



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

To compare and contrast the efficacy of user authentication methods.

by Kazuaki Ieuan Roach

Supervisor: Tim Bashford

Second Marker: Dr. Glenn Jenkins

Project submitted as part of the requirements for the award of
BSc (Hons) Software Engineering.

May 2016

DECLARATION

I, Kazuaki leuan Roach, hereby declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed :

Date :

FORM OF CONSENT

I, Kazuaki Ieuan Roach, hereby consent that my Project, submitted in candidature for the B.Sc. (Hons) Software Engineering degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed :

Date :

Table of Contents

Table of Figures	4
Table of Tables	4
Chapter 1: Introduction	5
Chapter 2: Research and Review of Literature	6
2.1 Introduction	6
2.2 Security.....	7
2.3 Knowledge-based Authentication	8
2.4 Token-based Authentication	9
2.5 Identity-based Authentication	10
2.5.1 Fingerprint Scanning.....	11
2.5.2 Finger-Vein Scanning	13
2.5.3 Facial Recognition	14
2.5.4 Ethics.....	15
2.6 Comparison of Methods	17
2.7 Conclusion.....	19
Chapter 3: Methodology	20
3.1 Research Methodology.....	20
3.2 Development Methodology	21
Chapter 4: Design and Implementation	22
4.1 Requirements	22
4.2 Diagrams	23
4.2.1 Class Diagram	23
4.2.2 Entity Relationship Diagram.....	24
4.2.3 Top-Level Use Case.....	24
4.2.4 Activity Diagram	25
4.3 Implementation	26
Chapter 5: Analysis.....	27
Chapter 6: Evaluation	29
Chapter 7: Conclusions and Recommendations	31
Chapter 8: Reflections.....	32
Chapter 9: References	33
Appendices.....	35
Appendix A.....	35
Appendix B	36
Appendix C	36
Appendix D.....	36
Appendix E	36
Appendix F.....	37
Appendix G.....	37
Appendix H.....	37
Appendix I	38

Table of Figures

Figure 1: An example model of Frustrated Total Internal Reflection [15].	11
Figure 2: Examples of common minutiae and how they are identified [14].	11
Figure 3: The same user having their fingerprint measured twice [14].	12
Figure 4: An example of a finger-vein scanning device and the images it captures [16].	13
Figure 5: A sample finger-vein image (a) and its corresponding template (b) [16].	13
Figure 6: Class diagram for the system.	23
Figure 7: The Entity Relationship Diagram for this system's database.	24
Figure 8: The top-level use case for the system.	24
Figure 9: Activity diagram for the system.	25
Figure 10: Screenshot of format used for survey.	27
Figure 11: A decomposition of the login use case showing ideal operation.	37
Figure 12: A decomposition of the login use case showing the 'Student Not Found' error.	37
Figure 13: A decomposition of the security question use case showing ideal operation.	37
Figure 14: A decomposition of the security question use case showing 'Answer Incorrect' error.	38

Table of Tables

Table 1: Relative security of biometric authentication methods. [1]	17
Table 2: Comparison of biometric authentication methods by Jain et al. [14]	17
Table 3: Results of Student's t-test.	27
Table 4: Results for the fact-based questions of the survey.	28
Table 5: Results for the ethical questions of the survey.	28
Table 6: Comparison of wide range of user authentication methods. [8]	35
Table 7: Results for the strength of security question before reading the passage.	36
Table 8: Results for the strength of security question after reading the passage.	36
Table 9: Results for the comfort of use question before reading the passage.	36
Table 10: Results for the comfort of use question after reading the passage.	36

Chapter 1: Introduction

Gorman [1] defines authentication as ‘the process of positively verifying the identity of a user, device or other entity in a computer system’. This is not a process exclusive to computers by any means: in any other context authentication may be carried out simply by recognising someone’s face or voice or by giving them the key to a door; these are valid means of ensuring someone’s identity and that they are trusted with access. However, this report concerns itself specifically with computerised authentication, specifically how to authenticate human users – machine authentication is a separate field that is a lot more predictable and reliable than user authentication.

The area of computerised user authentication methods is a critical field of study in the modern age: ensuring data security is an ever-present concern, especially in areas such as commerce, law enforcement and public services, therefore it follows that much research must be done into methods of positively identifying a user and ascertaining that they are who they say they are. To that end many diverse technologies have been developed, dividing the field of authentication into categories that can be studied individually and compared. The broad fields that will be discussed later in greater detail are knowledge-based, token-based and identity-based authentication [1], each of which has distinct technologies.

It is the aim of this project to study the current state of authentication methods, to compare their technical effectiveness and to evaluate their suitability in terms of human-machine interaction. This will require research into the objective measures used to compare authentication methods and the more subjective usability of these methods.

This project also includes the development of a system which uses user authentication. This system can then be tested to see if data collected from research can be corroborated. The wider the range of authentication methods that can be used, the better the results will be: ideally the finished system will incorporate at least one example of each of the three categories of authentication mentioned above.

Finally, the project includes a survey component which will be used to gauge user perceptions of authentication. This will be useful to find out the level of information concerning authentication that the average user is likely to have and their views on such issues as use of private data in secure systems. The data gathered will be used to ascertain the difference between user perceptions and reality, thus highlighting areas where future efforts to educate users could be focused.

Chapter 2: Research and Review of Literature

2.1 Introduction

User authentication is by no means a new idea: long before computers were invented people had to find ways of identifying potential entrants to a secure system to determine whether they were authorised to gain access to it, for example by having a guard on duty who could recognise their faces or by giving them a key to the door. The basic principles of authentication have not changed but the means used must, of necessity, be updated to accommodate the unique properties of computer systems.

It is important to make the distinction between machine and user authentication: later mentions of authentication will refer to user authentication specifically. Computers have a variety of means for ensuring machine authentication between each other that are quick and secure, but verifying the identity of the user is rather harder for a computer [1]. The overall strength of any security system is measured by its weakest link and humans – with their faulty memories, their propensity for losing things and making mistakes, not to mention their susceptibility to coercion – are often identified as that weakest link [1-3].

Considering that authentication is a vital part of system security it is a field that is constantly being researched and refined – but however sophisticated authentication methods become, there are three fundamental factors that can be used to classify them. These factors are determined by what the authentication system requires of its users (which may be referred to as the ‘authenticator’)[2, 4]:

1. Something you know.
2. Something you have.
3. Something you are.

It is worth mentioning at this point that there is such a thing as Multiple Factor Authentication (MFA) that uses a combination of authentication methods.

