Implementation of biometric authentication methods for home based systems

A dissertation submitted in partial fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Business Information Systems.

By Rafie Rahim

ST20054574

Department of computing & Information Systems
Cardiff School of Management
Cardiff Metropolitan University
April 2016
Declaration

I hereby declare that this dissertation entitled *Implementation of Biometric Authentication Methods for home based systems* is entirely my own work, and it has never been submitted nor is it currently being submitted for any other degree.

Candidate: Rafie Rahim
Signature:
Date: 22/04/2016

Supervisor: Dr. Hilary Berger
Signature:
Date: 22/04/2016
Abstract

Biometric authentication systems use physical traits of a user in order to give the user access control. Previously the most common and widely method of securing access control is done via knowledge based authentication systems (e.g; Passwords) and Token based Authentication systems (e.g; USB Security key fob). These traditional systems however are not able to meet strict security performance requirements of a number of modern applications such as in devices and home security systems. Biometric systems offer quite a lot more advantages over these traditional methods of authentication, they are more secure and more reliable. In this dissertation, the aim of this dissertation is to evaluate the possibility of implementing a biometric system of authentication to be used for home systems such as desktop computers and home security systems. The issues which will be talked about in this dissertation will be about how secure the biometric system is compared to the traditional methods of authentication which are knowledge based and token based authentication methods. The research will also look into the current trends and patterns into what the public thinks about these biometric systems as a replacement to their current usage of knowledge based and token based methods of authentication. Finally the research will evaluate on whether it is possible to implement the biometrics into daily use or not depending on the data that is received from the research sample.
Acknowledgement

I would like to thank my parents for always supporting me, my close friends and housemates who have always been there for me whenever I needed help with anything especially with the assignments and dissertation, my lecturers from Cardiff Metropolitan University which have helped me throughout my 3 years of study in the university particularly Dr. Hilary Berger who is my supervisor for my dissertation project, I also would like to thank the respondents of the research sample which had made this research possible.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.3 – Sampling Technique</td>
<td>18</td>
</tr>
<tr>
<td>3.2 – Sample study on the security of their devices</td>
<td>19</td>
</tr>
<tr>
<td>3.3 – Sample study on home security systems</td>
<td>24</td>
</tr>
<tr>
<td>3.4 – Awareness of available biometrics</td>
<td>25</td>
</tr>
<tr>
<td>3.5 – Sample’s thoughts on implementation of biometric systems</td>
<td>30</td>
</tr>
<tr>
<td>4 – Conclusion</td>
<td>34</td>
</tr>
<tr>
<td>References</td>
<td>36</td>
</tr>
<tr>
<td>Appendices</td>
<td>38</td>
</tr>
<tr>
<td>Appendix A – Ethics Approval Form</td>
<td>38</td>
</tr>
<tr>
<td>Appendix B – Sample of Participant Information Sheet</td>
<td>43</td>
</tr>
<tr>
<td>Appendix C – Sample of Participant Consent Form</td>
<td>45</td>
</tr>
<tr>
<td>Appendix D – Participant Questionnaire Form</td>
<td>47</td>
</tr>
<tr>
<td>Appendix E – Results of Primary data Gathering analysed from Google forms</td>
<td>52</td>
</tr>
</tbody>
</table>
Investigating the plausibility of implementing a Biometric System on to home based systems

1.0 – Introduction

Biometric security systems are systems which use information about a person which is unique only to that one person in order to identify and authenticate that person is the authorised person that is given access to a certain object/device or a security clearance for restricted locations. These systems rely on specific data about the unique biological traits of the user such as finger prints, face recognition, voice recognition and irises in order to operate effectively. Biometric systems tend to become a more reliable security measure than traditional forms of access control such as token-based identification systems and knowledge based systems. These traditional knowledge based systems basically use user’s identification and knowledge such as drivers licence, passports, passwords and personal Identification numbers and information such as these are able to be stolen or copied by others which is not quite a very secure system. The biometric systems eliminates this threat by using the user’s unique biometric identity in order to give access to the user as the biometric properties on each person such as their fingerprints, voice and iris patterns. These biometric patterns are usually not able to be copied and thus these biometric systems tend to be a much more reliable system to be used for access control for many companies and government facilities such as security firms, police, intelligence agencies and military installations that may hold sensitive information in multiple restricted areas. As it is becoming a much more common type of security measure for most companies nowadays, there may be a demand growing to have these biometric systems to be implemented into homes as biometric security systems or for home devises. Home based systems such as personal computers, desktops and even home security systems are usually using knowledge based identification systems such as pin numbers or passwords. Although this may be secure for some users, this can be quite a problem for home owners as anyone can easily copy of a pin number or password or even hack their way into a password protected system given the correct tools and software. Having a biometric security system for home based systems will eliminate the problem of having unauthorized users from accessing the computer or entering the house.
1.1 – Aims and Objectives

1.1.1 - Aim
The main aim for this project is to investigate the possibility of implementing biometric security systems on to home based systems such as desktop PCs or home security systems.

1.1.2 – Objectives
- To identify the security systems which are available to be used for home based security systems or computing devices such as desktop computers for home use.
- To investigate any problems with using a current knowledge based systems in order to access control for home based security and computing systems.
- To identify whether it is possible or not to integrate biometrics into home based security and computing systems.
- To investigate whether it is plausible to have knowledge based security system and biometrics at the same time to improve the security level of the systems.

1.2 – Methodology
The main purpose for primary data gathering for this research will be to gather general information about how much the public sample is aware of biometric systems which are available to them and whether they are willing to implement such systems into their daily working habits or devices.

The methods that will be used in order to undertake this research will rely on quite a few data gathering techniques to gather qualitative and quantitative data about the current issues in question. The data which will be collected is going to be a combined mix of primary and secondary research data. This data will be taken from the views and opinions of a public sample of which will be collected by conducting online surveys created by Google forms. The reason for which Google forms will be used is that the forms provide built in analysis tools as well making data analysis easier and saves time.

Secondary research data such as definitions about biometric systems, the type of biometrics which are available to the public and other relevant data on biometric systems will be also collected from online sources such as websites on biometric systems and forums and other forms of secondary research data which may be available from library books and journals. All the primary research data will then be analysed altogether by using the help of built in features of Google forms as well to look for trends of what the public sample thinks about having biometric systems as security systems for home based systems.
1.3 – Scope and Constraints
The main scope of this research will be concentrated on what are biometrics and what kind of biometrics are currently available out there which are available for to the public. The research will also be concentrated on identifying the advantages and disadvantages of having a biometrics system for home based systems. Another aim for this research is to investigate the threats which are possible to be encountered when using traditional forms of authentication methods such as passwords and tokens and how is it possible to use biometrics to remove the threat of the system from being tricked into giving access to unauthorised users.

1.4 – Resources
The University’s Library and IT facilities would be adequate enough for the majority of the research and analysis that will be required to undertake this research. Availability of the researcher’s own Computer to conduct research off campus may also be adequate enough to help the researcher to conduct primary and secondary research through online sources. Online E-books are also widely available online to be used as referencing material in order to conduct the research.

1.5 – Timetable/Gantt Chart

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Name</th>
<th>Duration</th>
<th>Start date</th>
<th>End date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary research gathering</td>
<td>42 days</td>
<td>11/12/15</td>
<td>08/02/16</td>
</tr>
<tr>
<td>2</td>
<td>Secondary research gathering</td>
<td>42 days</td>
<td>11/01/16</td>
<td>08/03/16</td>
</tr>
<tr>
<td>3</td>
<td>Analysis of gathered research data</td>
<td>41 days</td>
<td>01/02/16</td>
<td>28/03/16</td>
</tr>
<tr>
<td>4</td>
<td>Finalising research data for report</td>
<td>26 days</td>
<td>14/03/16</td>
<td>18/04/16</td>
</tr>
<tr>
<td>5</td>
<td>Report write up</td>
<td>41 days</td>
<td>22/02/16</td>
<td>18/04/16</td>
</tr>
<tr>
<td>6</td>
<td>Preparation for Submission</td>
<td>5 days</td>
<td>18/04/16</td>
<td>22/04/16</td>
</tr>
</tbody>
</table>
2.0 – Background Research

2.1 – Introduction to Biometric Systems

2.1.1 – What are Biometrics?
“Biometrics refers to the automatic identifications of a person based on his or her physiological or behavioural characteristics” (John Chirillo and Scott Blaul 2003, p.2) Biometrics are basically the measurement and statistical analysis of an individual’s physical and behavioural characteristics. The term has been derived from Greek words “bio” which means life and “metric” which means to measure and biometrics usually are identified by two main characteristics namely the physiological characteristics which include an individual’s fingerprints, DNA, facial pattern, hand imprints, retina, ear pattern/features and even odour; and the behavioural characteristics which is the behaviour of the individual as a whole which includes typing rhythm, gait, gestures and voice. These features are very much unique to each and every individual and this makes it ideal for use as an identification and access control and security purposes.

“A biometric system is essentially a pattern-recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristics possessed by the user” (Scott Blaul 2003, p.3). Typically biometrics have been developed in two ways which is to mainly for verification and identification. Verification systems are basically systems which are designed to verify that the individual is who the individual really is by comparing the individual’s biometric data with the individual’s biometric data which is already enrolled within the database of the system. Identification systems do not require the individual to claim an identity as the provided biometric data is compared to data from a number of users to find a match (Nanavati 2002, p.12).

