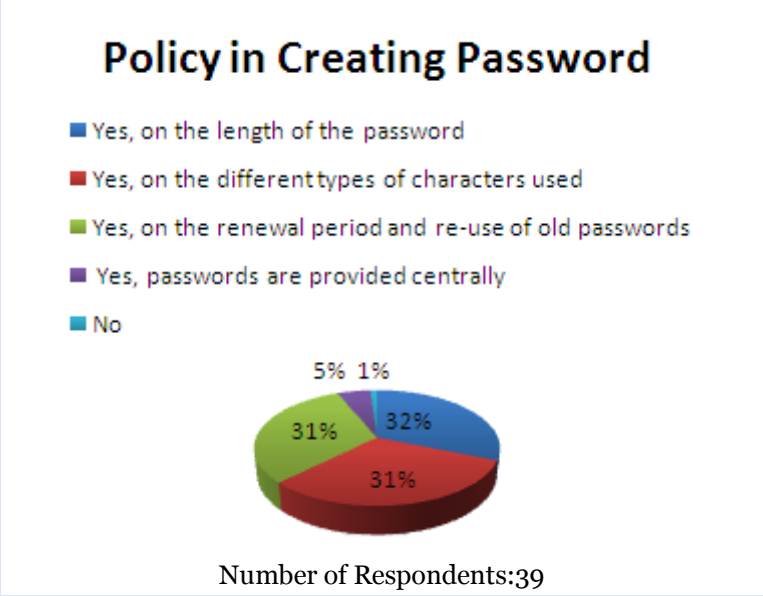

Figure 7. Policy in password creation.

Question 10 is a multi select question. Some of the participants have exerted multiple policies. Figure 7 illustrates more than 95% of the companies have limitations in password creation.
Password length, different types of characters, renewal password after a specific time, preventing user using previous passwords and controlling password mechanism centrally are examples of policies uses by the companies/organizations. All the limitations are in order to promote username/password authentication technology in general. For instance, variety in the characters and length of the password impress the time need for cracking in brute force attack. The time can be altered regard to the following formula which is analogous for MD5, crypt, LM, NTLM, etc: (possible chars) ^ (length of password). The great value for these two factors causes the time require to crack the password be lengthy. However, this formula is not correct for rainbow table. Rainbow table technology simply looks up to crack the passwords hashed by a hash function. Therefore, username/password authentication mechanism is vulnerable against rainbow table methodology[13].
Centrally password creation could be useful when the IT department motivates to be sure that password policies have considered properly. In addition, it eliminates the burden of password creation from the users.
These statistics prove that companies are aware of security breach in username/password methodology. Hence, they attempt to harden their system against possible attack via applying several policies for password creation.

11. Are you aware of the existence of the following biometric modalities (0: Completely unaware; 1: Heard of it before; 2:I know it somewhat; 3:I know it well; 4:I am an expert):

[13] http://en.wikipedia.org/wiki/Rainbow_table

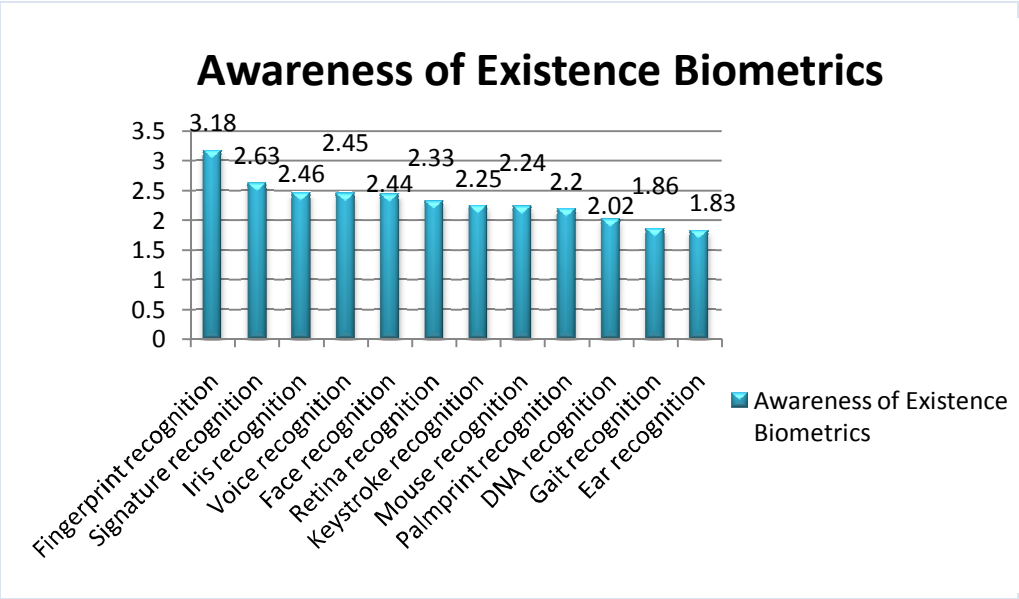

Figure 8. Awareness of biometric recognition methods.

The most well known biometric system for the respondents is finger print recognition. The lowest familiarity belongs to ear recognition and gait authentication respectively. Signature recognition technology is the second biometric system acquainted for the most of the respondents. There are approximately same familiarity for retina recognition, keystroke recognition, mouse recognition and palm print recognition. See Figure 8.
The companies almost have equivalent awareness for most of the biometric systems. Except fingerprint recognition, ear authentication and gait authentication methods. However, there is a considerable distance between the most familiar authentication methodology and the lowest one for the respondents. It could be since some of the biometric techniques are efficient in the various applications such as finger print.

12. Do express your opinion on the security of the following authentication mechanisms (0: No opinion; 1: Unsecure; 2: Slightly unsecure; 3: Neutral; 4: Slightly Secure; 5: Secure):

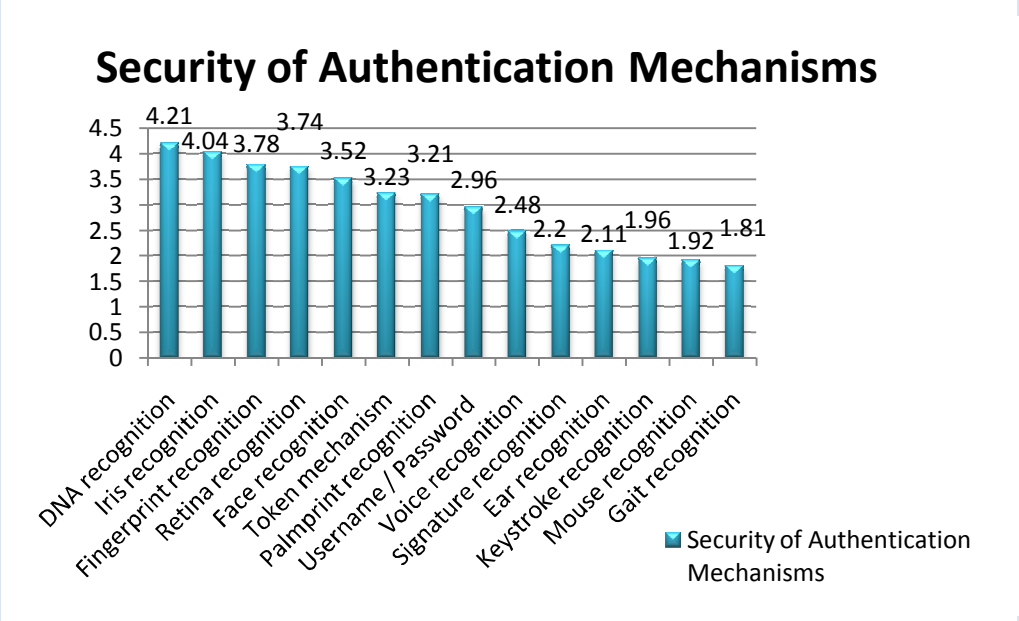

Figure 9.Security of authentication methods.

There is a great distance between provided security by DNA recognition mechanism with mean 4.21 and gait authentication as a lowest secure authentication mechanism with mean 1.81. Iris recognition and finger print recognition are two others secure authentication technologies. Retina is introduced a secure authentication methodology after fingerprint feature.

Two traditional authentication mechanisms token and username/password are considered to have almost neutral security attribute. These two have recognized more secure than biometrics such as voice print, signature recognition, ear recognition, keystroke recognition, mouse recognition and gait authentication in the respondents opinion. The respondents believe that token even is more reliable than palm print.

Human physical characteristics have been introduced safer than human behavioral characteristics such as voice, signature, keystroke, mouse recognition and gait authentication.

There are some studies for security of the biometric systems with respect to reliability and confidentiality features that play key role to decrease security risks [58, p150]. See Table 13.

Security	Biometric feature				
Very High	Iris	DNA			
High	Retina	Fingerprint	Palm print (H to M)		
Medium	Face(M to L)				
Low	Voice	Signature	Gait	Keystroke	Mouse
Very Low	Username/password	Token			

Table 13. Security of biometric features.

Security level is reduced from left to right in each row of the Table 13.
Iris authentication method is more secure than DNA, retina recognition and fingerprint recognition methods. Iris works well through eye lenses even colored one. Iris guarantees high speed and highly distinctive biometric feature even between identical twins. On the other hand, DNA cannot differ between monozygotic and it takes days for comparison results. DNA not only supports lower speed than iris, it also is simple to steal [58]. Hence, we believe iris proposes more security than DNA recognition systems.
Palm print recognition method is more secure than face recognition. As comparison with the participants' opinions that have introduced DNA security is more than iris recognition. The respondents mentioned face recognition technology provides more security than palm print recognition technology. The participants expressed that security provided by gait authentication is lower than keystroke dynamics and mouse recognition methodologies. This opinion could be due to the respondents have the lowest familiarity with gait authentication with regard to the Question eleven. The statistics determine the security of gait authentication is not only higher than keystroke dynamics and mouse recognition also it is higher than username/password and token mechanism. The respondents are more acquainted with fingerprint authentication method than retina recognition. Hence, it probably causes the respondents construe fingerprint is more secure than retina recognition.
There was an agreement between the united state and Ireland to accept digital signature in 1998. European countries constructed a frame work for digital signature recognition in 1999[14]. These histories procure the use of signature recognition return to several years ago. Therefore, people include the participants probably have good comprehend of signature authentication method. The familiarity have not caused the respondents conclude that signature authentication introduces higher security than the more secure authentication mechanisms. This expression also is correct for voice recognition. The participants mentioned have good knowledge about voice recognition. As a matter of fact, utilization of signature

[14] http://en.wikipedia.org/wiki/Electronic_signature

and voice authentication methodologies for almost long time caused advantages and drawbacks of the methodologies disclose for the respondents. Hence, signature and voice authentication technologies are well known for the people.
As a result awareness of the participants could have significant impression in security classification of the biometric systems by the respondents.
Ear recognition accuracy has been introduced as unknown [58, p154]. Therefore, determining Ear recognition belongs to which of the categories is not easy. This method is used in the police organizations to identify criminals by optophone Ear shape verifier device in U.S.A [67].
Token based devices such as key and card and username/password support very poor security when they forgotten or stolen [58, p182].

13. Do express your opinion if the following authentication mechanisms can provide privacy for the users (0: No opinion; 1: No privacy guaranteed; 2: Little privacy guaranteed; 3: Neutral; 4: A lot of privacy guaranteed; 5: Privacy totally guaranteed):[15]

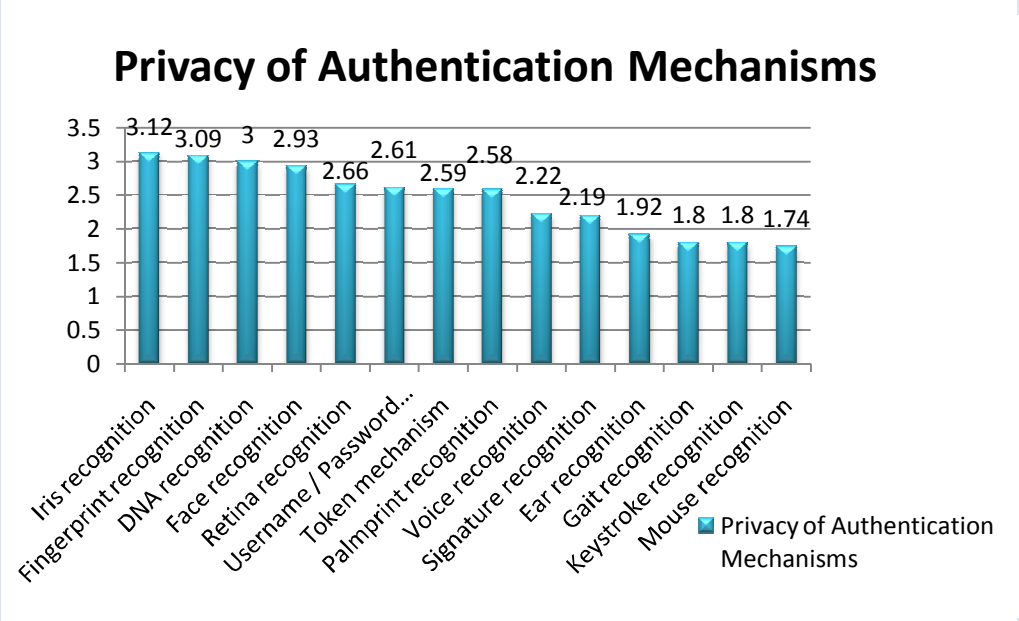

Figure 10.Privacy of authentication methods.

Figure 10 illustrates the individuals' opinion about privacy provided by the authentication mechanisms. Although there is some changes in the privacy provided via the authentication methodologies, most of them present same level of privacy. The authentication mechanisms are classified into three groups according to their privacy.