2.2 Security

The main point of a user authentication system is of course to provide security, but it can be difficult to provide an absolute metric of how secure a system is: while it is easy to make the distinction in relative terms, for example by saying that a token requiring a PIN is more secure than a token that does not require a PIN, pinpointing where exactly one's system stands on an absolute spectrum of security is harder.

Gorman [1] proposes that 'A strong system is one in which the cost of attack is greater than the potential gain to the attacker', which makes a certain amount of sense: more secure systems that employ iris scanners are unlikely to be used in any but the most high-security of situations, since it simply would not be economical to buy such sophisticated equipment for cases where the security risks are relatively low. The matter then becomes one of matching the security needs of your system to the appropriate level of security provided by one or more means of user authentication.

Also to be considered is the human factor. Technically speaking, passwords are actually a very strong form of authentication – if one can remember an alphanumeric string hundreds of characters long. Users either do not see the need to or simply cannot be bothered to generate and remember strong passwords, assuming that they even know what constitutes a strong password in the first place. Adams and Sasse [3] argue that the lack of secure passwords is partly due to a lack of education about what makes a password secure and also to a lack of motivation to maintain security protocols. This leads to a perception among designers of authentication systems that users are a security disaster waiting to happen and, on the other hand, leads users to believe that those who design these systems do not even try to make them convenient for busy professionals. An authentication system can be the most technically advanced marvel of modern technology in the world, but if its users are not trained in its use or do not see its importance then the system is vulnerable.

One metric often used when attempting to rate the effectiveness of an authentication system (from a purely technical standpoint, usability and acceptance notwithstanding) is the comparison between the percentage of successful authentication attempts by non-authorised users (False Acceptance Rate or False Match Rate) and the percentage of failed attempts by authorised users (False Rejection Rate or False Non-Match Rate): clearly a lower FAR means a more secure system but an excessive FRR will lead to user frustration and should also be kept as low as possible [5].

2.3 Knowledge-based Authentication

Although there are other forms of knowledge-based authentication, the archetypal and most widely-used form to this day must surely be the password. Password authentication lends itself naturally to modern-day computers due to the lack of a need for specialised hardware: the computer displays a password prompt on-screen and the user then types in a password via the keyboard, fulfilling the simple challenge-response pattern of a password authentication system with standard computer hardware.

Passwords as a means of user authentication for computerised systems can be traced back as far as 1961[4], but in a manner similar to the design flaws of IPv4 the future popularity of user account-based systems was drastically underestimated. In those early days it was anticipated that each user would have only a few user accounts at most and therefore would only have to remember a couple of passwords, but the overwhelming proliferation of computing systems over the Internet since then has led to a situation where the average user can expect to have anywhere around 25 accounts on various different systems, eight of which they will log into every day [6]. This leads to a situation fraught with problems: the average user cannot possibly be expected to remember 25 separate passwords, so they will naturally tend to reuse the few passwords that they can remember; Florêncio and Herley [6] say that the average user will have ‘6.5 passwords, each of which is shared across 3.9 different sites’. Users may use memory aids or password management programs to keep track of their passwords, both of which compromise system security [3, 7].

The above assumes that would-be hackers even require knowledge of passwords to break them: unless forced to choose something more complex, users will tend to choose short passwords with only lowercase letters, no numbers and no special characters [1, 3, 4, 6, 7], making it laughably easy for a brute-force attack with a relatively small dictionary to guess passwords for accounts that do not have good password moderation – speaking of which, the oft-used organisational policy for replacing passwords on a regular basis further increases the burden of memorisation on the part of the user, increasing the likelihood that users will resort to memory aids and definitely increasing users’ frustration with the system.

2.4 Token-based Authentication

In any system where the authenticator is a physical object like a card, that object is referred to as a ‘token’ (although it may also be known variously as a ‘security token’, an ‘access token’ or some variation thereof) [1]. Token-based authentication replaces the complicated business of remembering multiple passwords with a single point of failure: do not forget or lose your token. This still happens often enough that card-based authentication often incorporates a PIN as part of a MFA approach (like the typical ATM system) [1, 2, 8]; even in the case that someone loses their card and it is picked up by someone else who wishes to gain unauthorised access to the system they are still missing a key piece of knowledge (the PIN) required to gain access, thus maintaining the system’s security.

The idea of authenticating via a token is an easy concept for new users to grasp since token-based authentication already has a commonplace analogue equivalent in the form of using a key to open a locked door – but it goes without saying that computers require much more specialised equipment such as a card-reader, making the implementation of a token-based authentication system expensive compared to simple password authentication.

Proctor et al. [9] suggest that the process of using a card-reader is perhaps too complicated to pick up easily, even more so than using a fingerprint scanner, but the study conducted by Braz and Robert [8] compares MFA cards positively to biometrics, saying that smart cards integrated with public key security provide an equally good level of usability and a superior level of security to even static biometrics. Paul et al.’s study [2] concluded that MFA smart cards (integrating PINs) were popular and perceived as easy to use compared to a regularly changing password system, although it is worth noting that they did not find any reason to believe that cards were necessarily more secure, especially when users made mistakes while acclimating to the new authentication process, perhaps lending some credence to Proctor et al.’s assertion.

2.5 Identity-based Authentication

Identity-based authentication, more commonly known as biometrics, attempts to verify a user's identity by some property of the user's own body, either physical or behavioural. The advantages here are obvious: there is no chance of losing the authenticator (except in cases of injury) and, if chosen well, said property is likely to be unique and difficult to reproduce.

Jain et al. [10] propose that a biometric property should have the following qualities to make it effective as a means of authentication:

- **Universality**
The chosen property should be applicable to everyone, assuming that they have not suffered from disfiguring accidents.
- **Distinctiveness**
The biometric property should be distinctive enough that it can be used to tell apart two users with ease.
- **Permanence**
The property should be unchanging, at least for the period of time that the system is anticipated to be in use.
- **Collectability**
The property must be capable of being measured in a quantitative manner.

Using these points as a guide, one can assess the suitability of various biometric properties as authentication methods. Traditionally speaking one's signature is regarded as a trustworthy biometric property, but considering the impermanent nature of a signature which may undergo change according to a user's tastes or a simple motor error, not to mention the ease with which a signature may be forged after sufficient practise, it is perhaps not the most reliable or secure property to use. Properties like a user's fingerprint or iris are much more likely to remain constant over time and are much harder to replicate. It should be noted, however, that biometrics are by no means unforgeable, and therefore are best used as part of a MFA approach [1].