2.1.2 – Types of Biometrics

There are multiple types of biometrics for an individual who uses a form of biometric identification form of access control and these include a variety of properties which are recorded from the individual to identify the individual and these include DNA matching, ear shape recognition, eye pattern recognition, face recognition, finger print recognition, finger geometry recognition, gain, hand geometry recognition, odour, signature recognition, typing recognition, vein recognition and voice pattern recognition (Biometricsinstitute.org, 2016). Of all these different types of biometric recognition types, the most common biometrics being used are the fingerprint pattern recognition, facial recognition, eye pattern recognition and voice pattern recognition, but by far the most commonly used form of pattern recognition is the fingerprint pattern recognition as it is the most simple and cost effective one to be used.
2.1.2.1 – Fingerprint Recognition

“Biometric data found in the fingerprint develops with the individual, they are naturally unique and provide reliable recognition points for identification.” (Ievoreader.com, 2016). Each and every person has a unique unchanging fingerprint pattern and this can be used as a unique identifier. Each fingerprint of an individual is made of a series of ridges and furrows on the surface of the finger and these patterns of ridges and furrows are used to determine the uniqueness of the fingerprint. The way fingerprint recognition works is that the fingerprint pattern is firstly needed to be registered on the fingerprint scanner database. Once registered onto the database of the fingerprint scanner, the image of the patterns are converted into a code through a mathematical sequence called an algorithm which effectively becomes a digital form of the individual. When the individual scans their fingerprint, the current scan of their fingerprint pattern is stored in a temporary buffer database for comparison with data that is already stored within the database and if the comparison comes up as a match, the system then grants the individual access for control of the device or access through a secured area.

2.1.2.2 – Facial Recognition

“Like all biometrics solutions, face recognition technology measures and matches the unique characteristics for the purposes of identification or authentication.” (FindBiometrics, 2016). Facial recognition basically works in the same manner as fingerprint scanners but the difference is that facial recognition records the facial features of an individual rather than the fingerprints of the individual. It measures and matches the unique characteristics of the individual’s unique facial characteristics for the purpose of identification and authentication. This is usually implemented by using a digital or connected camera, the facial recognition software is able to detect the faces and store them in the database as images which are then processed as to identify specific features of the individual’s facial structure which will then be compared and matched against a stored template within the database.

2.1.2.3 – Eye pattern recognition

Eye pattern recognition is usually divided into two different categories which are mainly the iris recognition and the retina recognition. Both these pattern recognition techniques share the same techniques in identifying and matching patterns in that they both use the individual’s eyes but iris recognition uses mathematical pattern recognition techniques on video images of one or both the iris of the individual’s eyes whose complex random patterns are unique, stable and can be seen from some distances. Retina scanning on the other hand is different because it is the ocular based biometric technology that
uses the unique patterns on an individual’s retina blood vessels (Wikipedia, 2016).

Iris recognition systems are quite complex systems as these recognition systems can identify nearly up to more than 200 identifications points on an individual’s iris which include the rings, furrows and freckles within the individual’s iris (Wikipedia, 2016). The first stage, the system needs to localize the inner and outer boundaries of the iris which is the pupil and the limbus in an image of the eye, the system then detects and excludes any other unnecessary items such as the eyelids and eyelashes and specular reflections which often occur in several parts of the iris. The set or pixels which contain only the iris is then normalized by a rubber sheer model to compensate for pupil dilation or constriction and is then analysed to extract a bit pattern encoding the information needed to compare two iris images. Eye pattern recognition is one of the most secure forms of recognition systems available out there but as complex as it is, it is quite costly to implement and thus is rarely used in common day to day operations. This type of recognition is mainly used for companies or government firms which deal with heavy security that requires a very strict data and location access.

2.1.2.4 – Voice Pattern Recognition
“Voice has emerged as a viable authentication method because just like a fingerprint or iris, voice is unique to the individual” (Authentify, 2015). Voice is another biometric property which can be measured in terms of voice patterns and is unique to the individual just the same as fingerprint and iris recognition systems. Voice biometrics is a numerical representation of the sound, pattern and rhythm of an individual’s voice and this “voice print” is as unique to an individual as a palm or a fingerprint. An individual’s exact voice is quite difficult to forge for biometrics comparison and authentication purposes as qualities that are measured within the voice print include a wide range of qualities such as the dialect and speaking style to pitch, spectral magnitudes and format frequencies. The vibration of the individual’s vocal chords and the patterns which are created by the physical components result in a speech pattern which is distinctive as an individual’s fingerprint.

2.1.3 – Biometric Authentication Systems
“Biometric authentication systems compare the current biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed and access is granted.” (SearchSecurity, 2016).

Biometric Authentication by verification of biometric features are becoming increasingly common in corporate and public security systems, consumer electronics, and point-of-sale applications nowadays with the advancement of rapidly evolving technologies and in addition to the secure nature of
biometric security systems. Another main driving force behind the biometric verification is the ease of use and convenience it offers to individuals who implement this technology in their normal work routine. This is due to the fact that with the use of biometrics as a source to verify that the individual is in fact the authorised individual, there is no longer use for any passwords or security tokens to be entered or used in order for the individual to access anything.

2.2 – Biometric systems vs other known security authenticators.
Security systems offer various ways of authentication and these are usually categorised into 3 which are knowledge based authentication methods, security token based authentication methods and biometric based authentication methods.

2.2.1 – Knowledge Based Authentication
Knowledge based authentication methods are the simplest form of secure authentication methods which are widely available to the public. Almost everyone in the world is using some kind of knowledge based form of authentication in everyday routines the most common of which is in this modern world people log into social media on a daily basis using simple passwords. Knowledge based authentication is basically an authentication scheme in which the individual provides some sort of secret answer to a secret question or a password which is then compared to a database template for authentication (SearchSecurity, 2016).

Knowledge based authenticators are categorized in two types and these are static and dynamic authenticators. Static knowledge based authenticators are commonly used by banks, financial services, companies and email providers. The static knowledge based authenticator uses a kind of system in which shared secrets or shared secret questions are exchanged between the individual and the provider to prove the identity of the individual before allowing access to accounts or as a backup access to when the individual forgets their password (Wikipedia, 2016).

Dynamic knowledge based authenticators is a much more higher level of authenticator which uses knowledge questions to verify the identity of the individual but it does not require the individual to provide the questions and answers beforehand unlike static which requires the individual to provide secret questions and answers to the provider for identification purposes. Both these knowledge based authenticators are quite secure in their own ways but at time it can be easily cracked as an individual only needs to know the secret question and answer or password from another individual and this might be in the form of birth date, home address, memorable places and other personal data which can be easily identified.
Facebook for example uses a knowledge based authenticator for its users. An individual may simply put in their email address and password to easily log into their account. Most people try to keep passwords as simple as possible and this means that their passwords would be something memorable that only that individual knows which might be the name of their first pet, the name of their spouse, son or daughter, birthdates, memorable places and favourite things. Some even have a mix of words and numbers in their passwords to improve the complexity but still include things which are easily to remember for the individual. This means that anyone who knows the individual well enough is easily able to hack into their Facebook account and may cause harm by taking over their account and locking out the legitimate user from using their Facebook account.

2.2.2 – Security Token Based Authentication
Security tokens are basically hardware token or USB token in which is a physical device that an authorised user is given to in order to ease authentication processes (Wikipedia, 2016). Security tokens prove an individual’s identity electronically for example when an individual wants to access their bank account, a token which is given to the individual in the early stages of administration will allow the individual to have access to the bank account. Security tokens for banks usually ask for the individual to input a set pin number by the individual and in turn will give the individual some sort of 6 digit pin number which changes every time the individual uses the token as a form of a security ticket which is available for only a short period of time. The individual will firstly give the bank their details and once the bank has confirmed it, the bank will then ask for a security token pin number on the security token and the individual will then activate the token by entering their pin number into the token to retrieve the randomized set of pin numbers or security ticket and give it to the bank to complete the authentication process and in turn will allow the individual access to their bank account. These tokens provide quite a heightened level of security authentication as the security ticket is basically a form of authentication which verifies that the individual is the legitimate owner of the account and in turn gives access to the individual. This however has its drawbacks as the security token may be susceptible to damage or be misplaced or stolen as it is a physical token (Wikipedia, 2016).

2.2.3 – Biometric Based Authentication
"Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems.” (SearchSecurity, 2016).

Biometric systems offer a higher degree of security than other systems used for authentication such as knowledge based systems, this is due to the fact that biometric systems use the user’s biometric systems which are unique to
themselves only compared to knowledge based systems which use passwords or tokens which can be easily hacked into given the right tools and software. Traditional passwords are also characterised by long and alternated sequence of numbers or text and thus may be harder to remember for some people whereas tokens on the other hand are quite easy to misplace or have it stolen by anyone. Regardless of authentication type, passwords and tokens are able to be shared by anyone and thus there is no way of authenticating that the user is actually the real authorised user or some other random unauthorised user hence it is not that quite secure. Since biometric characteristics are not able to be shared among others, this basically eliminates the threat of unauthorised users accessing the system at any time.

Homes are at constant threat of intrusion and current security systems for homes use pin numbers and passwords, some even use remote security linked to their homeowner’s smartphone or tablet. This may cause an alarming problem for home owners as these systems have their own flaws, for example the knowledge based security system that uses pin numbers or passwords can easily be hacked or accessed by anyone who has somehow figured out or shared the systems pin number or password. And remote security systems usually use Wi-Fi and networks and without proper protection this network would be easily accessible to hackers. This problem can be easily eliminated by the use of biometric security systems as biometric properties are unique and cannot be shared by others.