- The first group comprises biometric authentication technologies such as iris

[15] http://www.biometricscatalog.org/Privacy/Default.aspx?sindex=3

recognition, finger print recognition, DNA recognition and face recognition methods with mean 3.04. This group supports high privacy in the participants' opinion. Iris guarantees the highest privacy.

- The second group involves retina recognition, username/password mechanism, Token method and palm print recognition. This group introduced medium privacy in the respondents' perception with mean 2.61. Retina poses high privacy in the group.
- The third group encompasses authentication methods with low privacy with mean 1.95. Voice recognition, signature recognition, Ear recognition, gait authentication, keystroke recognition and mouse recognition belong to the third group. Mouse recognition provides the lowest privacy among these three groups.

Privacy argues the amount of personal data that a biometric system might reveal. In addition, a biometric feature will be privacy invasive if original image of biometric feature is reconstruct able from the raw data.

- Fingerprint recognition: Recent scientific attempts present fingerprint could be re-fabricated from minutiae template. The latest attempt was published by Cappelli et all in 2007 [70]. For example, a complete fingerprint can be utilized to open a door [69].
- Face recognition: Companies might implement facial system to trace shopping habits of their retail customers [73]. Face recognition can be done overtly or covertly at a distance. Therefore, it refers to fear of surveillance and determines people identity [78, p56].
- Palm print recognition: The structure of the lines in palm print contains personal information such as genetic disorders [80, p31]. Advantage of palm print is that the original palm print image cannot be reconstructed from the raw biometric template [80, p25]. Palm print can be utilized instead of fingerprint because some individuals do not provide proper fingerprint image because of physical job or skin problem. Palm print is very unique feature even between identical twins who present the same DNA feature [80, p15].
- Iris recognition: Iris identification mechanism discloses some health care information such as AIDS, diabetes and pregnancy [79, p70]. However, there is no need to store any private data in a database in iris recognition systems. Encrypted iris template causes reengineering of the original data and tracking individuals infeasible [79, p43].
- Retina recognition: Retina reveals preserved health care and limited medical information [74]. This information encompasses AIDS, diabetes and pregnancy [79, p70]. Retina recognition is a privacy sensitive methodology. It reduces user acceptance and cooperation. Therefore, retina utilization may not recommend for public usage. But retina authentication is a preferred method for the high security application such as military.
- DNA: DNA specifies potential of further privacy concerns. It involves information such as health situation, genetic information, ethnic, etc [72, p11]. This information can be passed to commercial companies, insurance companies and government. DNA also could be steal and abuse in a crime scene. The reason is that there is no sensor in DNA recognition for real time identification. Hence, most of the biometric experts do not accept it as a biometric feature [78, p53].
- Ear recognition: we could not find information that proves ear shape recognition is a privacy sensitive method and revealing personal

characteristics.

- Voice recognition: voice can be at risk of eavesdropping adversary. Vocal information might be used for blackmail attack to acquire benefits from the individuals. Voice privacy can be supported by various scrambling methodologies [75].
- Signature recognition: signature can be miss used to identify and locating individuals with other data sources.[16] Hash function and cryptology methods promote signature privacy.
- Gait authentication: It can be implemented covertly. It does not need individuals' interaction. Gait characteristic had not been employed for identification/verification aims till recently. The reason was due to lack of accurate and inexpensive sensor. Gait feature is well-known for two applications. First, it utilizes in orthopedic medicine field. Second, it can be implemented for recognition and rehabilitation purposes [81, p42]. Moreover, if all gait motions are captured and studied a signature reach for gait that introduce gait feature as a biometric authentication method. Gait discloses people state [81, 25]. For instance, drunk and injured situations [81, p42]. Utilization of gait recognition technology in the medical and the authentication applications distinct from each other.
  If medical document of patients reveal by medical centers, the documents will provide profitable information for the third parties such as insurance companies. People privacy can be at risk in this manner in gait authentication.
- Keystroke recognition: keystroke dynamic capture user activities during a session. The activities are controllable by administrators remotely [76]. Keystroke dynamic discloses some limited health information such as recognizing the user is a disable person. Furthermore, it could show the user is working with the PCs is a local person or foreigner by typing rhythm. This issue will be solved as people learn and improving their typing abilities.
- Mouse recognition: mouse recognition can be utilized for identifying users such as game players, recognizing musical and entertainment interests, etc. A compound of a camera and a mouse sensitive to pressure estimates users' anxiousness and interests to a specific subject. This is recognizable via facial emotions from the camera and users muscle anxiousness captured from pressure sensitive sensor on the mouse [77]. Age of people and a problematic wrist is identifiable through working style to the mouse. This information could be valuable for some companies/organizations that sale relevant product.
- Username/password: Username and password mechanism seems are not privacy sensitive. Username/password can be recreated in case of lost or forgotten.
- Token mechanism: Token can contain information that discloses anonymity of a person. For instance, in voting electronic system that each voter receive a token to accomplish voting process [82]. Moreover, token can pass to others by individuals.

[16] http://en.wikipedia.org/wiki/Personally_identifiable_information

Based on information provided above for privacy sensitively, biometrics privacy is concluded for the authentication technologies. The authentication methods are classified into groups based on privacy preserving. Moreover, this classification is according to sensitivity of the information each class reveals. In each group provided privacy by the authentication technologies decrease from left to right.

- First group encompasses username/password method, voice recognition and mouse recognition that provide very high privacy level in sequence.
- Second group comprises token and signature recognition methods. These two authentication mechanisms guarantee high and almost similar privacy level.
- Third group includes gait authentication and keystroke dynamics that provide medium privacy level. This technologies discloses limited health problems.
- Fourth group involves face recognition, palm print recognition, fingerprint recognition. This group of authentication mechanisms supports approximately low privacy. Face recognition identify people passively or actively. Furthermore, it discloses people habits and custom. Although palm print encompasses more feature than fingerprint and then revealing serious personal information such as genetic problems, it is infeasible to reconstruct palm print from raw data in contrast with fingerprint characteristic. Furthermore, fingerprint is vulnerable against stealing and misusing.
- Fifth group comprises iris recognition, retina recognition and DNA recognition. These three authentication technologies divulge less and more health care information. Hence, this group guarantees very low level of privacy. We believe iris provides more privacy attribute than retina because iris does not need to store personal data that have not already existed. Furthermore, re-fabrication original data from encoded iris template is impossible. Moreover, retina discloses both limited and sensitive health care data. Privacy situation is even more worth for DNA. DNA not only reveals very accurate and sensitive personal information also it might be stolen and abusing.

To summarize, template-based biometric systems are not privacy preserving. But biometric systems still provide high safety level for a system especially when they use with one or both authentication mechanisms such as token and password. Hence, security and privacy will be guaranteed [73, p12]. Furthermore, some factors should be considered when implementation a biometric system. For instance, security risks, implementation purpose(s) include identification/verification, number of users, environment, results derived from information leakage, etc [69].

14. Do express your feeling about the cost of operation for a system using the following authentication mechanisms (0: No opinion; 1: Very expensive; 2: Slightly expensive; 3: Neutral; 4: Slightly cheap; 5: Very cheap):

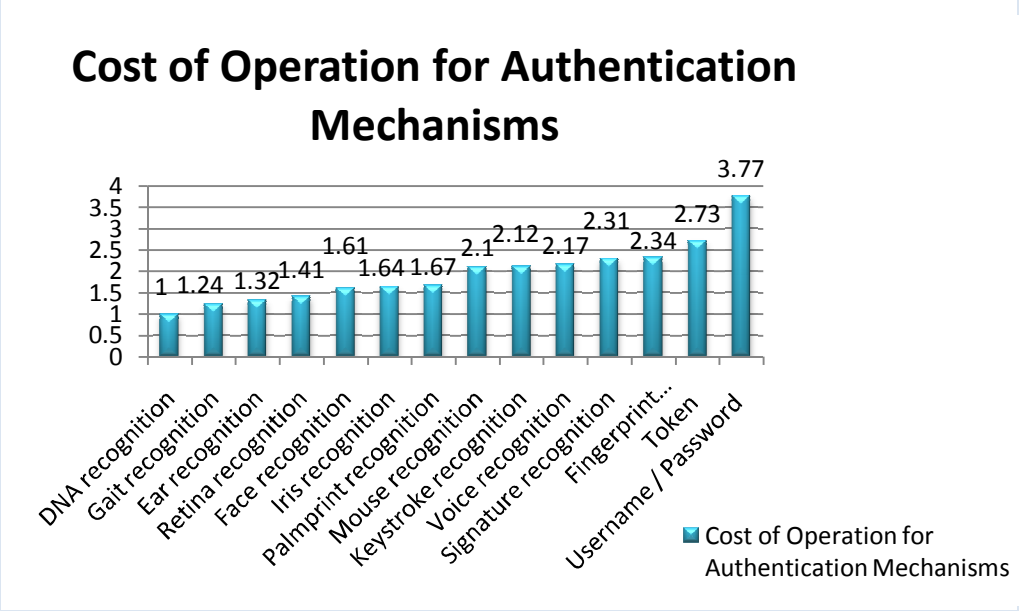

Figure 11.Cost of operation for authentication mechanisms.

According to Figure 11 username/password are the cheapest authentication methods. Cost of operation is escalated from username/password methods to DNA. In other words, the highest operation cost has been assigned to DNA recognition. Gait recognition has introduced the second expensive authentication mechanism. Face recognition, palm print recognition, iris recognition and retina recognition are approximately at the same level of operation cost. Keystroke recognition is known approximately as expensive as mouse recognition.

There are some differences between the statistics discovered from the respondents and operational cost has been assigned to the biometric systems. The opinions of the respondents are mustered in the table14. Cost increases from up to down in each column at the table. For instance, at the first column fingerprint is more economical than signature authentication technology.

A scientific study in the implementation cost of the biometric authentication mechanisms will be provided in this part. The biometric systems that require low budget to operate are introduced at first, then medium and high capital consuming authentication methods. See Table 15.

The biometric systems that need low cost for operation include: voice recognition [56], face recognition [56], keystroke recognition [62, p95], fingerprint recognition that is almost the most economical authentication method[17] with regard to the benefits are introduced, signature recognition [60], mouse dynamic recognition, and palm print recognition [59]. There are some experiments performed in mouse dynamic which demonstrate it is a cost-effective method. More information is found in [61]. Cost of operation and necessary budget to purchase the hardware equipments for keystroke dynamics authentication could be decreased and differing with the physical biometric systems. However, the budget of administration and software are as resemble as for the other biometric systems [62]. This probably is correct when keystroke dynamic should be implemented in large scale companies/organizations.
The biometric system requires medium amount of operation cost comprises hand geometry recognition which has not been study in this thesis.
The biometric systems introduce high operation cost encompasses: iris recognition [58, p144], ear recognition [65], gait authentication [64], retina recognition [56] and DNA. DNA analysis for forensic cases requires greater fees than the commercial utilizations [63, p30].

Operation Cost				
Very low	Low	Medium	High	Very high
Fingerprint recognition	Voice recognition	Palm print recognition	Gait recognition	DNA recognition
Signature recognition	Keystroke recognition	Iris recognition	Ear recognition	
	Mouse recognition	Face recognition	Retina recognition	

Table 14.opinion of companies about operation cost of biometric systems.

[17] http://media.wiley.com/product_data/excerpt/26/07645250/0764525026.pdf [p4]

Cost of operation collected from various references about biometrics systems studied in this thesis has been collected in the table15.

Operation cost				
Very low	Low	Medium	High	Very high
Voice recognition	Keystroke dynamics	Palm print recognition	Ear recognition	DNA recognition[18]
Face recognition	Mouse dynamics recognition	Hand geometry recognition	Gait recognition	Iris recognition
	Signature recognition		Retina recognition	
	Fingerprint recognition(low to medium)			

Table 15.Scientific statistics about operation cost of biometric systems.

Voice and face recognition are the cheapest biometric systems in sequence. In contrast respondents have been considered fingerprint and signature recognition as the most economical authentication methods. Cost of fingerprint recognition could be low to medium and it introduces as almost the economical authentication method. But its cost is not less than signature recognition, voice recognition and face recognition authentication mechanisms in reality. We inform operation cost of keystroke dynamics mechanism is low because it only needs a sensor, software installation and maintaining. In addition, it does not need to train users [57]. However; it could be more expensive than fingerprint authentication mechanism when it should be implemented for large scale organizations with high number of PCs [57, p9].

Palm print recognition method not only is more unique than fingerprint authentication mechanism but also comprises more feature than fingerprint [59]. Hence, there should be more complicated algorithms to analyze the templates with noticeable amounts of data. Moreover, computational cost will be high. Furthermore, palm print sensors are larger and then more expensive than fingerprint systems [7002]. These factors are reasonable reasons to believe that it requires medium cost for operation. Hand geometry is a type of the biometrics needs medium cost. Hand geometry requires a little user training because user should know to squeeze their finger in enrollment time for instance. Hand geometry utilizes in authentication/verification mode. The uniqueness attribute of hand geometry is less than fingerprint. It is achievable to distinguish some individuals have same hand geometry pattern in a population [58]. Therefore, there might be more features calculated in hand geometry authentication/verification to deal with the drawback.

[18] http://www.bromba.com/faq/biofaqe.htm

Although we believe retina recognition, ear recognition and gait authentication belong to the high cost authentication category, we think retina recognition is more cost-consuming authentication methodology than ear and gait authentication methods. Retina recognition is profitable for the high security applications such as military because it is easy to use, very accurate, robust against spoofing attack and constant in various environments [58].
The iris recognition technology is very expensive authentication technology [56]. However, DNA recognition is introduced as the most expensive authentication mechanism by the participants.