As an example of MFA incorporating biometrics, the area of keystroke dynamics [11-13] is being looked into as a means of hardening conventional passwords: each user will tend to type in a way that can be measured with some degree of accuracy, so it makes sense to use a user's typing patterns to verify whether they are the one typing in the password. While the method is by no means perfect (not that any system that required high security would use only password authentication in the first place), it is a good example of how unobtrusive extra layers of authentication can be introduced to a system with which users are already familiar and which places no further burden of expenditure or learning on the user.

One area in which biometrics are lacking when compared to other methods is repudiation, that is to say the case where an unauthorised individual gains access and the legitimate user is consequently seen as the attacker [1]. In a case where someone has lost a token, the solution is simple: remove access rights for the lost token, instate a new one and give the new token to the user. In a case where fingerprints are copied and used to gain unauthorised access, the answer becomes less evident; one can't simply issue a new set of fingerprints for the user. It is entirely possible that such a user may become unable to use the system as a result.

2.5.1 Fingerprint Scanning

Fingerprints are formed during foetal development and, as far as we know, there are no two people in the world who have exactly the same set of fingerprints (not even twins), making them making them distinct enough to use as a biometric property. They can be measured and recorded and last potentially for the user's whole lifetime, although it is worth noting that deformation or erosion of one's fingerprints via injury, constant friction or corrosive chemicals can render them entirely useless as a form of authentication [14].

The principle is to scan the user's fingerprint(s) (some methods scan only one, some scan multiple; obviously the more scanned the higher the accuracy) using specialised hardware; the scanned image can then be analysed by algorithms that ascertain the unique features of the user's fingerprint and reduce that to a code that can be used to uniquely identify the user.

The oldest and most common form of fingerprint scanner uses the technique called Frustrated Total Internal Reflection [15]: due to the properties of light when shined through a prism, light reflected at the correct angle off a fingerprint placed on top of the prism will produce an image for a camera on the other side of the prism that shows the ridges of the fingerprint as dark and the valleys as light.

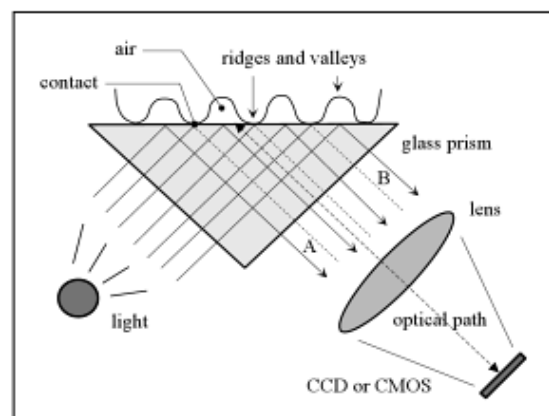


Figure 1: An example model of Frustrated Total Internal Reflection [15].

Once the image has been captured it is then analysed by the system which will attempt to identify patterns, also known as 'minutiae': the system will record all the minutiae it can find, including the position and orientation of each minutia, to build a template [5].

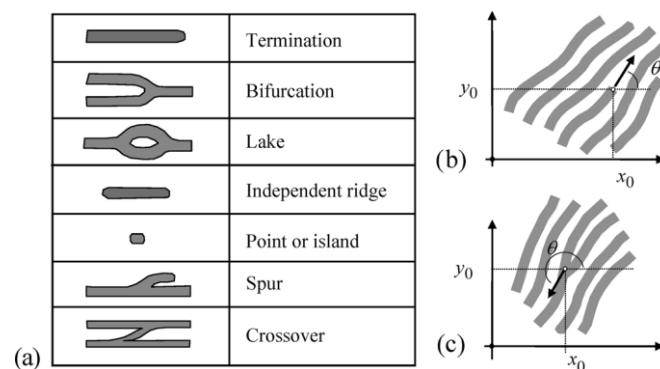


Figure 2: Examples of common minutiae and how they are identified [14].

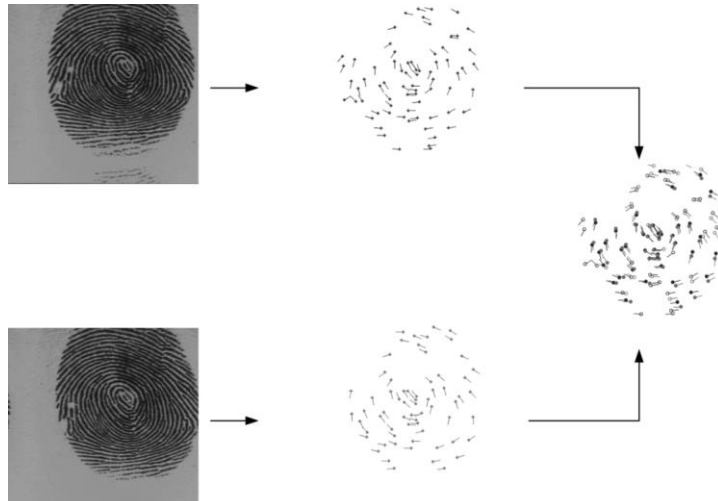


Figure 3: The same user having their fingerprint measured twice [14].

It is important to note that a host of problems can interfere with fingerprint reading, such that even templates taken from the same user on different occasions may not be absolutely identical: factors such as light levels, the moistness or dryness of skin, the distortion or compression of the finger's skin as it is pressed onto the sensor can all have a significant impact on the image and the template derived therefrom [5, 14, 15]. As such, it is highly unrealistic to expect that a user's authentication template will be a one hundred percent match with the template they provided on enrolment; to compensate for this a threshold is built into every fingerprint authentication system, a margin for error that will allow the system to accept templates that are similar enough to be acceptable: the matter of where to place the threshold is a delicate balancing act between the False Acceptance Rate and the False Match Rate that is, in the end, up to the discretion of the developer [10].

2.5.2 Finger-Vein Scanning

While fingerprints are useful as a means of authentication, the fact that they are an external biometric property can sometimes lead to them becoming damaged and unreadable. Finger-vein scanning avoids this problem by measuring an internal property, one that is unique to each individual and can be read without invasive means.