The research which will be conducted will allow the user to investigate and identify the viable options for implementing biometric security systems for home based systems.

2.3 – Advantages and Disadvantages of Biometric systems

Traditional methods of authentication are usually the most widely used form of authentication method that is used and the most frequently used ones are passwords and pins. Their usage typically involves controlling access to a building or a room, securing access to computers, networks and in some other higher security applications, handheld security tokens such as key fobs or USB tokens and smart cards are also implemented in order to increase the strength of the encryption. Because these methods are usually associated with problems with suitability and reliability, these authentication methods have been questioned quite a lot especially in this modern world with modern applications of these systems and biometrics usually offer more of a benefit compared to these more traditional authentication systems.

2.3.1 – Increased Security

Biometric recognition systems are able to provide a higher degree of security compared to traditional forms of security authentication methods. Biometrics usually needs to have the physical presence of the authorised individual in
order to gain access and this means that only the authorized person has access to the location, account or device. The most common problem with traditional methods of authentication is that the efforts made by people to manage several different passwords has resulted in a large number of these people in choosing quite easy and or general words as password and also a considerable amount of people also writing them down in conspicuous places at times. This means that this vulnerability will lead to their passwords to be easily guessed and compromised. Security tokens on the other hand are physical security devices and these take the form of little key fobs or USB tokens and these can be easily stolen and or misplaced. By using biometric system of authentication this eliminates the risk of having the biometric data being guessed or even stolen in the same manner as security tokens or passwords (Griaulebiometrics.com, 2016).

2.3.2 – Increased Convenience
“Traditionally, in many authentication environments, a user may have different tokens or passwords. In these cases, biometrics can be used to simplify the authentication process since the multiple passwords or tokens can be replaced by a single biometric character” (Griaulebiometrics.com, 2016). Because biometrics technologies are based on the individual’s own biometric characteristics, it eliminates the problem of forgetting passwords or lost security tokens. This means that the characteristics of the biometrics technologies offer much more convenience than other systems which are based on more traditional methods which is to keep possession of cards or remembering a set of several passwords to gain access. Biometrics greatly simplifies the whole process that is involved in authentication and in turn also reduces the burden on the user of the system as well.

2.3.3 – Increased Accountability
Traditional methods of authentication can be shared and this means that there is an increase in the possibility of unaccountable access even though it might be authorised. Organisations for example share common passwords among higher level administrators for the purpose of facilitating the system administration. Because there is no way to figure out who at a particular point in time is using the shared password or token, accountability of any action is greatly reduced and the user of the shared password may not be authorised and sharing makes it even harder to verify and thus means that the security of the system is also reduced (Griaulebiometrics.com, 2016). By deploying biometrics to secure access to computers and other facilities eliminates the occurrence such as buddy punching and therefore provides a greater level of certainty as to who accessed what computer at what point in time.
2.3.4 – Increased Cost

Because there are many types of biometric technologies widely available for use, these biometric technologies need the use of quite a few different devices that have a variety of costs to them. Yes these biometric systems may be much more secure than the traditional methods of authentication but with that also comes the disadvantage of cost, most of these biometric systems need extra input devices in order for the system to work properly and efficiently and most of these devices are mainly scanners that range from simple fingerprint scanners to more complex and much more expensive iris scanners. Compared to traditional methods of authentication, there is no need for any other scanner as it only needs a small keyboard to input the password whereas a biometric system will need a biometric scanner and related recognition software to be installed which may cost more to be licenced and also a database system may also need to be purposely built to handle the load at which the facial recognition software will store templates of data for comparison purposes (Biometrics.pbworks.com, 2016).

2.4 – Implementation of biometrics into homes

Most people have simple forms of home security systems which are mostly simple keys and locks. While this has been the most secure way to lock up the house doors, it has its own flaws as well. One of which is that as the key is designed to fit into a specific lock with specific grooves in them, repeated use of the lock and key may cause the key to start losing its pattern and in turn will not allow the key to turn the lock giving the owner access to their home. Another disadvantage is that keys as a physical item, can be somehow misplaced and lost at any time and in some cases the keys might be stolen which means that anyone who is not the authorised individual may be able to access the house with the stolen key and in turn may cause harm.

“Security systems can actually become less complex if they incorporate fingerprint biometrics. There is a common belief that if biometrics are incorporated into your home security system, it will become more sophisticated and therefore more expensive. This is in fact a myth” (Mayhew, S. 2012).

Implementing biometrics into home security is not as costly as it seems, homeowners and small businesses are able to affordably use biometrics to secure their properties from intruders and theft and the most frequently used form of biometrics which is inexpensive and convenient is the use of fingerprint technology to secure door locks for homes and small businesses. These fingerprint biometric locks only need to have a thumb sized scanner somewhere on the handle which makes it look simple and other locks may also combine fingerprint scanning features and keypads for added security. By having these kind of biometric locks on doors, only allowed members of
the family or authorised individuals may enter the home which makes it very secure.

Another way biometrics may be useful for homes are by using biometric computer locks for home based computer systems such as desktop computers. By implementing computer locks via by using fingerprint scanners, the computer remains locked only until the individual scans their fingerprint into the fingerprint scanner. There is no need to remember any passwords or click on all the right boxes in order to start up the desktop, just a quick scan of the finger and the system starts up automatically (Digital Landing, 2012). Laptop computers often have fingerprint scanners built in, but for desktop computers, the fingerprint scanners have to be bought separately and these come in a variety of choices whether the scanners come on built in onto the mouse, the keyboards or as a standalone unit.

3.0 – Research Methodology and Findings

3.1 – Method of Research
3.1.1 – Research Philosophy
The methods of research which will be used for this research will be using a form of interpretive research method or also known as Interpretivism. Interpretivism or interpretivist involves the researcher to interpret elements of the study and thus it integrating human interest into the study accordingly, “interpretive researchers assume that access to reality (given or socially constructed) is only through social constructions such as language, consciousness, shared meanings, and instruments” (Myers, 2008, p.38).

Interpretivism is “associated with the philosophical position of idealism, and is used to group together diverse approaches, including social constructionism, phenomenology and hermeneutics; approaches that reject the objectivist view that meaning resides within the world independently of consciousness” (Collins, 2010, p.38). Interpretivism studies usually focus on meaning and may employ multiple methods in order to reflect different aspects of the issue.

3.1.2 – Research Strategy
The research strategy which will be used in this research will be by using an inductive approach to the research. This means that the researcher will begin the research by firstly collecting the primary data and secondary data that is relevant to the topic of interest. Once the substantial data is collected, the researcher will then observe and look for patterns within the data and develop a theory which could explain those patterns of data.

Inductive approach of research basically starts with the observations and theories which are formulated towards the end of the research and as a result
of observations (Goddard and Melville, 2004). Inductive research “involves the search for pattern from observation and the development of explanations – theories – for those patterns through series of hypotheses” (Bernard, 2011, p.7). In other words, no theories would apply in inductive studies at the beginning of the research and the researcher is free in terms of altering the direction for the study after the research process had commenced.

3.1.3 – Sampling Technique

“Convenience sampling, as the name implies is a specific type of non-probability sampling method that relies on data collection from population members who are conveniently available to participate in study.” (Research Methodology, 2016).

For collecting primary data for analysis, a convenience sampling method is used as this form of sampling method is the most simple to implement, this sampling method relies on data collection from population members who are conveniently available to the researcher to participate in the study. Convenience sampling method basically involves getting participants wherever the researcher can find them and typically wherever is convenient. With this research topic being related to electronic biometric systems, there may be quite a large sample from online sources such as computing forums and websites thus spreading the questionnaire online would be a good way to collect primary data for the research topic.

This research will be done by the use of Google forms to create the questionnaire for the data collection. Google form allows creation of forms in a simple way and will provide a link to be shared online via any forms of social media which could reach a very audience locally or internationally. The proposed number of responses which are required for this research ideally would be around 60 participants as a minimum; this will allow the researcher to gain a good overall knowledge of what the sample thinks about the topic of study.

To protect the confidentiality of the participants of this study, all the data from the participants which will be received by the researcher will be kept safe and secure in a password protected computer system. Firewalls will also be implemented to prevent any breach of information via online methods. The anonymity of the participants will also be kept confidential; Participants will remain anonymous and all the data which is received by the participants will not be traceable back to specific people.

Within the 42 day period of data gathering, the amount of responses gained from the public was a total of 104 responses out of the proposed 60 responses which is 44 more responses than expected, but this is good as more primary data would mean that the research would have better accuracy on what the
public thinks about the study. These responses come from a mix of random sample of people including those samples from close friends and families. Most of the respondents had answered all the questions and only a few invalid questions were received so the data which was useful for this study was about 101 responses in total. The data gathering was mostly done by completing questionnaires online as it is the most convenient way for the respondents to answer the questions at their own time and pace. The aim of the questionnaires was to find out the trend of how aware the public sample was about biometric security systems and also to find out how percentage of the sample will be willing to implement a biometric security system for home use or for their devices. The first few questions set in the questionnaires is intended to find out what percentage of the sample have electronic devices at home and also to find out how many devices if they have any at home and do they have a security system for their home or not. The study will then further ask the sample about their thoughts about will they think about or will they actually implement a biometrically secure way of authentication for their home devices or home security system.