15. Do you know that many new laptops have a fingerprint reader incorporated that can be used instead of the usual password mechanism?

Alternatives	percent	Value
1. Yes, but I do not think it is secure?	8.9%	4
2. Yes, but I do think that administration is too much work	22.2%	10
3. Yes, but company/organization policy prohibits its use	4.4%	2
4. Yes, and I would like to use it in the future	22.2%	10
5. Yes, and we are using it already	24.4%	11
6. No, but it sounds interesting	4.4%	2
7. No, but it is not of interest to our company/organization	0.0%	0
8. Other, please specify	11.1%	5
9. Don't know	2.2%	1
Total		45

Table 16. Laptops fingerprint versus password method.

As table 16 shows, although finger print authentication is almost a new technology in the laptops, the technology has recognized by the industry. Although, the participants have various opinions about fingerprint recognition technologies in the laptops, approximately 46.5% of them mentioned already used or ambitious to utilize it the method in the future. Few percentages of the respondents expressed their opinions in the usage of fingerprint recognition in the new laptops in the option eight:

- He knows the authentication method in the new laptops. But he mentioned it doesn't work in every system, on different computers. It refers to too much administrative tasks.
- He knows fingerprint authentication embedded in the new laptops. But we do not use it. The reason could be because the company/organization implemented other type of authentication mechanism.
- They know this technology, but they do not utilize it.

- They know this authentication methodology, but it does not apply to the PCs of the organization. It could prove implementation of the recognition methodology needs a lot of administrative work.
- They know about fingerprint recognition in the new laptop. They do not know anything about how the software works, how it scans and storing the data on the computer for later match and how secure is storage on the laptops. They do not aware if there are encryption technologies. The laptop could be stolen and the right person fingerprint might be exploited in order to gain access to the laptop. Hence, they must do research about that before use it.
  These expressions prove that they are suspicious to the security provided by the new laptops and they believe require more knowledge about the new technology. Results of question fifteen clarify the necessity of providing information about the new authentication methodology in the new laptop for the industry.

Acer and Compaq are two companies generate laptops with fingerprint recognition technology [84]. Laptops are at risk of theft. Fingerprints remain at the reader screen and it is collectable from there by the thief. Therefore, there should be another resistant authentication method simultaneously with fingerprint recognition in the laptops.
Some vendors recommend utilization of peripheral devices such as PC card reader with fingerprint authentication to harden the laptop verification system. The peripheral equipments mostly are expensive. A PC reader cost is between $150- 250 [84].
There also are other methods in order to harden the laptop systems. When a laptop is stolen the thief can remove its hard disk to other PC and boot by the floppy disk. Then, the thief accesses to the files at the system simply. The solution is data encryption in laptops. Utilizing cable locks is a strong barrier against laptop theft. Another solution has been suggested is installing monitoring and tracing software. It enables to track the stolen laptop by revealing the IP address when it connects to the internet. The software informs the responsible afterward [84].
Fingerprint recognition comprises too much administrative tasks. Moreover, it is an expensive method in the laptops. In addition, it is not secure enough and it is better to be implemented with a resistant authentication method. Fingerprint recognition technology in the laptops could be more robust than password authentication against remote attack. Password authentication mechanism is vulnerable versus dictionary attack and brute force attack.

16. Do you know that many new laptops have a webcam incorporated that can be used for face recognition instead of the usual password mechanism?

Alternatives	percent	Value
1. Yes, but I do not think it is secure?	15.6%	7
2. Yes, but I do think that administration is too much work	13.3%	6
3. Yes, but company/organization policy prohibits its use	6.7%	3
4. Yes, and I would like to use it in the future	13.3%	6
5. Yes, and we are using it already	0.0%	0
6. No, but it sounds interesting	24.4%	11
7. No, but it is not of interest to our company/organization	20.0%	9
8. Other, please specify	2.2%	1
9. Don't know	4.4%	2
Total		45

Table 17. Face recognition in new laptops versus password method.

There are some negative opinions against face recognition method in the new laptops according to the table 17. Statistics in choice 1, 2, 3 and 7 introduce, high percentage of the companies/organizations prefer not to utilize webcam authentication technology in the laptops. There is not any companies/organizations have already used the webcam authentication mechanism in the laptops.

A Vietnamese researcher published a paper about security of face recognition technology in the laptops in 2009. Three companies manufactured the technology in their laptops. The companies include: Lenovo, Toshiba and Asus. The algorithm utilized for the face recognition comprises flaws. This flaws cause the face recognition becomes vulnerable against “fake face brute force” attack. This is a name that the researcher gave to the attack. The reason is that the attacker has to generate a huge number of the images from an authorized user by a fake photo generator program. It is because the attacker does not aware of the image stored for the user [85].

The weaknesses of the face recognition in the laptops include:

- Effect of light changes: The algorithm just work properly when the light of environment is constant. It the other words, it does not guarantees sufficient security and safety when the light is changed.
- Effect of recording images devices: The resolution of the web cams made by the companies is very low. Lenovo, Toshiba, Asus produce resolution 0.3 mega pixel, 1.3 mega pixel and 2 mega pixel respectively. Low resolution is not the certain weakness of the laptops, but it introduces a security breach in the algorithm.

- Effect of image processing: All the algorithms employ digital images. It is a substantial security disadvantage in the face recognition mechanism.

In the "fake brute face" attack an adversary musters images from a legal user according to one of the methods. For instance, video chat, face book, flicker and utilizing Tele cameras which can collect images from far distances and/or ask the legal user to take a picture with him.

The owners of the three companies were aware of such flaws and weak points in their products. They attempted to solve or reduce the risks but the manufacturers have not been solved the issues completely.

The researcher claimed that there is no solution to deal with the weak points in the laptops. Hence, the researcher recommended that removing the face recognition mechanism from the laptops is the best solution. He informed the manufacturers from these flaws in the laptops. However, he has not been received any response from the companies.

Table below illustrate sensitivity of face recognition in the laptops [85]:

	Lenovo		Asus		Toshiba	
	Gray Image	Color Image	Gray Image	Color Image	Gray Image	Color Image
Brute Force	High	High	-	High	-	High
No Brute Force	High	High	-	Medium	-	Low

Table 18. The results of a face recognition research in the laptops.

17. Do you know that the ordinary username/password mechanism can be secured better by using biometric keystroke dynamics?

Alternatives	percent	Value
1. Yes, but I do not think it is secure?	6.7%	3
2. Yes, but I do think that administration is too much work	8.9%	4
3. Yes, but company/organization policy prohibits its use	2.2%	1
4. Yes, and I would like to use it in the future	20.0%	9
5. Yes, and we are using it already	4.4%	2
6. No, but it sounds interesting	44.4%	20
7. No, but it is not of interest to our company/organization	6.7%	3
8. Other, please specify	2.2%	1
9. Don't know	4.4%	2
Total		45

Table 19. Security of keystroke versus username/password method.

Table 19 shows most of the companies/organizations are optimistic about the security provides by using username/password method simultaneously with keystroke dynamics. It is comprehensible from choices 4, 5 and 6.
Keystroke dynamics is a passive method, almost cost effective and a foolproof method than the traditional methods such as password. Use of the biometric system with traditional authentication methodologies could demonstrate resistant security level [83]. Keystroke dynamics authentication methodology concentrates on continuous identification during login to the PCs and over the session.
It is better not to employ keystroke dynamics to identify users lonely. Implementation keystroke technology is recommended in collaboration with other technologies because it affected by users' status [67]. Therefore, false non match rate increases which causes unsatisfactory of the users.

18. Is your company/organization in some way using, or interested in using biometrics?

Alternatives	percent	Value
1. Yes, we are using it today already	13.3%	6
2. Yes, we are interested in using it in the future	66.7%	30
3. No, we are not interested in using it now or in the future	20.0%	9
Total		45

Table 20. Biometric features in the future.

Approximately thirteen percentages of the participants have been expressed that they already utilized biometric systems in their companies. Huge numbers of the companies/organizations are eager to employ the biometric systems in the future almost 67%. There is not any plan to make use of the biometric systems now or in the future by some of the companies/organizations. There is surely reason(s) that some companies/organizations are not anxious to exert the biometric authentication technologies. This will be reviewed more over following questions.

19. What kind of biometrics is using today?

Alternatives	percent	Value
1. Fingerprint recognition	83.3%	5
2. Face recognition	0.0%	0
3. Palm print recognition	0.0%	0
4. Iris recognition	0.0%	0
5. Retina recognition	0.0%	0
6. DNA recognition	0.0%	0
7. Ear recognition	0.0%	0
8. Voice recognition	0.0%	0
9. Signature recognition	0.0%	0
10. Gait recognition	0.0%	0
11. Keystroke recognition	0.0%	0
12. Mouse recognition	0.0%	0
13. Other, please specify	16.7 %	1
-1 Don't know	0.0%	0
Total		6

Table 21. Biometric types is using today.

Whole the companies expressed finger print recognition is the biometric system that they utilize to authenticate the users. A participant mentioned that they do not use biometric system for the internal usage.

20. In your experience, is the biometric system as secure as a username/password mechanism?

Alternatives	percent	Value
1. Security of biometrics is higher	83.3%	25
2. Security of biometrics is comparable to security of a username/password mechanism	3.3%	1
3. Security of a username/password mechanism is higher	3.3%	1
4.Other, please specify	6.7%	2
-1 Don't know	3.3%	1
Total		30

Table 22. Security of biometric system versus username/password method.

Some numbers of the companies/organizations have been emphasized security of biometrics is higher than username/password authentication method.
Two companies have stated security of the biometrics could be higher than username/password method. One explained its security depends on the type and the technology. The second company has expressed the security of the biometrics should be investigated.

21. Did you provide the users with information on what kind of personal data will be stored?

How the companies/organizations informed their users about the personal data will be stored in the databases when the biometric system was implemented. Does providing information about the implemented biometric system derive a profit?

Alternatives	percent	Value
1. Yes, we provided them with a lot of written information.	16.7%	1
2. Yes, we provided them with a lot of spoken information	0.0%	0
3. Yes, we provided them with some written information	0.0%	0
4. Yes, we provided them with some spoken information.	16.7%	1
5. No, but we did announce that some personal data would be stored.	16.7%	1
6. No, we did not mention this at all	16.7%	1
7. Other, please specify	16.7%	1
8. Don't know	16.7%	1
Total		6

Table 23. Data storage.

As we considered earlier six of the companies/organizations clarified the biometric system has employed in order to access to the resource. There did not provide any type of awareness methods for the users about the utilized biometric system for three out of the six companies. One of the companies emphasized fingerprint recognition method is the only biometric system has implemented. This is the reason that relevant awareness did not explain for the users. This company is counted as a corporation that did not present information their users. Among few number of the companies are utilized the biometric system, few of the corporations have provided explanations for the personnel.

22. Did the opinion of the users on the biometric system change over time?

There are not many responses about alteration of the users credence over time. It could be due to most of the companies/organizations have not utilized a biometric system. The second reason could be due to the companies/organizations are not concern about the users acceptance. A respondent answered the users opinions are altered as the users get familiar with benefit of the biometric system.

23. How satisfied are the users with the biometric authentication?

Alternatives	percent	Value
1. Very Unsatisfied	0.0%	0
2. Unsatisfied	0.0%	0
3. Indifferent	60.0%	3
4. Satisfied	20.0%	1
5. Very Satisfied	20.0%	1
Total		5

Table 24.Users satisfaction in use of biometric systems.

User of the implemented biometric system has divulged tree different reactions encompass: Indifferent sentiment, pleased feeling and very pleased feeling.

24. What kind of biometrics are you planning to use in the future?

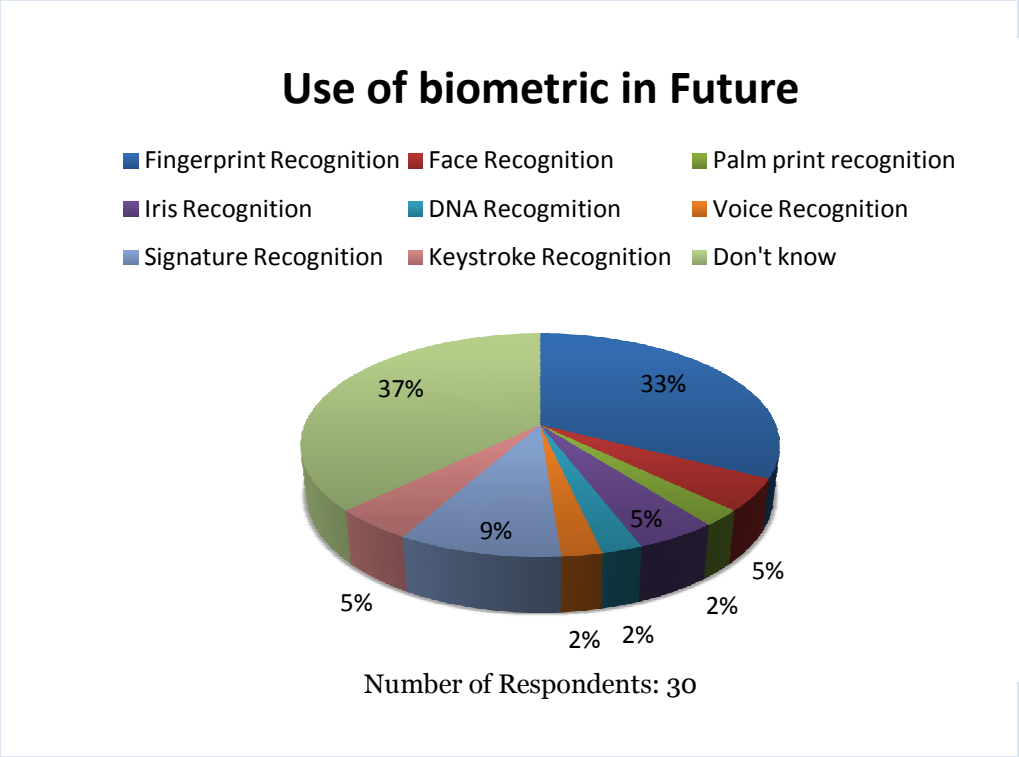

Figure 12. Use of biometric in the future.