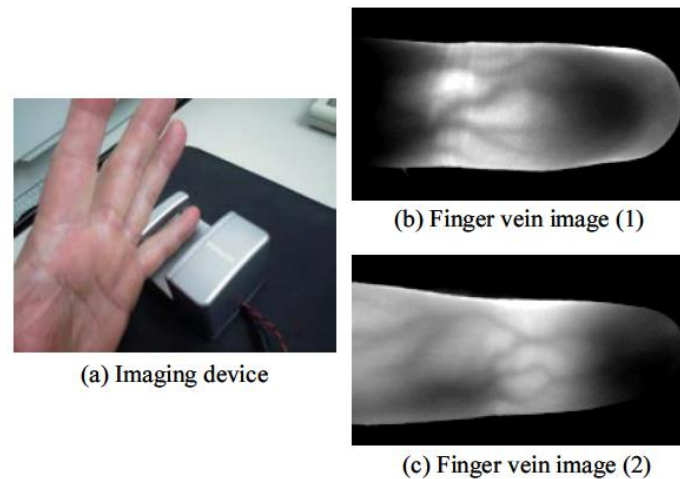


Figure 4: An example of a finger-vein scanning device and the images it captures [16].

Finger-vein scanning captures an image of the veins inside one's finger by shining light on it which is close to the infrared side of the visible spectrum [16, 17]: this particular frequency of light has the special property of being able to pass through skin (rather than being reflected by it like other frequencies of light) while still being reflected by haemoglobin present in the finger's veins, such that a camera on the other side of the finger can capture an image where flesh appears light and the veins are visible as dark lines. The brighter the light used, the clearer the image will be – although bone and muscle can sometimes cause imperfections.

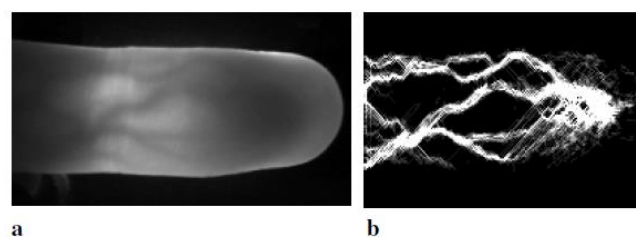


Figure 5: A sample finger-vein image (a) and its corresponding template (b) [16].

The system can then run analysis on the image, using line-tracking algorithms to identify the 'valley' of darker pixels that composes each vein and following the routes they take to create a template. After that, noise-reduction on grey boundary pixels and 'shading' caused by skin, bone or muscle which may occlude portions of the veins helps to make the final matching algorithm more accurate. Another way to increase the accuracy of the matching algorithm is to increase the number of tracking operations used to generate the template: Miura et al.'s [16] experiment found that increasing the operations from 100 to 3,000 and above made templates generated from the same finger much more consistent.

2.5.3 Facial Recognition

Facial recognition technology attempts to replicate a process that humans can do seemingly automatically: identify a person by their facial characteristics alone. Facial recognition has been studied for decades now and is still being explored as a means of authentication, despite its relative lack of accuracy in comparison to other biometric methods [14]: facial authentication is a technology that requires only a photographic image of the participant, a procedure that is non-invasive and with which most users are quite familiar, and as such is much more likely to find acceptance than other methods.

There are two main approaches to facial recognition: the holistic method and the feature-based (or structural) method. Holistic recognition relies on the comparison of the user's image with a database of sample faces known as 'eigenfaces'; the percentage similarity of a user's face from a range of often just a few eigenfaces can be used as a metric to describe their appearance [18]. However, holistic recognition is extremely sensitive to changes in light, orientation and distance of the capture image, requiring a close-up frontal shot, and is therefore often used as the baseline to which new methods are compared. Feature-based recognition makes note of specific features of the face, for example the eyes, nose and mouth, to calculate the distance, proportion and orientation between them, and generally speaking is far more robust than the holistic approach. That is not to say that these two approaches cannot be combined into hybrid methods, which they often are.

Facial recognition technology has come a long way from its inception: in the beginning it was restricted to two-dimensional static images, but there are methods in development as of this writing that can construct a three-dimensional model of a person's face from video footage and potentially identify them even from a profile perspective [18].

2.5.4 Ethics

There is some concern surrounding the ethics of using biometric properties as a means of authentication. Since such properties are an inseparable part of our own bodies people can sometimes feel uneasy about allowing them to be recorded, claiming that biometric recording is necessarily an invasion of our privacy whether we allow it or not [19]. Authentication by biometric properties is by no means a new idea – the field of criminal forensics has for a long time used such measures as fingerprints to identify possible criminals – but the integration of biometrics with complex computer systems raises questions as to the security of our personal data and the purposes for which it might be used.

Biometric data is potentially sensitive personal data and as such should be subject to data protection laws. Although data protection laws may not be absolutely uniform the world over, they generally state that no-one should have personal data held about them that they have not agreed to give to the holder and which is not being used for any useful and lawful purpose – although law enforcement authorities themselves are exempt from such rules which raises issues of possible abuse by the powers that be, particularly in light of an incident at the 2001 Superbowl in which the Tampa Police Department took covert footage of the crowd in an attempt to identify criminals through facial recognition software [19].

Sutrop and Laas-Mikko [20] point to two particular examples of biometric technology as possible breaches of ethics: the Future Attribute Screening Technology (or FAST) being developed by the U.S. Department of Homeland Security and the Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces system (ADABTS) which is funded by the European Union. Both of these systems are being developed with the express intention of identifying dangerous individuals in light of the terrorist attacks of recent years and both of them use a method similar to the Superbowl incident mentioned above: covertly recorded data is used to analyse, without their knowledge or consent, the behaviour of suspected individuals to predict the likelihood of them being terrorists or otherwise dangerous.

Another concern that people might have with biometric data is the idea of scope creep [5, 19, 20], namely that data given voluntarily for a seemingly innocuous purpose may be used for other purposes for which consent was not given, much in the manner of direct marketing companies that buy your details from more legitimate organisations to harass you with unwanted advertisements or confidence frauds. Weaver [5] gives the example that a country's government might take biometric data recorded from non-citizen immigrants purportedly to help them integrate into their new home and use that to try and identify them as criminals.

All of the problems discussed so far seem to have a common element: the problem is not anything intrinsic to biometric technology specifically, but rather concerns a breach of data protection law that could apply to any other form of personal data, namely that the data is being used without the owner's knowledge or consent for purposes to which they have not agreed. Jones et al.'s study [21] corroborates this: the top three concerns of respondents were that they should be told when their biometric data is collected, that they should be informed of its intended uses and that it should never be used for any other purpose. The issue here seems to be less one of whether biometric systems are intrinsically dangerous and more whether we can trust those who are collecting this data to use it responsibly.