3.2 – Sample study on the security of their devices

The results which that was gathered from the first question of the study shows that about 86.1% of the respondents have more than 3 electronic devices at home, about 4% have about 3 devices, 5% have about 2 devices and a further 5% have about only 1 electronic device at home, this shows that majority of the study has access to electronic devices which means there is a possibility that this majority of respondents may already are aware of biometrics and may already be implementing it on a few of their devices.
Further studies show that almost 98% of the respondents use these electronic devices on a daily basis, this is quite common occurrence as technology nowadays has become very convenient and mainstream, it also allows people to be more efficient and productive in their daily work routines. The other 2% of respondents use their devices on a weekly and monthly basis which means that these 2% of respondents probably are not that very computer literate as most likely they only have 1 electronic device available to them.

With rapidly advancing technologies widely available for the public, it is quite common to see someone on their phones or laptops 24/7 nowadays. These devices usually have simple ways of locking themselves to secure access. For example a simple smartphone which has a touch screen interface such as the apple IPhone, the user would simply have to swipe their finger across the screen of the smartphone which will bring the user to a keypad screen in which the phone will then require the user to enter a pin number for the user to gain access to the phone. This form of security measure is quite secure for the normal everyday user but for more advanced users, this form of security measure is not enough as anyone else can look over a person’s shoulder and see which numbers are keyed into the screen lock and in turn will allow that person to have unauthorised access to the smartphone.

Laptops and Desktops however have simple passwords which allow the users to log in and use the computers. These PCs give access by firstly asking the user a password on start-up, the user will then type in the password and the computer will then give full access of the computer towards the user.
The same goes with other users if there are multiple users of the computer for example a household of 4 people may have a shared desktop computer between all the members of the household, an Administrator (primary user), 3 other member accounts (secondary users) and 1 guest account for whenever there are guests available in the household. These user profiles would have different passwords apart from the guest profile which would be an open profile but will not have many features available to be used. Having passwords as security passes for computers is quite secure for normal computer users but again for advanced users it is not quite secure because passwords can be easily hacked given the right tools and knowledge.

The study conducted also asked respondents what kind of security system they had on their devices and the results that were gained showed that a large percentage of the respondents use knowledge based authentication to protect their devices with a majority of 73.7% of the sample. This meant that the respondents use mostly password and pin number based security authentications for their computers, phones and home security systems. A small 11.1% of the sample had said that they are using a token based authentication system which meant they would most likely have an extra key fob or USB sized security token to be carried around all the time, this token based authentication would usually be tied with bank accounts and some home security applications. The other 15.2% of the sample used biometric based authentication for their devices and this shows that of all the 101 respondents, 15% of these respondents are quite well aware of biometric authentication systems.

One reason for this is that some device manufacturers nowadays have started implementing biometric authentication methods into their devices straight
from the box. Apple for example implemented biometric fingerprint scanners within the home button of their iPhone and HTC has also recently started to implement fingerprint scanners in their latest flagship model phone the HTC 10 which was just announced on the 12th April 2016, this is shown on the devices as a small scanner on the lower front of the device which also acts as a home button when the scanner is not in use. Other manufacturers which have also implemented biometric authentication technologies to their devices include laptop manufacturers like HP, acer and Sony.

Further studies of the sample have also found out that overall with these secure authentication systems implemented on their devices, the percentage of the sample which finds these authentication methods are secure enough for their devices are split quite evenly with 47.5% saying that it is secure enough for their own personal use but also about 52.5% of the sample believe that these security measures are not quite secure enough for their own personal use.

With a majority of the sample using knowledge based authentication systems, many of them believe that their systems are not quite secure enough is that some of the sample think that the main reason is that hackers are quite resourceful and are able to hack into an individual’s passwords. Some of the respondents have also commented that their computers were somehow hacked a couple of times as well. The other half percentage of the sample thinks that it is quite secure and this is because they may have biometrics fingerprint scanner on their devices as a deterrent from any possible unauthorised usage or they may just think that their password is quite secure enough and is not bothered about looking for other ways of improving the security of their devices.
With the use of knowledge based form of authentication methods, users are usually asked to put in a password or pin number for authentication and how users make up a password or pin number will basically be the deciding factor on how hard or easy the password will be hacked or not.

The graph above shows how the sample composes their passwords. Most passwords are usually restricted as in for example some websites that allow users to log in require passwords during their registration which must be 6 characters long or must have a mix or numbers or letters, this means that users will have to make up a password which fits the recommended criteria which will allow the user to register with that website. In the study, it has been found out that a large percentage of the sample use a mix of letters and numbers as passwords with about 44.6% of the total sample. Another percentage of 23.8% of the sample prefers to use a mix of letters and symbols, while this is much harder to guess for unauthorised people to gain access, it may be much easier to forget these kinds of passwords as they use symbols. 5.9% of the sample makes up passwords which are about 4-5 characters long, while shorter passwords are easier to remember, it may be much easier to guess what the password is. Another 23.8% make up passwords which are 7-8 characters long and another small 2% make up passwords which are more than 10 characters long. While longer passwords make it harder for unauthorised people to gain access, it may be even harder to remember due to the long password.

When the sample was asked whether they have had any of their devices being hacked into through online or of by someone that they know of, 21.8% had said yes while the rest of the 78.2% said that they have never had their devices being hacked via online means or by someone that they know of, the
sample was then asked what would they have done to ensure that the hacking incident will never happen again and most of the sample had answered to just simply change their passwords from a simple one to a much more harder password to guess. This clearly shows that a large percentage of these samples are using knowledge based system of authentication.

3.3 – Sample study on home security systems.
When asked whether the sample owns a security system for their home or not, a large percentage of 81.2% of the sample had answered no and this meant that they would most likely be using a simple lock and key for their home security, the other 18.8% answered yes to having an electronic home security system which meant that there may be a demand for home security systems within the market that use a biometric form of authentication method and when the sample which had said yes to having an electronic home security system was asked what kind of security system they had used whether it is a knowledge based, token based or a biometrically based system, only a small percentage of the sample had said that they were currently using biometric authentication systems and it consists of a small 18.4% of the sample which had said yes to having a home security system. A large percentage of the sample uses knowledge based and token based forms of authentication methods such as using pin numbers and passwords in combination with security tokens.

![Security authentication used by sample](image)

When the sample were asked about how secure their home security system is in terms of the authentication methods about 54.7% of the sample were unsure about how secure their authentication methods were and about 19.8% of the sample had said that they think their authentication methods were not
that secure enough while the rest of the 25.6% had said that their authentication methods were secure enough by their own standards.

3.4 – Awareness of available biometrics

As there are multiple types of biometrics that are available, the sample was asked how many of them know any biometric systems before this study was conducted and of the 101 responses that was received, 95 of the sample responded to knowing a few biometric authentication methods. Assuming that the other 8 respondents which did not respond to this question maybe have never heard of biometric systems or does not know it exists and is available for public use, this shows that the sample is pretty much aware of the availability of these biometric systems.

The graph above shows the composition of known biometric systems that the public sample may know of, the sample was asked what type of biometrics have they heard about and how do they find out about these systems, the most common form of biometrics which the public sample knows of very much is fingerprint biometrics with 92 responses, this is due to the fact that most of the sample had said that they currently have a few devices which implement fingerprint security on them such as their own smartphones as some phones come standard with fingerprint scanners. Other respondents have said that mostly the internet is the main source that they have heard about these biometric systems. 55 responses were received for voice pattern recognition, 53 responses for retina scanning, 39 responses for iris recognition and another 2 responses for other forms of biometrics which the respondents have answered palm scanning or hand print recognition. Another most likely source of information on where the public sample had found out about these systems is from movies, TV shows and advertisements on TV. Most movies
and TV shows nowadays implement scenes which include biometric locking systems for cars, doors and even suitcases sometimes and this may be fictional to some but there are systems out there that are implemented by private companies and even government facilities.

Social media has also helped with the awareness of biometric systems, quite a few of the respondents have also said that while they were browsing through social media such as twitter, Facebook and YouTube, the respondents have seen some posts and articles about these biometric systems and the types of biometrics that are available which were reposted on the social media sites by their own friends, families and even sometimes from the own companies that produce these systems as well. This is due to the fact that nowadays companies have their own social media presence such as in Facebook, twitter and YouTube in order to spread their brand awareness locally and internationally as the social media sites and internet is the best way to spread brand awareness as it reaches world-wide audiences with ease.

As the study had found out how much aware the public sample is about the biometric systems, the study had also continued to ask the sample what is stopping them from implementing a biometric system to their devices or home security system, is it because they had a strict budget?, is it because that they do not have much knowledge about the system? Or were they just not bothered to implement a new system? The responses what were received that a large percentage of the sample composed of 39.2% had said that they had a strict budget. Biometric systems cost a lot to be implemented as they need scanners to scan the biometrics of a person, these scanners also need to have recognition software built in them in order to identify the person using it and this may bring the price up as software would need proper licensing. A database program is also needed for the system as it is used to store the biometric templates to be used for comparison of data between the person and the data within the system. All this means that when implementing a biometric system for home use, it can be quite costly and this is most likely one of the main reasons that the respondents do not want to implement a biometric system into their home security system or devices.