Participants could select more than one answer for this question. Then, the total number of answers is forty four for this question. Noticeable percentage of the participants have been specified the biometric system that they might employ in the future. It could present that biometric systems have been recognizing as an

authentication mechanism in the industry. Some percentages of the corporations have not made decision for future usage of the biometric systems. The reason could be the companies either do not know whether they want to implement biometric systems or improving existing authentication mechanisms in their companies. The companies/organizations probably require to do search and mustering for proper knowledge and information about the biometric authentication systems. The corporations could make decision about the biometric systems is profitable for their organization afterward. Moreover, some of the companies/organizations might implement recognition methodologies in the laptops. According to Question 15 and Question 16 some of the companies/organizations considered that their ambition to exert the authentication methods in the laptops in the future. In addition, the companies probably need to consider the size of their company and number of personnel in the future.
Fingerprint recognition technology is the most attractive biometrics for future usage by huge number of the companies/organizations. Although signature recognition does not provide good security level, it is the second biometric system interesting for the future utilization by the respondents. The reason will be investigated in the part 6.2.6. A few percentages of the companies/organizations would prefer to use the other biometric recognition systems. The reasons could be found over Questions eleven till fourteen. We do believe that the factors investigated over the Questions have significant influence in the future utilization of the biometric systems.

25. What do you think are the operational costs compared to the username/password mechanism?

Alternatives	percent	Value
1. Operational costs of biometrics will be higher	60.0%	18
2. Operational costs of biometrics will be comparable to operational costs of a username/password mechanism	20.0%	6
3. Operational costs of a username/password mechanism will be higher	10.0%	3
4.Other, please specify	0.0%	0
-1 Don't know	10.0%	3
Total		30

Table 25. Operational cost of biometric systems and username/password.

High number of the participants expressed the biometric systems require more fees versus username/password mechanism. This opinion could support our deduction in Question eight. We concluded one reason why the companies/organizations prefer to use username/password instead of biometric recognition methods is that username/password is a cost effective mechanism. Small number of the respondents thinks username/password operational costs are more than the biometric systems. It almost could be true in case of forgetting username/password. There should be hired a person to support administrative tasks when it is necessary. Obviously, the companies need to spend budget for employing a skilled person for the position. Moreover, username/password can be captured stealthily in order to do malicious activities. Furthermore, username/password can transfer among

colleges to make easy each other duties. Hence, Operational costs derive from employing username/password not only could be sometimes high also could be irreparable. On the other side, the belief cannot be true since username/password mechanism has been introduced as an economical and cheap authentication technology [19]. Operational costs of these two methods could be comparable regards to opinion of 20% of the respondents. We do believe cost of implementation username/password and the biometric systems could be comparable for the challenges explained in this question.

26. How did the users react when hearing that they had to use a biometric system?

User acceptance could be a challenge in use of the biometric systems. Individuals would not like to be rejected when asking for a benefit in the society. Individuals can be denied to access to the service due to some reasons. For instance, they might put the finger in the screen reader incorrectly; the biometric feature does not have proper quality to be recognizable by the system, inserting the card wrongly in an ATM machine, etc. Although there is nothing wrong with the individuals' identity, they will shy in front of other users and might become motiveless to use the biometric system. The reason is that they possibly think there is something wrong with them. While the only reason the other users can access to the service is that they are aware of how to utilize the biometric system. In the other hand, these types of rejections cause FNM report and acceptability of the biometric system will reduce. We amass the participants' comments in the table 26:

Users' reaction versus biometric systems
1.User reaction is good
2. They have plan to implement but they have not taken any step to confront the users.
3. The users' reaction is positive when they get familiar with benefits of the biometric system such as enhancing security in authentication process and it is robust against ID theft.
4. They have not implemented yet.
5. They believe it is an immature technology.
6. They Only use the biometric system for access to the documents in the print queue optionally. Some printers need fingerprint recognition to activate the printer for the particular user. Most people have not activated to use the technology. The decision is based on sensitivity of information rather than the biometric mechanism.

Table 26. Users reaction in the use of biometric systems.

27. Will you provide the users with information on what kind of personal data will be stored?

Alternatives	percent	Value
1. Yes, we will provide them with a lot of written information	46.7%	14
2. Yes, we will provide them with a lot of spoken information	0.0%	0
3. Yes, we will provide them with some written information	23.33%	7
4. Yes, we will provide them with some spoken information	0.0%	0
5. No, but we will announce that some personal data will be stored	3.33%	1
6. No, we will not mention this at all	3.33%	1
4.Other, please specify	3.33%	1
-1 Don't know	20.0%	6
Total		30

Table 27. Information provided about data storage.

Companies/organizations will inform the users about data storage in the biometric systems via variety of notification methods. Some of the methods amassed in the table 27. Informing the users about the biometric systems characteristics and delivering sufficient information is an important effort. It could escalate the users cooperation as the users perceive their collaboration is crucial to provide resistant security for the company/organizations. In other words, to protect resources and assets against malicious activity the company reckon with the users role. Furthermore, the personnel are assured they are responsible to overcome the security breaches and vulnerabilities. Moreover, the users understand how the biometric system support and increasing safety and security issues.
There could be some reasons that some percentage of the companies/organizations have determine to notify the users with a lot of or some written information. It reveals the companies/organizations are aware of the profit they probably receive instead. Beside it proves the corporations take serious the users role in order to practice an environment devoid of false.
There are diverse methods to inform the users of the biometric systems. The question is that why most of the corporations are ambition to provide written information about data storage in the biometrics authentication mechanism. It might be since the individuals can refer to the written information document to review at the real time. Besides the document can be appropriate reference that there is a notification about security difficulties and responsibilities. In addition, the scope of the users' tasks is clarified.
Although providing information about the biometric systems authentication should be with discretion of the company/organization, the benefits of informing the users of the biometrics systems should not be neglected.
There should be a complete and honest explanation about process of the biometric system, health and privacy issues, implementation method by the company. Moreover, the explanations that emphasize how the biometric system improves the security offer better credence to the users. The result would be escalation in the user

acceptance and collaboration to deal with intrusiveness issues in some biometric systems [57].

28. Why is your company/organization not interested in using biometrics?

Alternatives	percentage	Value
1. Operational costs will be too high	17.39%	8
2. Initial costs will be too high	17.39%	8
3. System is not secure	17.39%	8
4. Regulations / Norwegian law prohibits the use of biometrics	15.21%	7
5. Strong opposition from the users	15.21%	7
6. Unfamiliarity with biometrics	17.39%	8
Total		46

Table 28. The effective factors on the respondents' opinion in the use of biometrics.

Table28 shows almost equal percentage of the companies/organizations are not keen on utilization of the biometric system due to for example operational cost, initial costs, lack of security, Norwegian laws, user acceptance and familiarity of the biometric systems. There is a connection between the respondents believe the biometric systems are not secure and the respondents have mentioned they are not familiar with the biometric authentication systems. Therefore, the companies/organizations refused to use the biometric technologies. The connection is more related to lake of correct knowledge about the biometric systems. As the security level of the biometric systems differs from type to type. Furthermore, security of the biometric systems is promotable by using combination of the authentication methods, implementing a complete risk analysis procedure in order to find the proper biometric systems the organization, etc. Hence, unfamiliarity with the biometric systems could be more than the statistics at the table 28. We do emphasize Knowledge and familiarity factor about the biometric systems significantly eclipse the other factors. Appropriate knowledge and information about authentication methodologies impress utilization of the biometric systems in the future. In the other hand, influence of Norwegian regulations restrictions cannot be overlooked. There are some limitations in Norwegian regulations relevant to privacy issues and human rights. Furthermore, the final decision to allow or denying implementation of a biometric system is with discretion of the authority. Moreover, Norwegian laws consider subverting trust in the work environment. Therefore, the regulations allow implementation of a biometric system when the purpose is fulfilled [6, 45]. However, the applicants ought to comply with other conditions to utilize a biometric system.

29. Do you feel that more knowledge about biometric systems could change your opinion on the use of biometrics?

Alternatives	percent	Value
1.Yes	64.4%	29
2.No	22.2%	10
3. Other, please specify	0.0%	0
-1 Don't know	13.3%	6
Total		45

Table 29. Awareness in the use of biometrics.

Most of the participants have been specified more information alter their conviction about the usage of the biometric authentication systems. This declaration emphasizes the correctness of the provided analysis in Question twenty eight about familiarity and knowledge of the industry about the biometric systems. Some of the respondents clarified more knowledge does not shift their belief in the utilization of the biometric authentication methodologies. There has not introduced any eager to change or promotion the existence authentication methods. In the other words, the corporations have received the expectation security with the current authentication mechanism(s). The companies/organizations ought to have in mind the extension of the new attack methods in the future. The adversaries attempt to reach new malicious techniques to receive more profits or for revenge purposes. Therefore, hardening of the authentication systems is unavoidable.
Half century ago there was not any opinion that a basic typing machine becomes an important asset of human one day. But today, we do believe this crucial device should be preserved and protected by powerful and robust authentication technologies.
The respondents that selected the option" *don not know"* they join to one of the two groups in the table 29. It occurs when more familiarity is provided about the advantages and the drawbacks of the biometric systems. Suppose the whole companies/organizations have chosen option "*do not know*" would join to the group "NO", still the percentage of the companies/organizations eager to receive more information about the biometric systems is the highest.

30. Do you feel that Norwegian laws/regulations stand in the way of usage of biometric authentication in Norway?

Alternatives	percent	Value
1.Yes	18.2%	8
2.No	34.1%	15
3. Other, please specify	9.1%	4
-1 Don't know	38.6%	17
Total		44

Table 30.1 . Norwegian regulations in the use of biometrics.

Some numbers of the corporations have mentioned that Norwegian laws hindrance implementation of the biometric systems. Unfamiliarity with the biometric systems that discussed in Question twenty eight could be correct for Norwegian regulations. It is perceptible referring to the statistic in the option "I do not know" in the table 30. Appropriate knowledge about the laws in the use of the biometric systems clarifies the legal scope of u the sage of the data amassed by the authentication systems. In addition, if the companies had proper knowledge about the regulations, the corporations would choose or refusing the utilization of the authentication mechanism reasonably.
The other profit of providing sufficient awareness about the laws limitations is that user acceptance increase. It will happen if the users perceive that the regulations allow controlling their personal information. Furthermore, proper awareness of the users reduces further usage of the personal data by the third parties.
A substantial example that proves proper knowledge escalates user acceptance can be found in the option two of the table 31. Although supporting the factors such as complying with POL, assuring of a safe storage, providing safe channel to transfer the data and retention time demanding robust and continual administrative work, the participants have accepted and dealing with it.
Norwegian regulations are an obligation in the use of the biometric systems. Therefore, there should be a balance between legal challenges and the limitations that are necessary in the reality. In the other words, appropriate regulations could be a powerful tool to prevent exploitation of the biometric data for the other purpose except certain aim(s) [45]. There are some weakness and strict laws in the Norwegian regulations in order to implement a biometric recognition technology. For example, there is not any law to specify a policy for the authority to make decision allowing or refusing the intention of implementation of a biometric system. Hence, the authority or the committee might make a personal decision case by case. There is a reference to Chapter 4 for Tysvaer Corporation.

Other
1. I certainly hope so.
2. Only to some extent. We just need to comply with POL and ensure safe storage, transmitting and deletion.
3. It may, and who is taking the risk when using biometrics? When my biometrics is copied, what should I do?
4.Perhaps, know too little

Table 31.1. Norwegian laws in the use of biometrics.

31. What is the size of the company?

Alternatives	percent	Value
1. 1-25	20.8%	10
2. 26-100	25.0%	12
3. 101+	47.9%	23
4.Other, please specify	6.3%	3
-1 Don't know	0.0%	0
Total		48

Table 32. Size of companies/organizations.

Size of the companies/organizations could effect on the use of authentication methodologies.
The companies are classified into four groups. The fist group involves the companies with the number of personnel between 1-25 people. The second group includes the companies/organizations with the number of employees between 26-100. The third group comprises the companies/organizations with more than 101 personnel. Three numbers of the companies/organizations encompass more than 101 people. The first organization involves fifteen thousand people. The second organization has five thousands students and six hundred employees. The third company includes four thousand people.

32. What type best describes your organization/company?

Alternatives	percent	Value
1. Governmental	22.9%	11
2. Non-profit organization	4.2%	2
3. Educational	6.3%	3
4. National commercial company	18.8%	9
5. International commercial company targeted towards northern Europe	14.6%	7
6. International commercial company targeted towards the whole world	22.9%	10
7.Other, please specify	8.3%	4
-1 Don't know	2.1%	1
Total		47

Table 33. Type of companies/organizations.

As table 33 shows the companies/organizations are categorized into six groups according to their type. Option seven is for type of the companies/organizations do not included into one of the six categories.
Type of the companies is the other factor should be investigated since there might be a link between the type of communications and the use of the biometric systems. The participants have introduced four other types for their organizations comprise: consult company, IT Company, Foundation Company and industrial organization.

33. Are you willing to participate in a possible follow up of this questionnaire (In case of a yes answer, please provide contact details in the next questions)?