Wickins [22] argues that biometric authentication is by its very nature discriminatory against certain kinds of people, which would become a major problem were biometric identification ever to become necessary for vital government services like healthcare or for getting a new job, running the risk of excluding members of society who are already vulnerable in other ways. Groups that he claims are at risk due to biometric systems are:

- People with physical and/or learning disability

A study by the UK Passport Service concluded that people with disabilities have a much harder time enrolling onto biometric systems.

- People with mental illness

No evidence is given here; Wickins uses only conjecture for this section.

- The elderly

The UKPS noted that the elderly were more likely to be technophobic and therefore likely to try avoiding using biometric systems altogether, although this begs the question how this is point is relevant to the argument when it is not biometric systems specifically that cause this problem so much as computerised systems in general.

- People of certain races

The UKPS also noted that black people had a harder time enrolling in facial biometrics, iris scanning and fingerprint scanning. If this is true then it is an interesting technical limitation that must be addressed (although it seems implausible that the colour of one's skin would affect measuring one's iris).

- People of certain religions

There are religions such as Islam and Sikhism that require their followers to wear head or face coverings that would disrupt facial recognition systems.

- The homeless

Wickins argues that the homeless will not be able to receive enrolment information from the government, having no fixed address to which it can be sent. Similarly to the technophobia of the elderly, this seems to be a problem that already exists and which is inherent to systems beyond biometrics' control.

Given the above examples it is possible that biometric systems could be socially problematic, but it seems that the main problems here arise in situations where people either are not physically capable of conforming to the system's needs (perhaps because of injury) or simply won't, either due to fear of the system or religious demands. It is worth considering auxiliary methods of identification and authentication intended for use by those for whom biometric methods may not be suitable.

2.6 Comparison of Methods

Biometric	Test	Test Parameter	Attempts	FNMR	FMR
Face	FRVT [54]	11-13 mo. spaced	1	16%	16%
	CESG [56]	1-3 mo. spaced	3	6%	6%
Fingerprint	FVC [55]	Mainly age 20-30	1	2%	0.02%
	CESG [56]	Mainly age 30+	3	2%	0.01%
Hand	CESG [56]	-	1	3%	0.3%
	CESG [56]	-	3	1%	0.15%
Iris	CESG [56]	-	1	2%	0.0001%
	CESG [56]	-	3	0.25%	0.0001%
Voice	NIST [53]	Text independent	1	7%	7%
	CESG [56]	Text dependent	3	2%	0.03%

Table 1: Relative security of biometric authentication methods. [1]

Table 1 compares various biometric authentication methods by their False Non-Match Rate and False Match Rate (synonyms for the FRR and FAR discussed earlier). One can tell at a glance which methods are superior in terms of technical security, but such a table does not necessarily take into account the full picture.

Factors →	Universality	Distinctiveness	Permanence	Collectable	Performance	Acceptability	Circumvention
Biometric identifier ↓							
Face	H	H	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 2: Comparison of biometric authentication methods by Jain et al. [14]

Table 2 takes a wider view, both in terms of the methods compared and the criteria used to compare them. Not only does it rate each method by its suitability as a biometric measure by the four properties mentioned earlier which tends to correlate with its Performance rating (defined as a measure of its matching speed and accuracy), but also the likelihood that it will be accepted and its susceptibility to forgery. This table agrees with the previous that iris-scanning is a very secure authentication method, but its low acceptance rating may be a more telling indicator of whether users would be willing to use such a system.

The table in Appendix A gives an even wider comparison, taking into account conventional (that is to say, non-biometric) methods as well. This table appears to corroborate the findings of the previous tables: retina or iris scanning is rated highly for security but lowly for usability, whereas less permanent biometric measures like voice or signature enjoy more usability at the cost of security (one can take usability here to incorporate acceptance in its meaning). Interestingly, Braz and Robert [8] assert in this table that non-biometric methods can be the equal of biometric ones in terms of security and even superior in terms of usability, namely MFA cards and public key encryption.

By taking a look at these tables it becomes evident that any attempt at designing biometric systems must necessarily take into account not only technical aspects like their FAR and FRR but also their usability; if we take it as read that a security system is only as good as its weakest link then we must also accept that a biometric system is only as good as its level of acceptance and usability among its intended users. Habituation and education are key to the integration of biometric authentication in future systems.

2.7 Conclusion

From the sources seen so far it is evident that there is already a vast body of literature covering the technical capabilities and limitations of authentication methods, allowing one to make comparisons in terms of pure effectiveness. While it is worthwhile to corroborate these findings by attempting to reproduce them, it would also be beneficial to find out more about the human aspect, i.e. how authentication methods (particularly biometrics) are viewed by their potential users and how that affects their acceptability and usability.

It is reasonable to assume that people not involved in the production and maintenance of authentication systems may not have a realistic understanding of how these systems work (case in point: previous discussion about what the average user thinks is a strong password) and this lack of accurate knowledge may unfairly colour their perceptions about what methods are best to use, possibly resulting in sub-optimal choices (like facial or vocal recognition over fingerprint scanning) or improper use of the system.

Taking the above into account, it would be of interest to compare the perspectives of users on authentication methods – particularly on biometric methods, which as the newest technology seems to have the greatest mystery surrounding it – to the reality of the situation; by studying the discrepancy between user expectations and factual data we may be able to highlight some gaps in understanding that would be of benefit to future attempts to educate potential users about authentication.

Chapter 3: Methodology

3.1 Research Methodology

Deciding on the correct research methodology to use for this project is somewhat problematic in that it could validly include both quantitative and qualitative data: there is the technical aspect of how effective in objective terms the technologies employed in authentication and biometrics are, then there is the usability aspect to be considered in which the users' views on the field being studied have to be taken into account, since one can easily put forth a strong case that a user authentication system cannot be deemed effective unless its users understand it and are comfortable using it.

Given the combination of quantitative and qualitative data sets to be gathered here, it will be best to take a pragmatic philosophy with this project. It would be incorrect to use any philosophy that values either factual or experiential data more highly than the other; considering that both forms are equally important in the realm of user authentication it only makes sense to adopt a philosophy that gives equal weight to both, thus allowing for research that can draw conclusions in a holistic manner rather than focusing solely on either.

It is because of the mixed nature of the data available on this subject that this project is to use mixed methods to gather data: while the development of an authentication system is the central focus of the project, running tests using that system will only go so far; it will also be of great value to elicit the opinions of users in a more direct fashion by using surveys, thereby finding out the views of as large a cross-section as possible concerning authentication and its applications using biometric technology.