The other reason why the respondents do not want to implement the system is because they do not have much knowledge of biometrics to want to be able to implement the system and this composes 23.7% of the sample. This maybe because they think it is a very complex system and needs quite a good knowledge of the system in order to use it effectively. The respondents might also think that the disadvantages of having a biometric system outweigh the advantages of having such system over the traditional knowledge based systems. Yes a small amount of knowledge is needed to be able to use the biometric system to its full potential but it is not that complex as a user that has already logged their data into the system can simply just put their
fingerprint onto the scanner and the system will give access whether the user is an authorised user or an unauthorised user. Initial start-up of the system may require some knowledge for storing the user’s data into the database but other than that, that is the only thing which the user needs to know is to input their biometric data into the system and let the system do it for them.

Other respondents have also responded in saying that they are not bothered to implement a new system and this comprises of 26.8% of the sample; this is due to the fact that they may think that their current way of securing access is quite secure enough with traditional knowledge based authentication methods such as using passwords and pin numbers. Some are also not bothered because they may be afraid that implementing a new system may in-fact not benefit them as their current system is working well enough.

A small percentage of 10.3% of the sample had also given other reasons why they would not want to implement a biometric system over the traditional knowledge based system, one of their reasons being that of the availability of the system and whether it is economically available within the country or not. For example developed countries may have the technology and resources to develop a cost-effective biometric authentication system but other countries such as the developing countries around the world may not have such technology and resource available to them and this may mean that these systems would have to be imported and this may be quite costly and have a huge impact on the cost of the biometric systems.

Another reason that a few of the respondents have given is that for devices and home systems such as desktops and laptops, the respondent usually does not have so much vital information for such forms of authentication and they do not see it as a necessary requirement for their own security and convenience. Maintenance and availability of repairing services may also be one of the reasons why the respondents do not want to implement a new system; the availability of a new electronic authentication system may need to be maintained well in order for it to work efficiently and effectively.

This may not be the case for portable devices such as smartphones or tablets which have biometrics built into them, one may simply just bring the device into the store and have it repaired if the biometric scanner is damaged, for example the Apple iPhone has biometric fingerprint scanners built into the home button of the phone, whenever someone has a problem with the scanner, one can just simply bring it to an apple store and have the specialists repair the damaged part of the phone. In terms of maintenance, portable devices are usually built to be able to endure tough daily use and maintenance wise all the user needs to do is to keep the device’s biometric scanner clean and the device itself safe from fall damage and any other possible risks that may damage the device.
In the case for desktops and laptops, which may have external biometric scanners plugged in, it may be a bit more costly to be maintained, if the scanner part of the system is to be damaged, the user will have to take into account the availability of shops which have the technology and skills which are able to repair the scanner and this may also cost a lot more to repair than to buy a new scanner.

In terms of home security systems, biometrics are usually used on doors as locking mechanisms, if the biometric system is to be compromised or damaged, the user will have to call the company that provided the user with the system and have a technician look into the problem which may put a strain on the user's budget. Another problem this may cause for the user is that because the user uses this biometric system for their home security system, the house may be vulnerable to intrusion if the system is damaged and this is quite a huge risk for the user.

With the availability of different types of biometrics, a user who wants to implement a biometric system is able to choose which one the user prefers whether it is fingerprint based, iris based, retina based, voice based or face pattern based form of authentication methods. The sample was asked which type of biometrics they would prefer if they were to implement it into their current daily lives and the results are shown below.

![Biometric Preferences Chart]

A large 65.6% of the sample had said that they would want to use fingerprint based form of authentication and the reason being that the respondents had said that it is much easier for them to use fingerprints for identification as one user will only have to scan their fingerprints onto the fingerprint scanner in order to give the user access. Fingerprint based forms of authentication is
also the cheapest among all other forms of biometric authentication methods. Other biometric authentication methods need to scan more than ridge patterns on fingerprints hence may cost a lot more to develop an algorithm for that.

A total of 19.8% of the sample would prefer the use of biometrics that is based on the eyes of the user. These are usually categorised into 2 forms of recognition systems which is the iris recognition and retina recognition systems. 11.5% of the respondents have preferred iris based recognition methods and the other 8.3% prefer the use of retina based recognition methods, this is mostly because that it is quite a very secure method of authentication, for example if a user is asleep, someone can easily access their fingerprint based biometric device by placing the user’s fingers on to the device while they are sleeping, but for systems based on the iris and retina, the person would need to scan their eyes in order to gain access to the device.

Another form of biometrics that consists of a small 3.1% which the public sample had preferred to use is voice pattern recognition methods, although this is unique in its own way as it records voice patterns in someone’s speech patterns, it may be too complex to implement as a biometric system for home security systems or devices. One reason of which is background noise may interfere during recording of the user’s speech pattern, for example if someone lived nearby a highway or an airport, the background sounds of aircraft flying overhead and cars passing by may hinder the effectiveness of the system when the user is using it. The cost of a system with voice recognition system may be quite cheaper as instead of a scanner, a microphone is used to record the voice pattern of the user but the software which is needed for voice recognition may be harder to develop and implement which means that the overall cost of the system may be as similarly expensive as systems that use scanners but not as expensive as them.

Face pattern recognition systems comprises of 7.3% of the preferred systems that the sample would want to implement. Face pattern recognition systems are the most complex form recognition systems, one of the main reasons is that the system uses a camera to take a picture of the user and the system then converts that image with an algorithm to convert it into a digital pattern data to be stored in the system’s database. This maybe the most expensive form of biometrics that is available to be implemented but the main drawback is that someone which looks like the user of the system may be able to access the system as well, twins for example have the same facial structure and the system will have way of distinguishing which of the twins is the real authorised user and will in turn accept both users as the authorised user.
Other forms of biometrics that were mentioned by the respondents include biometrics which is palm scanning or hand print pattern recognition systems. This system is similar to fingerprint forms of biometric authentication systems as the user will need to scan the palm of their hands on to the scanner for the system to record the user’s hand print. The system works in the same way as the fingerprint scanner but instead uses the user’s palm print instead. Being a system which records handprints and the positioning of the palm onto the scanner may be even more convenient than fingerprint scanning systems, this system is usually quite larger as the scanner needs to scan a whole hand print rather than smaller fingerprint scanners and thus the cost of implementing this system may be significantly more expensive than smaller button sized fingerprint scanner systems. Having a larger scan area also means that the system is able to get a better scan profile of the palm print and is able to scan the palm in a clearer and faster way.

3.5 – Sample’s thoughts on implementation of biometric systems

Further study into how much the sample agrees or disagrees to certain statements which were given to them have shown that the sample is much more likely to implement a biometric system for security measures over traditional knowledge and token based systems.

The first statement which was given to the sample was are they likely to use a biometric system as a security measure for their home, the results from this statement showed that a large number of the responses of 42 of the sample are neutral about this statement which meant that they neither agree or disagree about this statement. Even with a majority of the responses had answered that they were neutral about it, more responses were received on the agreed side of the scale which is a total of 36 responses split up between
14 strongly agreeing to the statement and about 22 casually agreeing on the statement which meant that the sample would most likely would want to implement a biometric form of security system for their home. The respondents which disagreed to this statement are equally split with 11 disagreeing and another 11 strongly disagreeing towards the statement. This maybe because they are more comfortable with using a currently knowledge based form of security or that they may be not bothered to implement a new system for their home security system.

The second statement which was given to the sample is; are they more likely to use a biometric security system to secure their computer system or their portable devices.

![Bar chart showing the distribution of responses](image)

Is the sample more likely to use a biometric system to secure their computer system or portable devices?

The results that were received were very much positive as most of the sample had agreed and strongly agreed with the statement, a total of 46 respondents both equally divided with strongly agreed and agreed responses, 30 of the respondents had answered they were neutral about the statement and about 25 respondents had disagreed about the statement.

This meant that majority of the sample are willing to implement biometric systems to be used in the protection of their computer systems and the devices which they are using on a daily basis. This may also be due to the fact that the devices that they are using currently are already using biometric authentication such as Apple’s IPhone which uses biometric fingerprint locks to secure access to the smartphones.

The third statement which was asked was what preferences would the sample want to use; is the sample likely to prefer using a biometric system rather
than to use the traditional forms of authentication methods such as knowledge based and token based authentication methods in order to protect their sensitive files and information?

The results had showed that again, a large majority of the sample had also agreed to this statement, a total of 49 responses in agreement with 24 respondents strongly agreeing to the statement, 25 respondents casually agreeing to the statement and around 31 responses were neutral about the statement. Only a few of the respondents were in disagreement with a total of 21 responses, 10 casually disagreeing and around 11 responses strongly disagreeing about the statement.

The last statement which was asked of the sample was that biometric systems offer more secure forms of security compared to other systems such as knowledge based or token based systems.
The results from that statement were also similar to the previous statement with a majority of a total of 49 responses in agreement split up into 22 strongly agreeing to the statement and about 27 casually agreeing to the statement. 34 respondents were neutral about the statement, and a total of 17 respondents were in disagreement with the statement which is split up between 7 responses casually disagreeing and around 10 respondents strongly disagreeing to the statement.

The results of this last statement basically shows what the sample thinks about how secure the biometric systems are compared to traditional knowledge based systems, and the results have shown that majority of the sample knows how secure the system will be if implemented with a biometric system compared to the knowledge based authentication methods.