Alternatives	percent	Value
1. Yes, I am willing to answer another questionnaires on this topic	22.9%	11
2. Yes, I am willing to participate in an oral interview	6.3%	3
3. No, I am not interested in further participation	75.0%	36
Total		50

Table 34. Statistics for further cooperation by companies.

There was feasible to need more collaboration of the participants after studying the responses. Hence, we asked the participants determine if they keen on for further cooperation relevant to this thesis. Approximately 29% of the participants would interest to assist more via sending new questions or attending an interview. However, high percentage of the respondents is not anxious for further collaboration.

34. If you would like to be informed about the results of this research, please enter your contact details here.

Some of the respondents introduced an email address to send the result of this research project encompass 24% of the companies/organizations. The companies/organizations with medium and large size are the most interested population to receive the result of this thesis including 18%. Only 6.3% of the governmental organizations believe that need to study the statistics. The other types of the companies/organizations constitute the rest of the statistic to peruse the thesis.

6.2 The Results of Questions Compared Together

6.2.1 The use of authentication method inside company

In this part the usage of authentication mechanisms in order to gain access to the building, critical areas and devices such as servers, PCs, printers, etc will be reviewed. In other words, information of Question one, Question four and Question seven are compared. The number of respondents differs from each other. Therefore, the mean of number of respondents is used for the calculations.

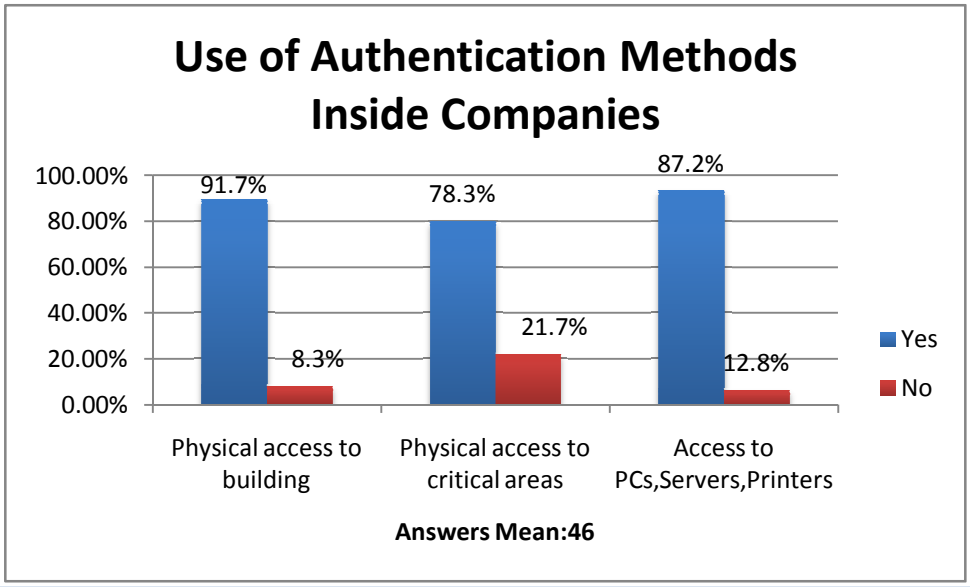

Figure 13. Authentication mechanism in Norway companies.

Figure 13 shows, massive percentage of the companies/organizations have applied an authentication methodology to access to the building. Only small percentage of the companies/organizations has not exerted any security protection to reach to the building. Physical access to critical places inside the companies/organizations is controlled by noticeable percentage of the corporations. However, there is an escalation in percentage of the companies/organizations construes the utilization of an authentication mechanism is not necessary for the critical areas. The reason could be since most of the corporations that have implemented a recognition mechanism for the resources such as servers have not embedded an authentication method to verify access to the crucial regions. Table 35 illustrates six numbers of the companies that have devised a protective technology for servers, printers and PCs have not deployed any recognition method for the critical areas. The utilization of a proper authentication mechanism for critical places constructs a double check mechanism for physical access to the resources. On the other hand, there are few corporations that applied an authentication mechanism in the both positions. Table 36 amasses the companies have not implemented a protective security techniques neither for critical regions nor for servers, PCs and printers. The importance of visual authentication methods would distinguished, when an adversary entered to the corporation after an authorized employee for the moments that door of the building is open [11].

The use of authentication methods to obtain access to servers, printers and PCs introduces more tend than exerting a verification method to access to critical areas. Username/password is the most desirable recognition method for servers, PCs and printers by the companies/organizations. It could prove that there is not a apparent security strategy to define the security vulnerabilities, challenges, critical regions and the assets for the companies/organizations and concluding the appropriate authentication technology that features the maximum protection for the place.

Number	Access to the building	Critical areas inside building	Access to servers, printers, PCs, etc
1	Did not implement	Did not implement	Username/password
2	Card+ PIN code	Did not implement	Password only
3	Card+ PIN code	Did not implement	Username/password
4	Card+ PIN code	Did not implement	Username/password
5	Card, card+ PIN code	Did not implement	Username/password, Biometrics
6	Card+ PIN code	Did not implement	Username/password

Table 35. The use of authentication methods for the critical areas.

Number	Access to the building	Critical areas inside building	Access to servers, printers, PCs, etc
1	Card+ PIN code	Card+ PIN code	Did not implement
2	Card+ PIN code	Username/password	Did not implement
3	Card+ PIN code	Did not implement	Did not implement
4	Visual, card, card+ PIN code	Did not implement	Did not implement
5	Did not implement	Did not implement	Did not implement

Table 36. Lake of security mechanism for the resources.

6.2.2 The size of the companies and critical areas

Size of the corporations is studied versus the recognition methods have devised to control physical access to the building and critical areas inside the companies/organizations. As a matter of fact, influence of the statistics of Question thirty one are reviewed on Question two and Question five. See Table 37.

Company size								
Alternatives	1-25 (N=10)		26-100 (N=12)		101+ (N=23)		Other (N=3)	
	access to building	Critical areas	access to building	Critical areas	access to building	Critical areas	access to building	Critical areas
1.Visual(guard)	0.0%	0.0%	13.33%	0.0%	17.14%	0.0%	20%	20%
Number of answers	0	0	2	0	6	0	1	1
2.Card	0.0%	12.5%	26.67%	33.33%	20%	10%	20%	20%
Number of answers	0	1	4	4	7	2	1	1
3.Card+PIN code	100%	62.5%	60%	58.33%	62.86%	80%	60%	60%
Number of answers	8	5	9	7	22	6	3	3
4. Biometrics	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Number of answers	0	0	0	0	0	0	0	0
5.Other	0.0%	25%	0.0%	8.33%	0.0%	10%	0.0%	0.0%
Number of answers	0	2	0	1	0	2	0	0

Table 37. Results of comparing question 31 with questions 2 and 5.

The Companies/organizations with immensity more than a four thousand staff are three according to Question 31. The first priority of these organizations in the utilization of authentication methods to secure the building and critical places is card + PIN code, visual and card authentication methods respectively.
Card + PIN code is the most popular verification method to preserve safe the areas inside the corporations. There is not tendency in the use of biometric systems for the places.
The companies/organizations with extent between 1-25 personnel have deployed neither guard nor card to control access to the building; these corporations implemented card + PIN code verification mechanism instead. The reasons could be indentifying the employees is facilitated with the low number of people. Hence, the companies/organizations concluded not to spend fee to hire somebody for the visual purpose. Moreover, card + PIN code mechanism is the most common recognition method to access to the building. It could feature the organizations procure card + PIN code method more secure than card only.
There is an escalation in the utilization of visual authentication mechanisms to protect the building simultaneously with size of the corporations.
A few of the companies with the number of staff between 26-100 have employed a person for visual monitoring for the building. The use of visual identification technology in compound with another authentication method rise to protect the building as size of the companies is grown up. Since recognition individuals work on various departments in the large companies/organizations guarantees more security via applying the combination methods. Furthermore, owing to the immensity of the large companies resources are distributed in diverse areas inside the companies. Therefore, there is a requirement to support security and controlling the usage of the assets through multiple authentication technologies. We believe hiring an individual to visual recognition purposes for the building depends on the corporations' size.
The use of combination authentication methodologies has devised to control access to the critical areas inside the building by all the companies/organizations regardless to the size. Almost none of the companies/organizations have employed a guard to visual check for the critical areas inside the building. It could be derived from the corporations already utilized visual verification mechanism to enter to the building. Hence, the companies/organizations have been utilized card, card + PIN code and other methods include safe code or donation key to the responsible person in order to gain access to the critical areas. Moreover, the number of individuals should have access to the critical areas might cause in the usage of guard for the areas. For instance, safe box room inside a bank is a place that many people obtain access to it. Therefore, the use of visual verification in compound with other types of authentication technologies could pose additional security.
Consequently, we believe the certain reason that the small companies/organizations with extent between 1-25 people have not hired guard to control security of the critical areas is the size of the companies/organizations.
All the companies/organizations have utilized a recognition method to obtain access to the critical areas inside the building. The reason is that the critical areas encompass the companies' assets. Therefore, the massive percentage of the

companies/organizations has been chosen the most secure recognition method in their opinion for the areas, card + PIN code.
Definition of critical areas and crucial data differ for various companies/organizations. This can be concluded of variations in the use of the authentication technologies by the corporation. Also, small percentage of the companies/organizations has been employed guard even for the critical areas. It could feature the companies/organizations awareness and knowledge about security breach exists in each physical and non-physical segment of the areas inside and outside their location. Sufficient knowledge about security of the authentication mechanisms and biometric systems causes not only suitable security protection is guaranteed for the place also financial cost will be decreased.

6.2.3 Company type versus use of the biometrics systems

In this part we will look at the companies/organizations type with relation to the companies/organizations interest in the use of biometrics. In other words, Question two and Question eighteen will be studied respectively. There are seven classifications for the companies/organizations type.

Company Type							
Alternatives in Question 18	Governmental (N=11)	Non-profit organization(N=2)	Educational (N=3)	National commercial CO (N=9)	International commercial CO targeted northern Europe (N=6)	International commercial CO targeted the all world (N=9)	Other(N=4)
1.Yes,we are using it today already	9.1%	100%	0.0%	11.1%	0.0%	22.2%	0.0%
Number of companies	1	2	0	1	0	2	0
2.Yes,we are willing to use it in the future	63.6%	0.0%	66.7%	66.7%	66.7%	77.8%	75%
Number of companies	7	0	2	6	4	7	3
3.No,we are not willing to use it now or in the future	27.3%	0.0%	33.3%	22.2%	33.3%	0.0%	25%
Number of companies	3	0	1	2	2	0	1
Total number of companies/organizations =44							

Table 38.Biometric systems versus company type.

The number of companies with type specified at the top of the table 38 should be forty six according to Question 32 whereas the number is forty four in the table. It is due to one of the International commercial company targeted northern Europe did not response Question 18. Hence, its number is six instead of seven at table 32. Moreover, one of the International commercial companies targeted the all world did not reply Question 18 as well. The number of International commercial companies targeted the all world is nine instead of ten at Table 38.
Number of the companies should be thirty in the second row of Table 38 regard to Question 18 whereas it is twenty nine. It is due to one of the International commercial company targeted northern Europe did not reply Question 18.
Noticeable matter is that the number of the companies tend to deploy a biometric systems increased in the future. As a comparison with number of the corporations utilize the biometric systems today. This statistic almost is fivefold of the companies/organizations that already used the biometric systems. It is owing to approximately 76% of the companies/organizations are avid to utilize the biometric systems in the future according to Table 38.
Almost 17% of the companies/organizations state will devise a biometric system in the future, expressed more knowledge will not alter their believe in the use of the biometric systems. It features the corporations importune in the usage of the biometric recognition systems. However, there is no clarification with respect to more knowledge and future use of the biometrics in the future by the other corporations.
All types of the companies/organizations are eager in the utilization of the biometrics in the future. The percentages of the International commercial company targeted towards the whole world are using already the biometric mechanisms are higher than the other types of the companies.

6.2.4Laptops Security versus username/password

Figure 14 shows opinions of forty five of the companies/organizations about use of fingerprint recognition, webcam recognition in the new laptops instead of username/password method versus using username/password with keystroke dynamics. As matter of fact, Questions 15, 16, 17 are comparing together in this part.

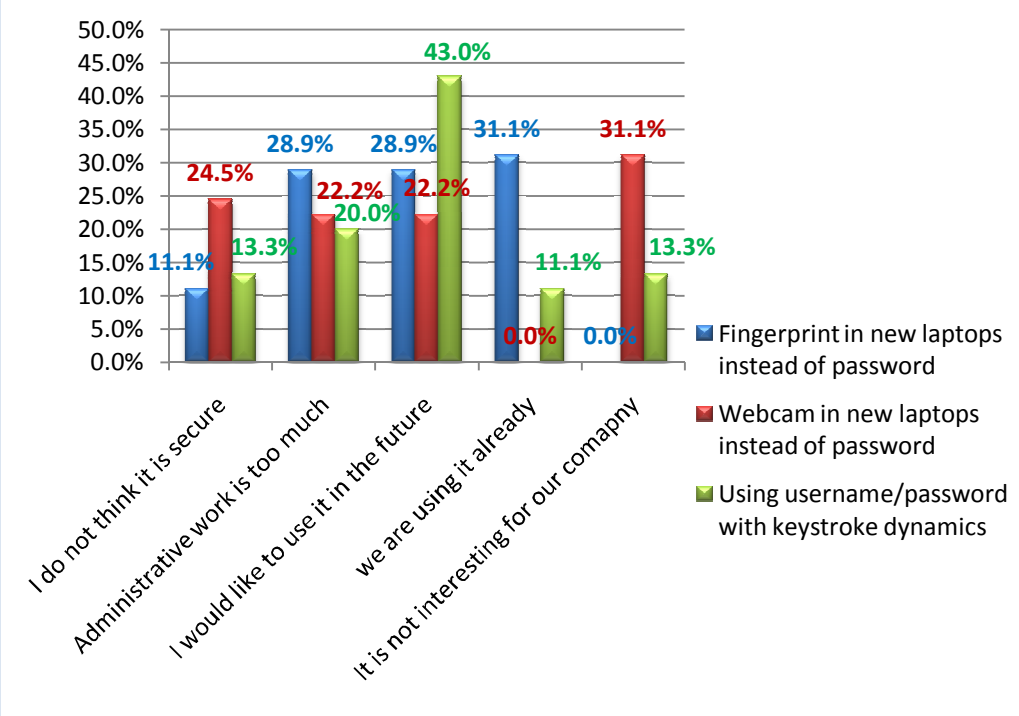

Figure 14. Fingerprint and face recognition mechanism in the laptops.