Although the original intent of this project was to be deductive, as a result of research into literature a new inductive angle has presented itself: it is a reoccurring theme in many of the sources researched so far that user understanding of even fairly simple and commonplace forms of authentication such as passwords is often wildly inaccurate, usually due to lack of education on the subject, so it would be interesting to devote part of this study to ascertaining whether that is also the case for biometric technologies. Given how new and rare biometric authentication systems are in relation to other forms of authentication, it would make sense for there to be a good deal of misunderstanding surrounding them. It would be of benefit to see what impact misconceptions regarding biometric authentication have on the average user's willingness to use them. Will the lack of education about such systems have a detrimental effect on their popularity in future? Do people eventually take to biometrics given time and training, or is there some aspect fundamental to their nature that makes people averse to using them? The survey in particular will be focused on answering these and similar questions to see whether there is any correlation between user misconceptions and willingness to use biometric authentication.

3.2 Development Methodology

The original development plan for this project was rather grander than the one with which it has now settled: the intention was to create a system with discrete modules, each one devoted to a particular form of authentication; one was to be password-based, another was to use smartcard technology, another to use fingerprint scanning. Regrettably, various pressures have resulted in the diminishment of the system to only one form of authentication, in particular the problems encountered trying to incorporate a third-party fingerprint scanner and its API into the system.

The above being so, after due consultation it was decided that the system should be reduced to a simpler one using only password-based authentication: the final system is to be a Windows Forms application using WCF to allow multiple instances of a client login form to update a list on the server, functioning as a means to allow students to register from their own computers as they arrive in class and log in.

The sheer simplicity of the program makes it difficult to fit into the context of a larger development methodology, which are usually designed for large-scale projects involving teams of software engineers working in concert. An advantage of the small scale of the project is that the requirements for this system are well understood at least, so it is unlikely that much iteration will be needed. Taking into consideration the time remaining, it is unlikely that there would be enough time for more than one cycle in any case. This is a relatively small and simple system, so following the development cycle through once in the classic waterfall model should yield the desired results. There is no particular need here to deviate from what may be thought of as the 'traditional' methods of software engineering.

In the event that the system does not operate entirely as planned, some white box testing should be able to iron out any bugs or unintended behaviour. As previously stated it is unlikely that there will be much opportunity for user feedback on the system as valuable as it would be, so any other form of testing is to be regarded as strictly unfeasible in this case.

Chapter 4: Design and Implementation

4.1 Requirements

The proposed requirements for the system are as follows:

1. Must allow students to log in client-side.
 - 1.1. Must receive valid First Name, Last Name and Password to allow login.
 - 1.1.1. Should use some form of password encryption to increase security.
 - 1.2. Must have the student correctly answer a security question.
 - 1.2.1. Should provide a variety of security questions for the student to provide answers for during enrolment.
 - 1.2.2. Must have answers for at least three questions to allow for random selection of question-answer pairs for each login instance.
 - 1.3. Must support multiple instances of client interacting with server simultaneously.
2. Must display logged in students to the lecturer server-side.
 - 2.1. Must add new students to the register with each successful login.
 - 2.1.1. Must check that each student added to the list is unique to avoid duplicates.
3. Must interact with a database to store all necessary data.
 - 3.1. Must have the structure to store data on each student's login details, their security questions and each question's corresponding answer.

4.2 Diagrams

4.2.1 Class Diagram

Figure 6 shows the complete class diagram for the system. Considering that the system to be constructed is a WCF application, the separation between the server and client portions of the system has been represented using packages: the two communicate via a ServiceHost object as part of the .NET framework, using metadata to expose services to the client.

It should be noted that the Password class used here is taken from another source and has a great deal more complexity than is shown here: the methods displayed are those which are directly called on by other parts of the system; the rest has been abstracted.