Overall the results of these statements that were asked to the sample have found out that a large majority of the sample had agreed to want to implement a biometric form of authentication for their computers and devices but not that much on home security systems.
4 – Conclusion
In conclusion, the main aim for this research project is to investigate the possibility of implementing biometric security systems on to home based systems such as devices, desktop PCs or home security systems and are biometric systems able to be implemented into home systems? Yes, Biometric systems are very much possible to be implemented to be used in home systems but only to a certain extent.

The main reason being that there are biometric systems for home devices available out there but not as much as every household has a biometrically secure home security system or biometrically secured desktop computer.

Based on the findings from the research conducted, there is quite a demand for biometrically secure home systems for the public.

The objectives of the research paper have been also been met which is firstly to identify the security systems which are available to be used for home based security systems or computing devices such as desktop computers for home use. This is achieved via the means of secondary research gathering from online sources, it has been found that there are 3 major forms of security authentication systems which are knowledge based, token based and biometric based authentication systems.

The second objective of the research project was to investigate the problems with using a current knowledge based systems in order to access control for home based security and computing systems and this was achieved by primary data collection and also a mix of secondary data gathering. It has been found out that knowledge based systems are quite easily hackable by anyone given the right knowledge of the system and the right knowledge of the authorised user as the knowledge based system uses authentication method based on the authorised user's knowledge.

The third and last objective is to identify whether it is possible or not to integrate biometrics into home based security and computing systems and this was also achieved by the help of secondary data gathering. There are systems which are available off the market which are able to convert knowledge based security authentication systems into biometric authentication systems.

Overall implementing a biometric system of authentication for home use for home systems and home security is possible but it may be quite costly to implement. It all depends on whether the user is willing to sacrifice their budget enough in order to gain a more secure way of protecting their data and or protecting themselves from any unwanted intrusion.

Biometric systems in short, are a quite complex and expensive form security authentication system, but it is also the most secure form of
security authentication system that is available out there. The complexity and security of the system is one of the main reasons that biometric security authentication methods are used in government facilities and some private companies in dealing with private data.

Some portable devices such as smartphones and tablets have already had biometrics built into them and this allows users to biometrically secure some part of their private information on their devices but only to some extent. Devices are still susceptible to online hacking problems which are something biometrics is not able to prevent.

Other more bulkier home devices such as desktop computers do not come built in with biometric systems as standard but there are external systems that are available in the market which are “plug and play” devices which means that the biometric security system needs only to be plugged in and installed in order for the computer to be able to implement a biometric security system.

In terms of home security, it may be better to maintain a more traditional token or knowledge based form of authentication. The reason being that usually a household would usually consist of a few occupants within the home and it would be much easier to share 1 password or pin number between all the occupants rather than using each person’s biometric profile. It costs way lesser than a biometrically secure system and it is more convenient for the whole household to use.
References


t
techologies.


Appendices

Appendix A – Ethics Approval Form
CARDIFF METROPOLITAN UNIVERSITY
APPLICATION FOR ETHICS APPROVAL

When undertaking a research or enterprise project, Cardiff Met staff and students are obliged to complete this form in order that the ethics implications of that project may be considered.

If the project requires ethics approval from an external agency (e.g., NHS), you will not need to seek additional ethics approval from Cardiff Met. You should however complete Part One of this form and attach a copy of your ethics letter(s) of approval in order that your School has a record of the project.

The document Ethics application guidance notes will help you complete this form. It is available from the Cardiff Met website. The School or Unit in which you are based may also have produced some guidance documents, please consult your supervisor or School Ethics Coordinator.

Once you have completed the form, sign the declaration and forward to the appropriate person(s) in your School or Unit.

PLEASE NOTE:
Participant recruitment or data collection MUST NOT commence until ethics approval has been obtained.

PART ONE

<table>
<thead>
<tr>
<th>Name of applicant:</th>
<th>Rafie Rahim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor (if student project):</td>
<td>Dr.Hilary Berger</td>
</tr>
<tr>
<td>School / Unit:</td>
<td>CSM</td>
</tr>
<tr>
<td>Student number (if applicable):</td>
<td>ST20054574</td>
</tr>
<tr>
<td>Programme enrolled on (if applicable):</td>
<td>BSc(Hons) Business Information Systems</td>
</tr>
<tr>
<td>Project Title:</td>
<td>Biometric Security systems for home based systems</td>
</tr>
<tr>
<td>Expected start date of data collection:</td>
<td>25th January 2016</td>
</tr>
<tr>
<td>Approximate duration of data collection:</td>
<td>60 days</td>
</tr>
<tr>
<td>Funding Body (if applicable):</td>
<td>N/A</td>
</tr>
<tr>
<td>Other researcher(s) working on the project:</td>
<td>None</td>
</tr>
<tr>
<td>Will the study involve NHS patients or staff?:</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve taking samples of human origin from participants?:</td>
<td>No</td>
</tr>
</tbody>
</table>

Does your project fall entirely within one of the following categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper based, involving only documents in the public domain</td>
<td>No</td>
</tr>
<tr>
<td>Laboratory based, not involving human participants or human tissue samples</td>
<td>No</td>
</tr>
<tr>
<td>Practice based not involving human participants (eg curatorial, practice audit)</td>
<td>No</td>
</tr>
<tr>
<td>Compulsory projects in professional practice (eg Initial Teacher Education)</td>
<td>No</td>
</tr>
<tr>
<td>A project for which external approval has</td>
<td>No</td>
</tr>
</tbody>
</table>
been obtained (e.g., NHS)
If you have answered YES to any of these questions, expand on your answer in the non-technical summary. No further information regarding your project is required.
If you have answered NO to all of these questions, you must complete Part 2 of this form

In no more than 150 words, give a non-technical summary of the project
The research will be gathering information from the public in an anonymous way in order to protect their identities and keep their confidentiality. It will be focused on investigating the plausibility of implementing a biometric system on to current home based systems which use traditional methods of authentication such as passwords for computers and laptops, and pin numbers for home security systems. This research will aim to investigate the advantages and disadvantages of the more traditional method of authentication compared to the biometrics method of authentication and will investigate how plausible it is to implement the biometric system as a stand alone system for authentication or be integrated with the traditional method of authentication for more secure authentication purposes. The research will also be gathering information from a sample population from the general public that includes samples that are computer literate via convenience sampling.

DECLARATION:
I confirm that this project conforms with the Cardiff Met Research Governance Framework

I confirm that I will abide by the Cardiff Met requirements regarding confidentiality and anonymity when conducting this project.

STUDENTS: I confirm that I will not disseminate any material produced as a result of this project without the prior approval of my supervisor.

Signature of the applicant: ___________________________ Date: 26/01/16

FOR STUDENT PROJECTS ONLY

Name of supervisor: ___________________________ Date: 26/01/16

Signature of supervisor: ___________________________

Research Ethics Committee use only

Decision reached: Project approved ✓
                    Project approved in principle  
                    Decision deferred    
                    Project not approved  
                    Project rejected    

Application for ethics approval v4 March 2015
CARDIFF METROPOLITAN UNIVERSITY
APPLICATION FOR ETHICS APPROVAL

<table>
<thead>
<tr>
<th>Project reference number: 2015D0572</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Dr. Hilary Berger</td>
</tr>
<tr>
<td>Date: 20/01/2016</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Signature:</td>
</tr>
<tr>
<td>Details of any conditions upon which approval is dependant: N/A</td>
</tr>
</tbody>
</table>

**PART TWO**

**A RESEARCH DESIGN**

<table>
<thead>
<tr>
<th>A1 Will you be using an approved protocol in your project?</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 If yes, please state the name and code of the approved protocol to be used¹</td>
<td>N/A</td>
</tr>
<tr>
<td>A3 Describe the research design to be used in your project</td>
<td>This dissertation will use both qualitative and quantitative data in order to gain valuable information about what the public thinks of a biometrically secure home based system such as their computers or the home's security system and also how much of the public would approve of the idea of having a biometrically secured system. Questionnaires and surveys will be used to collect primary data for the dissertation and will be developed from the analysis of current literature within the given domain. These questionnaires and surveys will be collected via convenience sampling from the public in a way which is anonymous to ensure that the participant cannot be specifically identified and to keep their confidentiality and their responses will be kept safe in a secure place during the research and will be destroyed after the research has been concluded. The questionnaires and surveys for data gathering will be distributed to a sample population through convenience sampling methods from online sources such as through social media such as facebook, twitter and other online computing forums such as CNET, FreePChelp, ComputerForum.com and TechGuy.org in order to collect quantitative information about the research topic in question. The results of the data gathering will then be analysed using excel via thematic analysis to identify trends and patterns in the data collection in order to gain a descriptive information for discussion.</td>
</tr>
<tr>
<td>A4 Will the project involve deceptive or covert research?</td>
<td>No</td>
</tr>
<tr>
<td>A5 If yes, give a rationale for the use of deceptive or covert research</td>
<td>N/A</td>
</tr>
<tr>
<td>A6 Will the project have security sensitive implications?</td>
<td>No</td>
</tr>
<tr>
<td>A7 If yes, please explain what they are and the measures that are proposed to address them</td>
<td>N/A</td>
</tr>
</tbody>
</table>

¹ An Approved Protocol is one which has been approved by Cardiff Met to be used under supervision of designated members of staff; a list of approved protocols can be found on the Cardiff Met website here.
B PREVIOUS EXPERIENCE

B1 What previous experience of research involving human participants relevant to this project do you have?
None

B2 Student project only
What previous experience of research involving human participants relevant to this project does your supervisor have?
Dr. Hilary Berger has over 12 years experience of research involving human participants

C POTENTIAL RISKS

C1 What potential risks do you foresee?