The corporations' former experiences features fingerprint possesses massive administrative difficulties. Today finger print in the laptops is the most applicable and pervasive authentication technology.

Web cam technology in the laptops accommodates the lowest percentage in implementation today and in the future. It could be due to inappropriate security level that it exposes in the respondents' belief. However, the profitability of face verification for dynamic authentication process combination with a static verification method to launch a session should not be neglected.

Username/password compound with keystroke authentication mechanism anticipates of fingerprint and webcam verification technology for the future utilizations. It could be owing to the lower administrative tasks that the compound method discloses than fingerprint and webcam technologies refer to the respondents' previous experiences.

6.2.5 Role of awareness in the use of biometrics

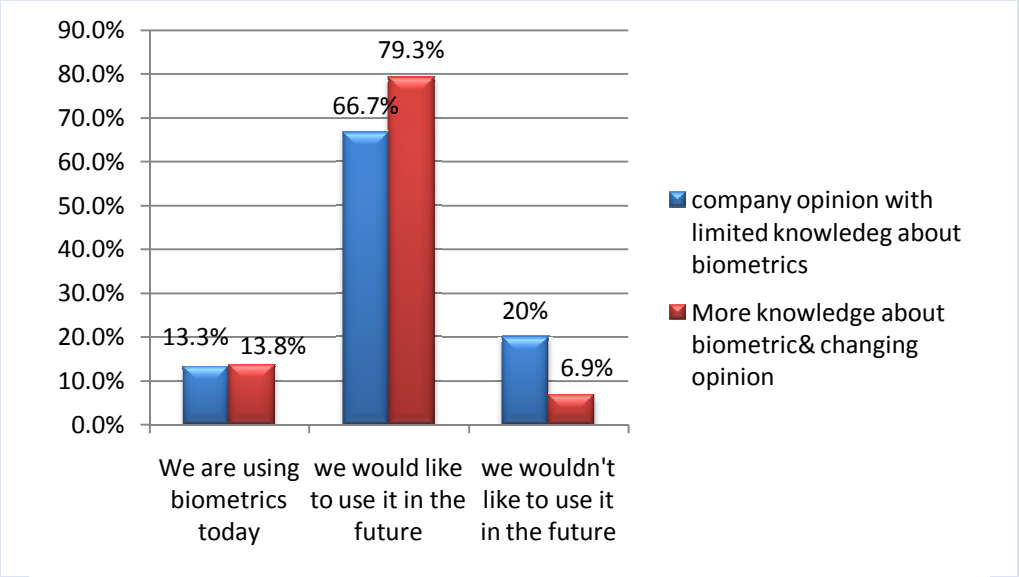

Figure 15. Knowledge factor in the use of the biometric methodology.

We queried whether more knowledge about biometric systems could shift companies' opinion in the utilization of the biometrics in Question twenty nine. In this part, the effect of answers "Yes" in Question twenty nine will be estimated on Question eighteen. In Question eighteen some companies already employ biometric systems. Some of the corporations ambition to exert a biometric recognition technology in the future. However, some of the companies are not keen on implementing biometrics currently or in the future.
There will be considerable alteration in enthusiasm of the usage of the biometrics by the companies/organizations in the future if they receive sufficient information. Some number of the corporations clarified not desire to implement biometrics today or in the future. There would be a reduction in the number by acquisition more knowledge about the biometric authentication systems. See Figure 15.
As we mentioned earlier knowledge factor play a key role to make decision to utilize a biometric recognition system. User acceptance and cost issues often hinder adopting the biometric systems as a solution for security purposes. While budget and maintenance costs of token-based systems sometimes are more than those for the biometric systems [55].

6.2.6 Use of the biometrics in the future

In this part we will investigate the factors influence in the companies/organizations conclusion in the use of biometrics in the future. To state difficulty, factors such as awareness, security, privacy and cost will be estimated for Question twenty four. The corporations' priorities in the use of biometrics in the future are amassed in the table 39.

Companies/Organizations selection for biometrics usage in the future
1.Fingerprint
2.Signature
3.Face=iris=keystroke
4.Palm=DNA=Voice
5.Retina=Ear=Gait=Mouse=0

Table 39. Preferences in the use of biometric systems.

Fingerprint recognition will be the first preference to implement by most of the companies/organizations in the future. The most acquainted biometric recognition method for the companies/organization is fingerprint. Fingerprint recognition features magnitude security level after DNA and iris. In addition, fingerprint recognition guarantees high privacy after iris. Moreover, fingerprint is the cheapest biometric mechanism based on the respondents' opinion. To review, the information is available in Question eleven to Question fourteen.

The statistics reveal massive percentage of the companies/organizations interprets awareness factor, security and privacy factors comparable with cost factor. It other words, the corporations prefer to utilize the most familiar biometric system which refer to proper level of privacy with cost efficiency.

The second choice of the companies/organizations for the future usage is signature recognition method. Signature recognition is the second well known authentication mechanism for the corporations. Although signature features low level of security and privacy, it is the second cheapest biometric authentication technology in companies/organizations opinion. These data state some of the companies/organizations implement the biometrics according to familiarity and cost in the future. This number of companies/organizations is significantly lower than the companies/organizations that interested in employing fingerprint recognition technology.

The third priority to deploy a biometrics will belong to face, iris and keystroke recognition method. The companies have medium awareness about Keystroke recognition. Also keystroke authentication technique provides weak security and privacy level in the respondents' belief. The participants clarify keystroke is the third authentication technology with low operation cost. On the other hand, face and iris recognition methodologies will be employed as equal number as the corporations ambition to implement keystroke technology in the future. The question is why analogous number of the corporations will implement keystroke recognition, face recognition and iris recognition? However, iris is familiar for the most of the corporations. Moreover, it guarantees very high security and privacy level. But the respondents have perceived face recognition and iris recognition expensive technologies. The effect of cost factor is revealed in these decisions.

This argument features two matters. First, small number of the companies/organizations has suitable knowledge or awareness about the biometric systems encompass security issue, privacy level and operation cost. Consequently, they prefer to comply with security and privacy factors versus cost concerns. Second, small number of the companies/organizations importunes to deploy a biometric system based on awareness factor and operation financial issue. Therefore, the corporations will accommodate keystroke authentication method however; it devises low security and privacy level than iris and face recognition mechanisms.

The same debate is carried for the forth prioritization in the table39. This group comprises palm print recognition, DNA recognition and voice recognition.

Operation cost of voice recognition is very lower than palm print and DNA authentication methodologies as its security is lower than these recognitions mechanisms. There is an inexpensive authentication method in each group, prioritized by the companies/organizations. The effect of cost concerns is inevitable in the biometrics implementation.

None of the companies/organizations will not equip the organizations with retina recognition, ear recognition, gait recognition and mouse recognition mechanisms in the future. There is an insufficient or low awareness, security and privacy issues for the biometrics such as ear recognition, gait recognition and mouse recognition in the respondents' opinion. It seems that operation cost has not been considered when there is no guarantee for the other factors. Retina is not attractive authentication method for the companies/organizations. Since familiarity with retina is lower than biometric systems that provide acceptable security and privacy level such as fingerprint and iris authentication technologies. In addition, retina possesses low security and privacy versus fingerprint, iris, and DNA recognition methods. Hence, we conclude that when a biometric system supports weak or low level of security and privacy necessities, and there is not proper knowledge and familiarity for the biometric characteristic, operation cost factor does not consider in the use of the biometric system.

To conclusion, we believe awareness/knowledge factor and operation cost of the biometric systems are extremely substantial factors for magnitude number of the corporations for future usage of the biometric systems. Operation cost will not be crucial when security and privacy requirements are anxieties and preferable for the companies/organizations. But still awareness/knowledge necessity plays a key role even for the companies/organizations with preference of security and privacy.

For more information about awareness and knowledge factor see Part 6.2.5.

7 Conclusion

Biometric systems market analogous all other markets requires its own risk analysis procedure, prediction and prioritization the necessities regard to the organizations discretion and security requirements.

Whether the policy of the organizations highlights the security needs for today and future has studied in this project. The results clarify the authentication methods have implemented by the organizations, the appliances and areas the authentication methods were deployed. In addition, influence of some factors in the use of authentication mechanisms were introduced such as the corporations' type and the companies' size. The companies' type can disclose the importance of the data and assets of the companies.

There is an essential ambition to feature the factors and attributes lead the companies/organizations policy to implement the biometric systems. For example, interests of the organizations, the incentives to adhere to an authentication methodology and biometric method, financial issue, users' cooperation, awareness and knowledge about the security, privacy, legal perspectives and need to progress the information security system. The essentiality derived based on provided security by the traditional methods, safety of the biometric systems and the combination authentication technologies. Usage of password to login to the system and keystroke dynamic to authenticate during the sessions is one combination methodology to increase safety.

During the work on this project we have looked at varied aspects of the use of biometrics in the Norwegian organizations and companies. We introduced authentication mechanisms in general in order to draw what frame work the verification and identification methods propose to authenticate the individuals. The main concentration was in the biometrics recognition technologies. The biometric systems requirements such as performance, reliability, user acceptance, easy to use and cost have studied owing to emphasize the crucial and proprietary attributes that pervasively conduct the utilization of the biometrics systems in the market. Moreover, the biometric systems vulnerabilities were stated since the weaknesses cause the biometrics refer to intrusive activities. Tackling with the vulnerabilities and security breaches will introduce better safety and privacy for the users' personal data. Therefore, the profitable capabilities of the utilization of the biometric systems will be exposed simultaneously with its drawbacks. Study of the users acceptance in the use of biometric authentication systems clarified there is a need to improve the individuals' knowledge and awareness about the authentication mechanisms. In sequence some solution were introduce to receive the users cooperation. Furthermore, some methods were determined to support individual privacy and security necessities.

Linkage between biometrics and forensic was looked at this report. Since in case of exploitation against a biometric system forensic experts can collaborate with biometric specialists to aggregate the evidences and recognize the adversary.

The security technologies implemented for the building, controlling methods to gain access to critical areas and the security methodologies employed for resources such as servers, PCs declared some results. For instance, inevitable factors, obstacles and challenges in the usage of biometric recognition systems.

Legal aspects hinder deploying the biometric authentication systems in Norway in the organizations' opinion. Some ceases were investigated in order to describe the challenges and constraints have exerted by Norwegian regulations. Knowledge of the users and the companies about the regulations definitely is benefit able to devise solutions to improve the use of biometrics in Norwegian industry. Comparison between European and Norwegian regulations acquaint various requirements to employ a biometric verification/identification system. Hence, there should be managed legal aspects to facilitate the data protection in the market. The legal perspectives in the use of biometrics transparently lead to privacy challenges. Therefore, it absolutely is crucial to study the regulations with users acceptance issues. Legal regulations can be a substantial incentive for the demanders to assure there is robust, fair and proportional laws to guarantee safety for the private and personal information.

There are considerable tendency to deploy a biometric verification mechanism in the future. Beside, some respondents have mentioned more information and research about the biometrics probably cause revision to boost the biometric recognition systems. The positive point of the tendency is that the companies/organizations will perceive and construct the necessity of a suitable and safe enough authentication technology(s) for their businesses. Moreover, the importance of the research and consultation with experts will be revealed in order to attain substantive and reliable security decisions. Furthermore, the corporations that believe there is no requirement to look over current security protection and promotion of the outdate safety devises, might change their strategies when get aware of the satisfaction of their partner companies in boosting or up to dating the authentication and security solutions.

We do believe the aforesaid elements eclipse the use and expanding of the biometric recognition mechanisms in Norwegian industry. We emphasize awareness element is the most vital factor in distinguishing security and privacy needs, the proportion between financial investment and security achievement, legal needs and user oppositions issues.

8 Future work

Since this project is rather a new survey in Norway there is a lot of aspect that would need more attempt and effort. This thesis can be a start point to work in this area for people who are interested in such survey. In this thesis we use questionnaire for data collection method. Other types of data collection mechanisms could be employed in compound with questionnaire to reach more feedback from the participants. Combination data collection methods particularly can be excellent opinion to muster the participants' responses for the questions that they have not replied in the first contact to participate at the research.

There can be more concentration in the type of companies/organizations. It reveals more attempt to contact with the companies/organizations refer to the type that introduced. This expose how indeed the corporations type eclipses the utilization of the biometric authentication systems. Furthermore, the usage of the biometric systems could be investigated in a specific field for instance medical usage of the biometrics today and in the future. How biometrics systems could employ for health services? Hence, there will be extra consideration to select the biometric characteristics should be studied.

There can be annexed some biometric features such as hand geometry recognition.

Regard to how enlarge the future work there could be employed other analysis applications.