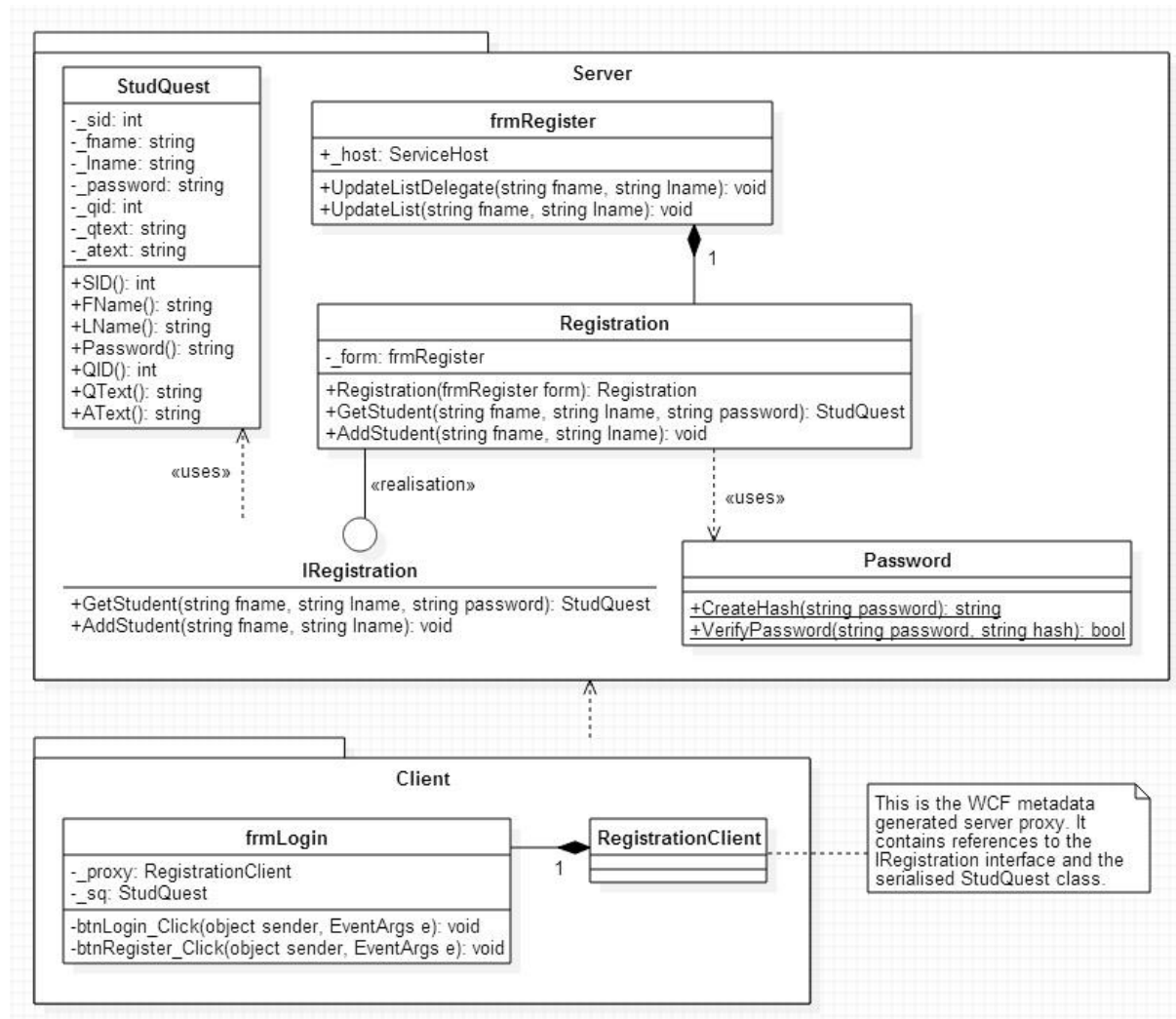


Figure 6: Class diagram for the system.

4.2.2 Entity Relationship Diagram

Figure 7 shows the composition of the database used by this system. It is a relatively simple one, requiring only two main tables (Student and Question): a point of complexity arises in the many-to-many relationship between these tables, but that has been resolved with the introduction of an intermediate table (StudQuest) which also stores the answer for each Student/Question pair.

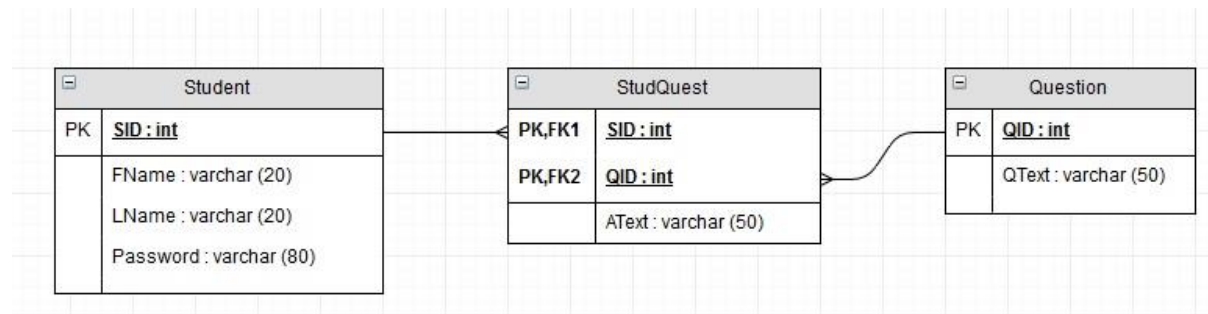


Figure 7: The Entity Relationship Diagram for this system's database.

4.2.3 Top-Level Use Case

Figure 8 shows the top-level use case for this system. Lower-level decompositions for ideal operation and error cases can be found in the appendices.

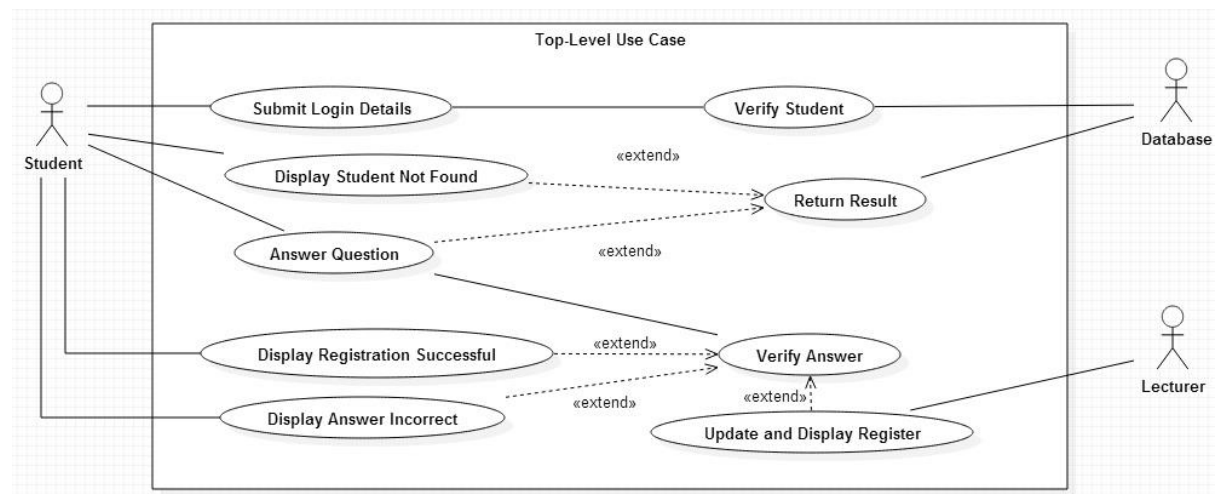


Figure 8: The top-level use case for the system.

4.2.4 Activity Diagram

Figure 9 shows the behaviour of the system from beginning to end for each instance of the client program. Operation of the system is split into two key segments: the login phase, where the user's identity is verified by their name and password, and then the question phase, where the user is further authenticated by their response to a security question. Both of these phases have checks and may result in the user having to re-enter details.