1. Personal Information on the Questionnaires.
2. Risk of not meeting research deadlines.
3. A risk to the participants would be the confidentiality of the data they provide.
4. Personal information and data storage must be taken into account.

C2 How will you deal with the potential risks?

1. Completion of the questionnaire is taken as consent and will be stated at the beginning, the questionnaire will not contain any questions that may reveal the identity of the contributor and will ensure the contributor’s anonymity throughout, this will be stated at the beginning of the questionnaires.
2. Every effort will be made to complete the research phases in accordance with the anticipated research deadlines.
3. Questionnaires will have no trace back to the contributor and access to the data will be restricted to contributor and supervisor.
4. All data will be held on a secure password protected external harddrive and paper copies will be kept in a locked cupboard.

When submitting your application you MUST attach a copy of the following:
• All information sheets
• Consent/assent form(s)
An exemplar information sheet and participant consent form are available from the Research section of the Cardiff Met website.
Appendix B – Sample of Participant Information Sheet
PARTICIPANT INFORMATION SHEET

Biometric Security system for home based systems

Project summary

The purpose of this research project is to investigate the possibility of implementing biometric security systems to home based systems such as desktop PCs or home security systems. Your participation will enable the collection of data which will form part of a study being undertaken at Cardiff Metropolitan University.

Why have you been asked to participate?

You have been asked to participate because you fit the profile of the population being studied; that is you are between the ages of 18 and 30 and may possess the knowledge and interest of such known systems. During the questionnaire survey, the questions which will be asked will be based on mostly questions relating on computing systems and how the way you interact with the systems in a daily basis. Your participation is entirely voluntary and you may withdraw at any time.

Project risks

The research involves the completion of a questionnaire which will be recorded for later analysis. We are not seeking to collect any sensitive data on you; this study is only concerned with investigation on whether it is possible or not to implement biometric security systems on home based systems and will not discuss any immoderate behaviours. We do not think that there are any significant risks associated with this study. However, if you do feel that any of the questions are inappropriate then you can stop at any time. Furthermore, you can change your mind and withdraw from the study at any time – we will completely respect your decision.

How we protect your privacy

All the information you provide will be held in confidence. We have taken careful steps to make sure that you cannot be directly identified from the questionnaire form; there is no information on these questionnaires that will identify you. Your personal details (e.g. signature on the consent form) and your questionnaire will be kept in secure locations by the research team. When we have finished the study and analysed all the information, all the documentation used to gather the data will be destroyed.

YOU WILL BE OFFERED A COPY OF THIS INFORMATION SHEET TO KEEP

If you require any further information about this project then please contact:

Rafie Rahim, ST20054574
Email: st20054574@outlook.cardiffmet.ac.uk
Supervisor: Dr. Hilary Berger
Supervisor’s Email: HBerger@cardiffmet.ac.uk
Appendix C – Sample of Participant Consent Form
PARTICIPANT CONSENT FORM

Investigating the possibility of implementing Biometric Security Systems for home based systems

Rafie Rahim – ST20054574

Participant to complete this section: Please initial each box.

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

3. I agree to take part in the above study.

_______________________________________   ___________________
Signature of Participant                          Date

______________________________  ___________________
Name of person taking consent                        Date

____________________________________
Signature of person taking consent
Appendix D – Participant Questionnaire Form
The aim of this questionnaire is to gather information on how much the public/focus group knows about security systems such as the traditional token/knowledge based security systems and the biometric security systems and how much the public/focus group would want to implement a biometric security system for home use.

The questionnaire will most likely take 10 to 15 minutes to complete. We greatly appreciate your effort by taking the time to fill out this questionnaire and all information that will be given to us in response will be treated confidentially.

Please circle the letters to the questions where appropriate

1. How many electronic devices or systems do you have at home?
   - a. 1
   - b. 2
   - c. 3
   - d. More than 3

2. How much do you use these devices or systems on a daily basis?
   - a. Once per day
   - b. Once per week
   - c. Once per month
   - d. Others: please specify

3. What kind of security measures do these devices have on them currently?
   - a. Knowledge based (using passwords)
   - b. Token based (using Security tokens that grant specialised pin numbers)
   - c. Biometrically (using fingerprints, voice recognition, retina scanners, etc.)
   - d. Others: please specify

4. Do you think it is secure enough or does it need more in terms of encryption?
   - a. Yes
   - b. No
   - If yes please specify why:
5. When using knowledge based method of securing your device or system, how long would your chosen password have to be for it to be secure by your standards?
   a. 4-5 characters long
   b. 7-8 characters long
   c. 10+ characters long
   d. A mix of letters and numbers
   e. A mix of letters and symbols

6. Have you ever had any trouble with forgetting passwords for these devices or systems?
   a. Yes
   b. No

7. If so, how likely are you to forget a long password?

8. How many times are you usually required to reset your device or system password?
   a. Once in a week
   b. Once in a month
   c. Once in 3 months
   d. Once in a year
   e. Others: please specify

9. Does your home have a security system?
   a. Yes
   b. No

10. If so, what kind of security measure does it use?
    a. Token based system (using Security tokens that grant specialised pin numbers)
    b. Knowledge based system (using passwords)
    c. Biometric based system (using fingerprints, voice recognition, retina scanners)

11. Is it secure enough for your privacy needs in terms of encryption?
    a. Yes
    b. No
    c. Not sure

    Please state why you chose the above answer:

12. What do you think would help improve the security encryption of your home security system?
13. If so do you know how to effectively use it to its full potential?
   a. Yes
   b. No

   If yes, please specify further

14. Is it well maintained? If so how often is it maintained?

15. Have you ever had your devices or systems being hacked into online or by someone you know of?
   a. Yes
   b. No

   If yes, what have you done to ensure that it will never happen again or will do?

16. Are you aware of the availability of these biometric systems below? Circle which one you know of.
   a. Finger print biometrics
   b. Iris recognition
   c. Retina scanner
   d. Voice pattern recognition
   e. Face recognition
   f. Others: please specify

17. How did you find out about these systems?

18. What is stopping you from not moving into a biometric system from other traditional forms of security systems?
   a. Strict budget
   b. Not much knowledge of the system
   c. Not bothered to implement a new system

19. Since there is numerous biometric systems available, which one would you prefer?
   a. Finger print scanner
   b. Iris scanner
   c. Retina scanner
   d. Voice pattern recognition
   e. Face recognition
   f. Others: please specify
20. State a reason why you have chosen the above answer?

Please comment on the following statements by circling or ticking the corresponding box:

21. I am likely to use a biometric system as a security system for my home.

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neither agree or disagree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
</table>

22. I am likely to use a biometric system to secure my computer system or device.

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neither agree or disagree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
</table>

23. I am likely to prefer using a biometric system than to use a traditional token/knowledge based system to protect my sensitive files and information.

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neither agree or disagree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
</table>

24. Biometric systems offer more secure form of security compared to other systems such as knowledge based or token based systems.

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neither agree or disagree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
</table>

Thank you for your time to complete the survey,

Your views are very much appreciated.
Appendix E – Results of Primary data Gathering analysed from Google forms
1. How many electronic devices do you have at home? (101 responses)

![Pie chart showing distribution of electronic devices at home.]

- 1 Device: 86.10%
- 2 Devices: 4%
- 3 Devices: 5%
- 3 or more Devices: 5%

2. How much time do you spend on using these devices? (100 responses)

![Pie chart showing time spent on electronic devices.]

- On a daily basis: 98%
- On a weekly basis: 1%
- On a monthly basis: 1%
3. What kind of security measures do these devices that you own have on them currently? (99 responses)

- Knowledge Based: 71.70%
- Token Based: 15.20%
- Biometrically Based: 11.10%
- Others: 2%

4. Do you think that the security measure currently available for your devices at home are secure enough in terms of encryption? (99 responses)

- Yes: 52.50%
- No: 47.50%
5. Please specify why for the above question (45 responses)

- Hackable.
- Hackers will try anything to break the password either for leisure or business.
- Random password. Date of birth etc is not included. But using some other numbers or names that people in the house cannot expect or even strangers. So far, no problem.
- No breaching so far.
- Hackers.
- Password keep changing.
- Needs stronger password.
- No security is secure enough... It all depends on needs and value of the information.. Since these are home appliances the needs for security is minimal.
- still prone to cyber attacks (hack).
- It is still susceptible to hackers.
- easily hacked and it even has been viral on ways of hacking it, esp in social media.
- Ignorance.
- The provider gives a guarantee that it’s secure.
- There are better systems available which is stronger & better.
- For safety reason.
- Technology hackers is becoming more prevalent.
- less hassle easy to remember.
- The asset value does not require strong encryption as no classified data lies within.
- Can be hack.
- It is sufficient for the security content of these devices.
- Not sure.
- The pin numbers are not duplicatable.
- Easy to get password.
- Hackers are a lot more resourceful these days, and are able to crack into individuals' passwords.
- No issue so far that I know of. Should be ok.
- got firewall n provider got one.
- Even the most secured government website was hacked thus I don't think my Samsung will be immune.
- Anything involve money transfer a token based security is needed.
- Can be hacked anytime.
- Due to simple passwords made.
- I assumed the service provider already provides the encryption.
- many kinds of hacking, even without the use of devices.
- Pass and token are kept safety by myself.
- Still open for public intrusion.
- My PC was hacked couple of times.
- The devices are kept safe at home and most of the family members are very forgetful, thus using specialised pin numbers with security questions is not favourable.
- Always change the password.
- Its too simple c and can easily be hacked.
- Easy to be crack open i think.
- Because people might know the password.
- Not secured at all cos fr my xperienced bfore my password was hacked many times by someone else even i have to changed the password many times.
- Because i dont have the knowledge.
- Anything manufactured by others is breakable electronically.
- Don't know - not sure.
6. When using knowledge based method of securing your device or system, how long would your chosen password have to be for it to be secure enough by your own standards of security? (101 responses)