Bibliography

[1]. Guide to biometrics: Ruud M.Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior
[2]. Biometric identification systems,Rodrigo de Luis-Garc'(aa , Carlos Alberola-L'opeza; Otman Aghzoutb,Juan Ruiz-Alz-la
[3]. Attacks on Biometric Systems: A Case Study in Fingerprints
Umut Uludag*, Anil K. Jain*Department of Computer Science and Engineering,Michigan State University.
[4].Biometrics,
http://en.wikipedia.org/wiki/Biometrics#Countries_applying_biometrics
[5]. A computer-based system to support forensic studies on handwritten documents Katrin Franke, Mario K¨oppen
http://www.clopinet.com/isabelle/Projects/WANDA/proper/proper_white.pdf
[6]. The principle of proportionality in biometrics:Case studies from Norway
Yue Liu, Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo, Norway
[7]. European Biometrics Portal, Biometrics in Europe Trend Report 2007.
[8].Identity Assurance in the Information Age Biometrics, John D.Wood ward, Jr,Nicholas M.Orlans, Peter T.Higging.
[9]. Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Andrew Teoh Beng Jina, David Ngo Chek Linga,Alwyn Gohb aFaculty of Information Science and Technology (FIST), 2004
[10].A Behavioral Biometric System Based on Human Computer Interaction. Hugo Gamboa and Ana Fred.
[11]. Counter Hack Reloaded, Ed skouds with Tom Liston.
[12].Forastieri, V. Evidence against a Relationship between erma ztoglyphic Asymmetry and Male Sexual Orientation.
[13]. Toward Reliable User Authentication through Biometrics. *Václav (Vashek) Matyáˇs, Jr., Zdeneˇk Rˇíha*
[14].An Introduction to Biometric Recognition. Anil K. Jain, Arun Ross and Salil Prabhakar. 2004
[15].Biometric Demystified an IBM Research white paper by Matthew Lewis.
[16]. Security of Biometric Authentication Systems Parvathi Ambalakat.
[17]. Toward Reliable User Authentication through Biometrics. *Václav (Vashek) Matyáˇs, Jr., Zdeneˇk Rˇíha*
[18]. Extracting forensic evidence from biometric devices
Zeno Geradts*, Arnout Ruifrok Netherlands Forensic Institute, Netherlands. http://www.forensic.to/biometrie.pdf
[19]. Authentication Dr.ir. Patrick A.H. Bours, Gjøvik University College, NISlab 2008
[20].User Psychology and Biometric Systems Performance Julian Ashbourn.http://www.adept-associates.com/User%20Psychology.pdf
[21].Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints NISTIR 7110 C. L. Wilson, M. D. Garris, & C. I. Watson
MAY 2004
[22]. Biometric SSO authentication using Java Enterprise security Architect and Ramesh Nagappan CISSP Java Technology.
[23]. Biometric: the future of identification. Sharath Pankanti Ruud M. Anil Jain Michigan State University
[24].Schneier, B. the Uses and Abuses of Biometrics; Communications of the ACM 42/8 (1999)136.

[25].Biometrics-how to put to use and how not at all? Andreas Pfitzmann, Computer Science Department of Dresden University of Technology, Germany.
[26]. Security and Privacy. Published: Oslo, June 2007 Cover: Enzo Finger Design AS Print: ILAS Grafisk Text: Christine Hafskjold Illustrations.
[27]. Schneier, B. The Uses an Abuses of Biometrics, Communications of the ACM42/8(1999)
[28]. Practical Digital Signature Generation Using Biometrics, Taekyoung Kwon1 and Jae-il Lee2, Sejong University, Seoul 143-747, Korea
Korea Information Security Agency, Seoul 138-803, Korea,
[29]. Digital Signature / Keystroke Biometrics
http://www.findbiometrics.com/signature-keystroke/
[30]. Biometric Authentication Technology: From the Movies to Your Desktop by Fernando L. Podio1 and Jeffrey S. Dunn2,
[31]. on biometrics-based authentication and identification from a privacy-protection perspective Deriving privacy-enhancing requirements, V. Zorkadis and P.
[32]. Hall, J. A. Y. and Kimura, D. Dermatoglyphic Asymmetry and Sexual Orientation in Men; *Behavioral Neuroscience*, 108 (1994) 1203-1206. www.sfu.ca/~dkimura/articles/derm.htm
[33]. A Discussion of Biometrics for Authentication Purposes:
The Relevance of Untraceable Biometrics and Biometric Encryption. Information and Privacy CommissionerOntario, Canada, July 2009
[34]. Biometrics and Standards ITU-T Technology Watch Report December 2009, International Telecommunication Union, Telecommunication Standardization Policy Division ITU Telecommunication Standardization Sector .
[35]. Bridging Biometrics and Forensics,Yanjun Yan and Lisa Ann Osadciw, EECS, Syracuse University, Syracuse, NY, USA,
[36]. Handwriting in Forensic Investigations by Georgi Gluhchev
http://www.foibg.com/ijita/vol11/ijita11-1-p07.pdf
[37].Paconsulting ,Biometrics Is that really you?
http://www.dematerialisedid.com/PDFs/foresight_biometrics.pdf
[38]. Biometric Exit Programs Show Need for New Strategy to Reduce Visa Overstays, Backgrounder published by The Heritage of Foundation, 2010
[39]. Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats, James Goldstein, Rina Angeletti, Manfred Holzbach, Daniel Konrad, Max Snijder, Editor: Paweł Rotter, JRC Scientific and Technical Reports EUR 23564 EN – 2008
[40]. SAS launches biometrics at airports all over Sweden, Scandinavian Airlines
http://feed.ne.cision.com/wpyfs/00/00/00/00/00/08/C8/F9/wkr0001.pdf
[41]. Council of the European Union Brussels, 24 October 2006
[42]. Visa Waiver Program(VWP).
http://travel.state.gov/visa/temp/without/without_1990.html
[43]. Sas får bruke fingeravtrykk
http://www.datatilsynet.no/templates/article 1852.aspx
[44]. Biometric Authentication —Security and Usability V´aclav Maty´aˇs and Zdenˇek ˇR´ıha Faculty of Informatics, Masaryk University Brno, Czech Republic.
[45].Data Protection Law, Approaching Its Rationale, Logic and Limits. Lee A.Bygrave.
[46].Biometrics in national and international solution.
http://www.datatilsynet.no/upload/Dokumenter/saker/2006/Revisjon_12biomerti.pdf
[47]. On the reconstruction of biometric raw data from template data Manfred Bromba http://www.bromba.com/knowhow/temppriv.htm

[48]. Flesland A. Begrenset adgang til bruk av biometriske kjennetegn. Retrieved Feb 14, 2006, from http://www.datatilsynet.no/ templates/Page____1342.aspx, 2006 (in Norwegian).
[49]. Wilson S. Lockstep submission to senate privacy inquiry.Retrieved August 26, 2006
[50]. COUNCIL OF THE EUROPEAN UNION, Brussels, 24 October 2006 [51]. MULTIMODAL BIOMETRICS: AN OVERVIEW, *Arun Ross and Anil K. Jain,* West Virginia University Michigan State University, Morgantown,WV 26506 USA East Lansing, MI 48823 USA
[52]. Cavoukian A. Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy. Retrieved March 8, 2007.
[53].Balancing the needs for increased security and the protection of fundamental rights in the new generation of video surveillance networks: the example of DYVINE project. Fanny Coudert Interdisciplinary Center for Law & ICT(ICRI)-Katholieke Universiteit
[54]. The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification, Jeremy Wickins.
[55]. Keystroke Dynamics: Low Impact Biometric Verification Tom Olzak september 2006
[56]. Biometric: the future of identification. Sharath Pankanti Ruud M. Anil Jain Michigan State University.
[57]. Keystroke Dynamics: Low Impact Biometric Verification, Tom Olzak September 2006.
[58]. Biometric Technology Application Manual Volume One: Biometric Basics Compiled and Published by:National Biometric Security Project Updated Summer 2008.
[59].Palement Verification Using Complex Wavelet Transform by Lei Zhang, Zhenhua Guo, Zhou Wang and David Zhang.
[60].Signature recognition, Ravi Das.
[61].Hands-Free Mouse-Pointer Manipulation Using ,Motion-Tracking and Speech Recognition, Frank Loewenich and Frederic Maire, Faculty of Information Technology, Australia.
[62].Biometric Authentication and Identification using Keystroke Dynamics with Alert Levels Master thesis, Alex Andersen Oslo University College.
[63].The DNA Field Experiment: Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes. John K. Roman, Shannon Reid, Jay Reid, Aaron Chalfin, William Adams, Carly Knight.
[64].Gait Recognition System: Bundle Rectangle Approach. Edward Guillen, Daniel Padilla, Adriana Hernandez Military University Bogota, Colombia. Kenneth Barner University of Delaware.
[65].Human Ear Recognition in 3D. Hui Chen, Student Member, IEEE, and Bir Bhanu, Fellow, IEEE.
[66]. Biometrics Newsletter 10 ,Rene Bense, 2009 http://www.riseproject.eu/_fileupload/Press/Hong%20Kong%20Conference/Biometrics4you.pdf
[67]. BIOMETRIC TECHNIQUES: Review and evaluation of biometric techniques for identification and authentication by Dr. Despina Polemi, Institute Of Communication and Computer Systems National Technical University of Athens.
[68]. The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification by Jeremy Wickins.

[69]. Privacy& Biometrics Building a Conceptual Foundation. National science and Technology Council and Committee on Technology http://www.biometrics.gov/docs/privacy.pdf
[70]. Fingerprint Biometrics: Address Privacy Before Deployment. Ann Cavoukian, Ph.D. Commissioner, 2008.
[71]. Biometrics: Enhancing Security or Invading Privacy? Opinion, Published by The Irish Council for Bioethics, Dublin 2009.
[72].Privacy and Biometrics by Ann Cavoukian, Ph.D. Commissioner, 1999.
[73].Biometric-Based Technologies, Working Party on Information Security and Privacy, organization for Economic Co-operation and Development
[74]. Retina & Vitreous Consultants of Wisconsin Notice of Privacy Practices, The U.S. Department of Health and Human Services 2003.
[75].Voice Privacy and Security By Mike Kelley.
[76].Reading Your Every Keystroke: Protecting Employee E-mail Privacy by Samuel D. Warren & Louis D. Brandeis.
[77].Affective Sensors, Privacy, and Ethical Contracts by Carson Reynolds and Rosalind W. Picard.
[78].Biometrics at the Frontiers: Assessing the Impact on Society, European Commission 2005.
[79].United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics, NBSP Publication 2006.
[80]. A Secure Template Generation Scheme for Palmprint Recognition Systems, by Saroj Kumar Panigrahy 2008.
[81]. Biometric Authentication System Using Human Gait by Philippe C. Cattin
Swiss Federal Institute of Technology Z¨urich, 2002.
[82]. Privacy Issues in an Electronic Voting Machine Arthur M. Keller, UC Santa Cruz and Open Voting Consortium.
[83].Keystroke Dynamic as a Biometric for Authentication, Fabian Monrose Mathematical Science, Network University.
[84]. Laptop Computer Security, White Paper, Caveo, November 2003.
[85]. Your face is NOT your password Duc Nguyen Bkis, Vietnam.
Http://www.bkav.com.vn

Appendix A

1. Is your organization/company using an authentication mechanism for physical access to the building?
   - Yes
   - No

2. What authentication mechanism is your organization/company using for physical access to the building?
   - Visual (e.g. a guard)
   - Card
   - Card + (PIN) code
   - Biometrics
   - Other

3. What biometric authentication mechanism is your organization/company using for physical access to the building?
   - Fingerprint
   - Face recognition
   - Voice recognition
   - Iris scan
   - Other

4. Is your organization/company using an authentication mechanism for physical access to critical areas inside the building?
   - Yes
   - No

5. What authentication mechanism is your organization/company using for physical access to critical areas inside the building?
   - Visual (e.g. a guard)
   - Card
   - Card + (PIN) code
   - Biometrics
   - Other

6. What biometric authentication mechanism is your organization/company using for physical access to critical areas inside the building?
   - Fingerprint
   - Face recognition
   - Voice recognition
   - Iris scan
   - Other

7. Is your organization/company using an authentication mechanism for access to computers, servers, printers, etc.?
   - Yes
   - No

8. What authentication mechanism is your organization/company using for access to computers, servers, printers, etc.?
   - Token

Username only
Password only
Username and password
Biometrics
Other

9. What biometric authentication mechanism is your organization/company using for access to computers, servers, printers, etc.?
Fingerprint
Face recognition
Voice recognition
Keystroke Dynamics
Other

10. Is a policy in place for the use of creating and using passwords?
Yes, on the length of the password
Yes, on the different types of characters used
Yes, on the renewal period and re-use of old passwords
Yes, passwords are provided centrally
No
Other

11. Are you aware of the existence of the following biometric modalities (0=Completely unaware; 1=Heard of it before; 2=I know it somewhat; 4=I know it well; 5=I am an expert):
Fingerprint recognition
Face recognition
Palm print recognition
' Iris recognition
Retina recognition
DNA recognition
Ear recognition
Voice recognition
Signature recognition
Gait recognition
Keystroke recognition
Mouse recognition

12. Do express your opinion on the security of the following authentication mechanisms (0=No opinion; 1=Unsecure; 2=Slightly unsecure; 3=Neutral; 4=Slightly Secure; 5=Secure):
Username / Password mechanism
Token mechanism
Fingerprint recognition
Face recognition
Palm print recognition
Iris recognition
Retina recognition
DNA recognition
Ear recognition
Voice recognition
Signature recognition
Gait recognition

Keystroke recognition
Mouse recognition

13.Do express your opinion if the following authentication can provide privacy for the users (0=No opinion; 1= No privacy guaranteed; 2= little privacy guarantees; 3=Neutral; 4=A lot of privacy guaranteed; 5=Privacy totally guaranteed)

Username / Password mechanism
Token mechanism
Fingerprint recognition
Face recognition
Palm print recognition
' Iris recognition
Retina recognition
DNA recognition
Ear recognition
Voice recognition
Signature recognition
Gait recognition
Keystroke recognition
Mouse recognition

14. Do express your feeling about the cost of operation for a system using the following authentication mechanisms (0=No opinion; 1=Very expensive; 2=Slightly expensive; 3=Neutral; 4=Slightly cheap; 5=very cheap):

Username / Password mechanism
Token mechanism
Fingerprint recognition
Face recognition
Palm print recognition
' Iris recognition
Retina recognition
DNA recognition
Ear recognition
Voice recognition
Signature recognition
Gait recognition
Keystroke recognition
Mouse recognition

15. Do you know that many new laptops have a fingerprint reader incorporated that can be used instead of the usual password mechanism?

Yes, but I do not think it is secure?
Yes, but I do think that administration is too much work
Yes, but company/organization policy prohibits its use
Yes, and I would like to use it in the future
Yes, and we are using it already
No, but it sounds interesting
No, but it is not of interest to our company/organization

16. Do you know that many new laptops have a webcam incorporated that can be used for face recognition instead of the usual password mechanism?

Yes, but I do not think it is secure?
Yes, but I do think that administration is too much work

Yes, but company/organization policy prohibits its use
Yes, and I would like to use it in the future
Yes, and we are using it already
No, but it sounds interesting
No, but it is not of interest to our company/organization

17. Do you know that the ordinary username/password mechanism can be secured better by using biometric keystroke dynamics?

Yes, but I do not think it is secure?
Yes, but I do think that administration is too much work
Yes, but company/organization policy prohibits its use
Yes, and I would like to use it in the future
Yes, and we are using it already
No, but it sounds interesting
No, but it is not of interest to our company/organization

18. Is your company/organization in some way using, or interested in using biometrics?

Yes, we are using it today already
Yes, we are interested in using it in the future
No, we are not interested in using it now or in the future

19. What kind of biometrics are you using today?

Fingerprint recognition
Face recognition
Palm print recognition
Iris recognition
Retina recognition
DNA recognition
Ear recognition
Voice recognition
Signature recognition
Gait recognition
Keystroke recognition
Mouse recognition
Other, please specify
Don't know

20. In your experience, is the biometric system as secure as a username/password mechanism?

Security of biometrics is higher
Security of biometrics is comparable to security of a username/password mechanism
Security of a username/password mechanism is higher
Other, please specify
Don't know

21. Did you provide the users with information on what kind of personal data will be stored?

Yes, we provided them with a lot of written information
Yes, we provided them with a lot of spoken information
Yes, we provided them with some written information

Yes, we provided them with some spoken information
No, but we did announce that some personal data would be stored
No, we did not mention this at all
Other, please specify
Don't know

22. Did the opinion of the users on the biometric system change over time?

23 How satisfied are users with the biometric authentication?
Very unsatisfied
Unsatisfied
Indifferent
Satisfied
Very Satisfied

24. What kind of biometrics are you planning to use in the future?

25. What do you think are the operational costs compared to the username/password mechanism?
Operational costs of biometrics is higher
Operational costs of biometrics is comparable to operational costs of a username/password mechanism
Operational costs of a username/password mechanism is higher
Other, please specify
Don't know

26. How did the users react when hearing that they had to use a biometric system?
Fingerprint recognition
Face recognition
Palm print recognition
' Iris recognition
Retina recognition
DNA recognition
Ear recognition
Voice recognition
Signature recognition
Gait recognition
Keystroke recognition
Mouse recognition
Other, please specify
Don't know

27. Will you provide the users with information on what kind of personal data will be stored?

28. Why your company/organization not interested in using biometrics?
Operational costs will be too high
Initial costs will be too high
System is not secure
Regulations / Norwegian law prohibits the use of biometrics
Strong opposition from the users
Unfamiliarity with biometrics

29.Do you feel that more knowledge about biometric systems could change your opinion on the use of biometrics?

Yes
No
Other, please specify
Don't know

30.Do you feel that Norwegian laws/regulations stand in the way of usage of biometric authentication in Norway?

Yes
No
Other, please specify
Don't know

31. What is the size of the company?

1-5
6-25
26-100
101+

32. What type best describes your organization/company

Governmental
Non-profit organization
Educational
National commercial company
International commercial company targeted towards northern Europe
International commercial company targeted towards the whole world

33. Are you willing to participate in a possible follow up of this questionnaire (In case of a yes answer, please provide contact details in the next questions)?

Yes, I am willing to answer another questionnaires on this topic
Yes, I am willing to participate in an oral interview
No, I am not interested in further participation

34. If you would like to be informed of the results, please enter your contact details here.

Appendix B

1 Article8 (95/46/EC)

(1)Amend recital 33 as follows:

(i) Delete the first sentence and substitute the following:
"Whereas personal data revealing racial or ethnic origin, political opinions religious or philosophical beliefs or trade union membership and personal data concerning health or sex life require special protection where they clearly describe intimate personal characteristics and their processing is particularly likely to infringe fundamental freedoms or privacy; whereas such data should in principle not be processed;"

(ii) In the second sentence, after "explicitly provided for" insert "where the data subject gives his explicit consent or".

(2)In Article 8.2(c), delete:
"where the data subject is physically or legally incapable of giving his consent"

(3) Add new Article 8.2(f):
"(f) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract, provided that the data subject has been expressly informed that the processing will involve such *data as are mentioned in paragraph 1."*

(4) In Article 8.5, delete:
"subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards".

2 Article 9

1. Personal data shall not be further processed in a way incompatible with the purposes for which they have been obtained.
2. For the purposes of assessing whether processing is incompatible, as referred to under (1), the responsible party shall in any case take account of the following:
a. the relationship between the purpose of the intended processing and the purpose for which the data have been obtained;
b. the nature of the data concerned;
c. the consequences of the intended processing for the data subject;
d. the manner in which the data have been obtained, and
e. the extent to which appropriate guarantees have been put in place with respect to the data subject.
3. The further processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible where the responsible party has made the necessary arrangements to ensure that the further processing is carried out solely for these specific purposes.

3 Article 11

1. Personal data shall only be processed where, given the purposes for which they are collected
or subsequently processed, they are adequate, relevant and not excessive.
2. The responsible party shall take the necessary steps to ensure that personal data, given the
purposes for which they are collected or subsequently processed, are correct and accurate.

4 Article 12: Related to knowledge

1. Anyone acting under the authority of the responsible party or the processor, as well as the processor himself, where they have access to personal data, shall only process such data on the orders of the responsible party, except where otherwise required by law.
2. The persons referred to under (1), who are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, are required to treat as confidential the personal data which comes to their knowledge, except where the communication of such data is required
by a legal provision or the proper performance of their duties. Article 272(2) of the Penal Code is not applicable.

5 Article 29 Data Protection Working Party[19]

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA
set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[20],
Having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,
Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

[19] www.europa.eu.int/comm/privacy

[20] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

Has adopted the present Opinion:

In recent years, the Working Party has repeatedly commented on the issue of retention of communication traffic data[21], and the European Conference of Data Protection Commissioners has issued several joint statements on the same subject[22]. The proposal for a draft Framework Decision on the retention of such traffic data presented by four member states in the Council of the European Union once again calls for an opinion of the Working Party. In view of the early stage of discussion in the relevant working party of the Council, this opinion has a preliminary character. The Working Party intends to reconsider the subject, on the basis of a revised draft, at a later stage.

The Working Party has examined whether the draft is in conformity with the standards of Article 8 of the European Convention on Human Rights.

In this context it is essential to take into account that citizens increasingly perform daily activities and transactions using electronic communications networks and services. The data generated by these communications - so called 'traffic data' - possibly including details about time, place and numbers used for fixed and mobile voice services, faxes, emails, SMS and other use of the Internet, therefore also increasingly reflect a range of details concerning the way in which these citizens conduct their daily lives.

In its *Recommendation 2/99 on the respect of privacy in the context of interception of*
telecommunications, adopted on 3 May 1999 the Working Party defined interception as the act of a third party acquiring knowledge about the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services. On that occasion the Working Party stated that each telecommunications interception (including monitoring and data mining traffic data) constitutes a violation of individuals' right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable unless they fulfill three fundamental criteria in accordance with Article 8 (2) of the European Convention and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention.

The Working Party takes the view that the same fundamental criteria apply to the retention of traffic data beyond what is needed for the delivery of communications

---

[21] See: Recommendation 3/97 on Anonymity on the Internet; Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications; Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes; Opinion 7/200 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385; Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime; Opinion 10/2001 on the need for a balance approach in the fight against terrorism; Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on
mandatory systematic retention of telecommunication traffic data; Opinion 1/2003 on the storage of traffic data for billing purposes. A summary of these statements can be found in the annex to this opinion. All documents are also available at

[22] http://europa.eu.int/comm/internal_market/privacy.See statements adopted in Stockholm (April 2000) and Cardiff (2002).

services and other legitimate business purposes, and to any subsequent access to these data for law enforcement purposes[23].
The Working Party again has considerable doubts whether these fundamental criteria are fulfilled in the Draft framework decision. To start with the first criterion (legal basis), considering the preliminary status of the discussions in the Council, the Working Party does not consider it opportune to deal with this at this moment. With regard to the third criterion (conformity with a legitimate and listed aim) the Working Party questions the very aim of the Draft. Would that aim indeed solely be the prevention, investigation, detection and prosecution of criminal offences as was stated in the draft (Ground 7), while excluding other aims listed in Article 8? This aim must be clear in the first place.
With regard to the second criterion (need in a democratic society), according to the ECHR's interpretation the interference must respond to a "pressing social need" (e.g. the judgment in class v. Federal Republic of Germany of 18 November 1977, European Court of Human Rights, Series A No 28). The Court of Human Rights recognized the right of the Contracting States to carry out secret surveillance on personal correspondence and telecommunications in exceptional cases and under specific conditions. At the same time, it added:
"... this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such as law poses of undermining or even destroying democracy on the ground of defending it, confirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate" (class, p. 3).
The routine, comprehensive storage of all traffic data, user and participant data proposed in the draft decision would make surveillance that is authorized in

[23] This is supported by the case law of the European Court of Human Rights. For example, in the Amann judgment (pp. 30) the storage by the authorities of information alone was held to be an interference, whether that data are used against the individual or not. In the Rotaru judgment as well, the storing of historical information by the secret services constituted interference. In the PG v. UK judgment the Court stated (pp.42) that metering does not per se offend against Article 8, for example if done by the telephone company for billing purposes. Obtaining information from the provider relating to numbers called on a telephone by the police, however does interfere with the private life or correspondence. In the Malone case (pp. 84) too the Court ruled that the transfer of metering data from an operator to the police was an interference with 'correspondence' in Article 8. From these cases one might conclude that the mandatory storage of traffic data by providers of telecommunication does in itself not constitute an interference with Article 8, while the transfer of such data to the authorities or the further processing does. That conclusion would be wrong. In MM v. The Netherlands the Court ruled that authorities cannot avoid liability by making use of private persons when they make a crucial contribution to the execution of the surveillance scheme. Consequently, this would mean for instance that data retention and data mining in their own systems by telecommunication operators for public order purposes will constitute an interference too.

exceptional circumstances the rule. This would clearly be disproportionate. The draft framework would apply, not only to some people who would be monitored in application with specific laws, but to all natural persons who use electronic communications. Additionally all the communications sent or received would be covered. Not everything that might prove to be useful for law enforcement is desirable or can be considered as a necessary measure in a democratic society, particularly if this leads to the systematic recording of all electronic communications. The framework decision has not provided any persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combating crime or protecting national security. The requirement for operators to retain traffic data which they don't need for their own purposes would constitute a derogation without precedent to the finality/purpose principle.

Analysis carried out by telecommunication companies in Europe reveal the biggest amount of data demanded by law-enforcement were not older than six months. This shows that longer periods of retention are clearly disproportionate.

It should be noted that representatives of the law enforcement community have failed to provide any evidence as to the need for such far reaching measures. Indeed, they have been totally and conspicuously absent at recent workshops organized with a view to consider the background and the consequences of the present proposal for a draft Framework Decision.

The Convention on Cybercrime provides only for individual secure storage on the "fastfreeze – quick thaw" model which, by contrast with the views of the four proposing Governments, is entirely adequate for the prevention or prosecution of criminal offences. It is characteristic of current legal discussions that the present proposal is being seriously discussed before the Convention on Cybercrime has entered into force in most signatory states and its practical consequences can be assessed. The Article 29 Working Party has already stated (Opinion 5/2002) that the retention of traffic data for purposes of law enforcement should meet strict conditions under Article 15(1) of Directive 2002/58/EC, i.e. in all cases, only for a limited period and when necessary, appropriate and proportionate in a democratic society. Also the European Data Protection Commissioners at their International Conference in Cardiff (9-11 September 2002) have made a statement on mandatory systematic retention of traffic data. It was pointed out that the systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable.

Not only does the draft Framework Decision fail to cover those conditions, it expressly seeks to nullify them by not requiring definite grounds of suspicion and a reliable basis in fact in individual cases and providing for comprehensive data storage as precautionary measure in future legal proceedings against any users of electronic communications systems.

The Working Party is of the opinion that the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided in the draft Framework Decision, is not acceptable within the legal framework set in Article 8.

Done at Brussels, on 9th November 2004
For the Working Party the Chairman