7. Have you ever had any trouble with forgetting passwords for these devices or systems? (101 responses)
8. If so, How likely from a scale of 1 to 5 are you to forget a long password? (94 responses)

9. How many times are you usually required to reset your device or system password? (100 responses)
10. **Does your home have a security system?** (101 responses)

- Yes: 81.20%
- No: 18.80%

11. **If so, what kind of security measure does it use?** (38 responses)

- Knowledge based: 63.20%
- Token based: 18.40%
- Biometric based: 18.40%
12. Is it secure enough for your privacy needs in terms of encryption? (86 responses)

![Pie chart showing the responses]

13. Please state why you have chosen the above answer (39 responses)

- Any security system can always get bypassed.
- Don't have anything to hide
- I don't understand the statement.
- No problem so far
- No security measure except doorlocks
- Depends on environment
- Needs more secured encryption
- So far no intrusion to the system
- Even if home security is technology advance, it is still at risk of being broken into.
- Have no security system because hardly to choose the best one and some is very expensive too
- Its just prevention
- Cos there are hackers who needs to prove themselves
- Threat from hackers
- I need all of these due to safety reason
- Don't have one but planning to get one with biometric
- Not applicable as I only use lock and key for home security.
- What the hell is encryption
- Unsure of the questioned.
- Not sure
- As stated before its not duplicating and its different every time its needed to be uploaded
- It works so far
- Simple and not hassle
- Passwords can easily be retrieved by determined hackers
- No idea
- Got firewall server
- It's a modern world full with greed and scam
- Every security system has a loop hole
Depends on hackers capability
- Unlikely to be hacked
- No security system at home
- Does i have no home security system.
- Passwords can be hacked
- n/a
- Alhamdulillah so far nothing happen in terms of theft
- No comment
- Not really.
- Im not sure what is the answer
- No security measure for home.
- Don't know so not sure

What do you think would help improve the security encryption of your home security system? (39 responses)
- Not sure
- Not sure
- Always keep the system updated.
- change the password regularly
- Complex security program
- Additional measures
- Not sure. Probably by remembering the password instead of writing it somewhere.
- Continous upgrade
- voice security
- camera
- Home based firewall
- Direct Link to Security Company or Closest Police Station
- Dont connect to internet your security device
- Systems that are impenetrable
- Yeah but need to add alarm as well and possible if it can linked to police station. Once there is an alarm sound . So it will automatically alert the police station
- Double verification via mobile device fingerprint/token password as second authetication device.
- Not applicable
- Simple question please
- Two factor authentication
- Biometric based
- Camera
- Use mix password
- Using biometric-based security measures
- User friendly and simple but very secure.
- Provider's firewall
- finger print, eye scanning?
- Strong password
- Added features such as fingerprint, voice recognition, iris scan
- Need to reset every week or month
- pin number and finger print ID combined
- Simple but secured system
- N/a
- Voice recognisation or thumbprint
- Always update the system
- Need to be protected by laws
- I think of using the fingerprint or more relevant rather than using password. So it is more safety n secure for me.
- Don't know
- Get one first, then think about improving it.
- Don't know

15. Have you ever had any of your devices or systems being hacked into online or by someone you know of? (99 responses)

16. If yes then what have you done to ensure that it will never happen again or will do? (25 responses)
- Change password
- Change password
- if using fb just change new password
- Change my password into a hard one
- Change the password immediately.
- hack proof
- keep changing password
- firewall n secure ports internet access
- Chnge d security code/
- Not applicable
- Change password and also choosing complicated characters.
- reset password
- Put more effort into a more robust password, or install tougher security measures
- increase security n rutin
- Change password, and notify the relevant agencies
- Reset password
- n/a
- Change my password to something that is not known by anyone.
- Change my password
- Reset my password and be very careful with junk emails
- regularly changing the password
- Change passwords
- Nothing much just changed my password many times again n again. Feel fed up wt it!!! The hackers are very annoying!
- Frequently change passcode
- Don't know

17. Are you aware of the availability of these biometric systems below?(95 responses)

18. How did you find out about these systems?(72 responses)
- Internet
- Internet
- Internet
- Internet
- Internet
- Online
- Online
- Movies
- Movies
- Ok
- internet; blogs, website, YouTube,
- Through internet
- Workplaces, communication devices.
- im an it student
- Some of these can be found on phone features
- Device information thru media
  - Movies
  - Work related
  - From the bank
  - Online newspaper
  - Web blogs
  - movies, implement at a few corporate org in the country
  - Reading
  - Media and actual use of no 1
  - Internet
  - Relative handphone
  - The internet and it's glory
- TV
  - Social media
  - Media
  - Very secure
  - Work
  - Convenience and no one can cheat on it
  - Literature research
  - From office
  - Security training
  - Reading/research
  - Have seen them being used for security in commercial and public sector use.
- At work
  - Books internet
  - From workplace
  - Complicated and hassle
  - iPhone, Media
  - TV show and movies.
  - Interesting
  - Reading some random articles on the internet
  - Current affair
  - Advertisement and social media
  - From work experience
  - Current system used in banks and some in government offices
  - mobile phone security
- online
- Its available
- Internet & tv
- I have seen them on movies and on web
- When doing Visa Applications
- Media
- Social media
- Very useful
- Family member
- From tv
- It came with the device
- My lap top got one
- On television
- I search it in,
- Quite useful
- From website just read it to get knowledge.
19. **What is stopping you from not moving into a biometrically secure system from other traditional methods of security systems?** (97 responses)

![Pie chart showing reasons for not moving to biometric security systems.]

- 39.20% Strict budget
- 26.80% Not much knowledge of the system
- 23.70% Not bothered to implement a new system
- 10.30% Other

20. **Since there are numerous biometric systems available to be used, which one would you prefer?** (96 responses)

![Pie chart showing preference for biometric systems.]

- 65.60% Fingerprint Scanner
- 11.50% Iris Scanner
- 8.30% Retina Scanner
- 7.30% Voice Pattern Recognition
- 4.20% Face Recognition
- 3.20% Others
- 1.00% Others
21. State a reason why you have chosen the above answer (72 responses)

- Easy
- Easy
- Easy
- Easy
- Easy
- Easy
- It's easier
- It's easier
- Simple
- Simple
- More secure
- More secure
- Most convenient
- Most convenient
- just simple n very easy 2 use fingerprint scanner
- Use that one only
- Its simple and everyone have a different thumb pattern
- One of the most developed biometrics.
- because iris, retina and fingerprint is something that u cannot duplicate, so it is very secure
- It's easier
- Added security
- More secure. Even when you are sleeping.. people can get your eyes (retina) to unlock the password. If you are using other.. eg fingerprint scanner.. when you are sleeping.. people can still unlock it by keep on trying to search which finger you are using for your password.
- Impossible to break
- easier recognition
- Would put your eyes to damage potential if you scan them.
- More secure than others
- More diffMore difficult to duplicate
- Positioning of the palm are more easier
- Not easily copied
- It never change
- Easy
- Easy to use
- Uniqueness
- Easier than the others, no hassle of taking of eyewear etc
- hardly to be duplicated
- difficult to copy
- Fast reading
- It s at d finger tip
- No hassle using any ten fingers we got if one finger , can use other finger
- We have 10 fingers option to choose from - extra layer of configuration & its convenient
- Ease of use. Just stare into the reader.
- Widely used by most devices,
- Simpler and more widely acceptable to people
- Faster and hygienic
- Most secure and convenient
- Probably the cheapest
- Mire secure
- Easy and reliable
- simple and precise
- Most convenient and somewhat safe
- Easiest, least hassle
- Hard to duplicate even if it can be done
- Security approved (unless there is other tactics to overcome this) I'm pretty sure it will. At the end, security systems are built to be broken into? (Phrase from movie)
- Simple and easy and fast perhaps and no fingerprint are the same
- Very practical on regularly use.
- Simplest identification
- More convenient to use
- Not sure, sounds secure
- Ease of use
- N/A
- It would be more recognizable and not retainable from other people.
- Easy to use
- Easy to recognize
- Every person has different fingerprints
- So that I don't have to remember my password, I hope nobody can hacked my fingerprints.
- More practical
- No chance of hacking
- It's easier using fingerprints
- Because it is convenient to use fingerprint
- Nobody could log in ONLY me the authorised person 😊
- Because it's already on my smartphone
- Not easily copied.
- Don't know so not sure
Please Comment on the following statements by ticking the corresponding scale from 1-5

22. I am likely to use a biometric system as a security measure for my home (100 responses)

23. I am likely to use a biometric system to secure my computer system or device (101 responses)
24. I am likely to prefer using a biometric system than to use a traditional token/knowledge based system to protect my sensitive files and information (101 responses)

25. Biometric systems offer more secure forms of security compared to other systems such as knowledge based or token based systems (100 responses)