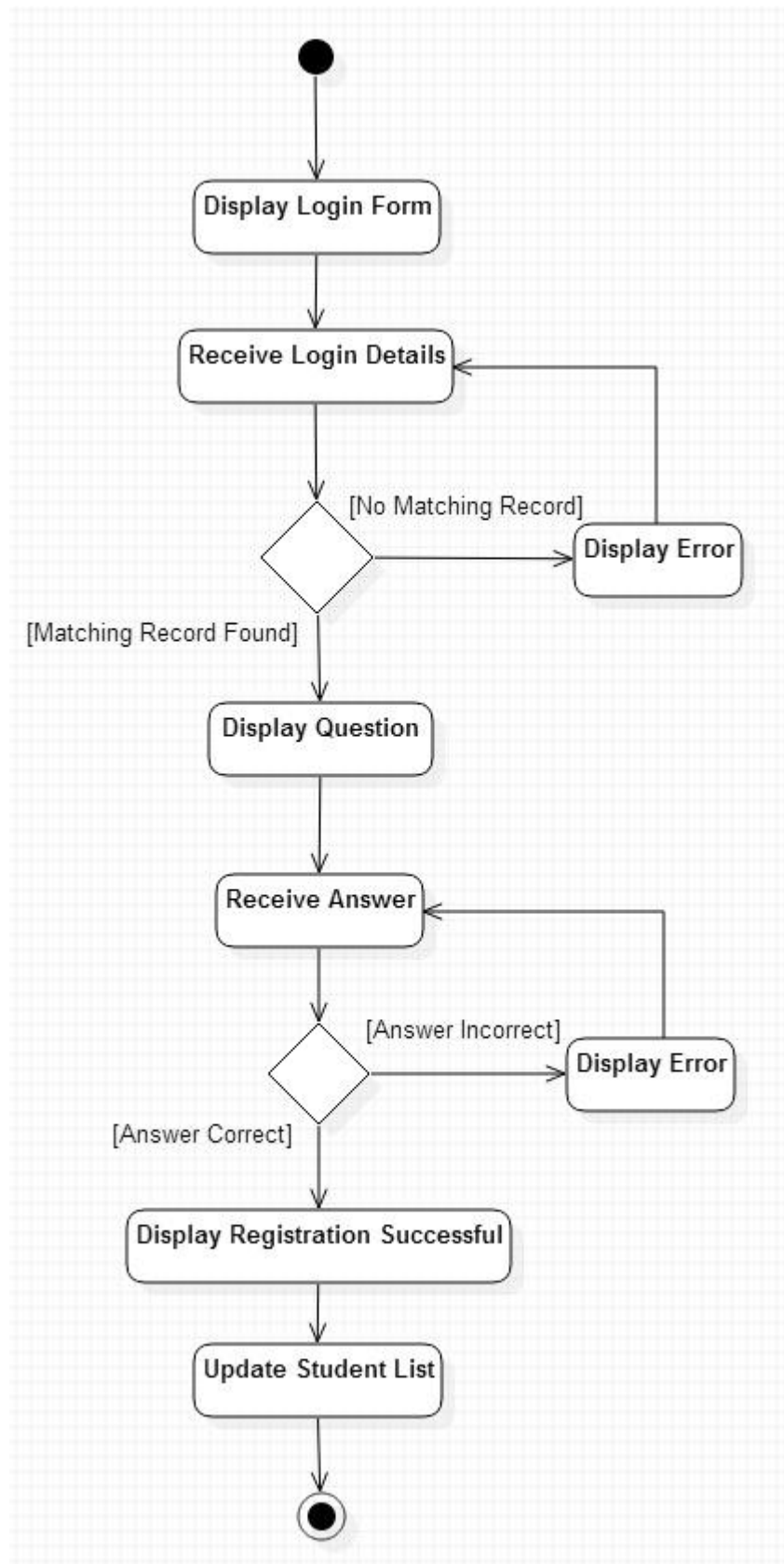


Figure 9: Activity diagram for the system.

4.3 Implementation

The program was written in C# using Visual Studio as an IDE to take advantage of the .NET framework's WCF to facilitate the creation of a client-server system. A relational database was used for the system, coded in SQL and handled using Microsoft SQL Server. The user interface was made with Windows Forms and program-database interactions were again managed using the .NET framework.

A central concern in any database-interactive program is reducing the amount of database operations to as small an amount as possible: such operations take time and unless handled asynchronously can lead to lag in the program. Considering that this is a secure login system, handling the problem asynchronously was not a valid option as each step in the authentication process required confirmation. This program contains only two operations in its ideal sequence: one to confirm that the student exists in the database and if so to return all of their Question IDs and, if the first succeeds, a second one to return a random question and its corresponding answer (more on the questions later).

In the early stages of design it was originally intended to create separate serialisable objects for the Student, Question and Answer, but it later became apparent that this was overly complicated and that it would be simpler to amalgamate these objects into one (the StudQuest object) that would more simply map the relationships between them as modelled in the earlier ER diagram.

A point of complexity arose in choosing a question. To explain: were this system to be deployed in a real-world context, each student enrolled would have to choose several (at least three) of the security questions to give answers for; having given these answers which would then be stored in the database one question-answer pair would have to be chosen at random for each instance of the client run. This required its own database operation to retrieve all of the set questions chosen by that student (identified by their name and authenticated via password) and then to programmatically pick one at random, after which that Question ID could be used to select the question-answer pair that would be loaded into the returned StudQuest object.

Chapter 5: Analysis

The following results were collected from an online survey. The first portion was organised in the form of a Likert scale from 1 to 5, asking respondents their opinion on the security strength and comfort of use for a range of authentication methods. Figure 10 gives an example of the layout used for this part of the survey.

* 3. Please indicate how strong you think each form of authentication is (1 = very strong, 5 = very weak).

	1	2	3	4	5
Password	☐	☐	☐	☐	☐
Smartcard	☐	☐	☐	☐	☐
PIN	☐	☐	☐	☐	☐
Smartcard + PIN	☐	☐	☐	☐	☐
Face recognition	☐	☐	☐	☐	☐
Fingerprint scanning	☐	☐	☐	☐	☐
Voice recognition	☐	☐	☐	☐	☐
Iris scanning	☐	☐	☐	☐	☐

Figure 10: Screenshot of format used for survey.

Respondents were asked to fill this out twice: the first time for their opinion beginning the survey, the second after they had been given an informative excerpt to read concerning biometric authentication. This technique allows the Student's t-test to compare between the two sets of data to see whether receiving information on the subject would in any way change their opinion. To see the full tables of survey results please refer to Appendices B-E.

The first issue to be addressed is the small sample size: six respondents answered but one set was incomplete and was discarded. As such, the statistical relevance of these results is questionable. The age of respondents varied greatly over a range of 19 to 76 with a good distribution. When asked to rate their own level of computer literacy three out of five respondents gave the middle response of 3, perhaps reflecting the poor choice of asking such a highly subjective question. That being said, these results still point favourably towards a relatively diverse demographic even in spite of the small sample size.

	Password	Smartcard	PIN	Smartcard + PIN
Security		0.18695048	0.035242	0.186950483
Comfort	0.186950483		0.18695	0.186950483
	Face recognition	Fingerprint scanning	Voice recognition	Iris scanning
Security	0.310654148	0.31065415	0.035242	0.186950483
Comfort	0.5	0.352	0.035242	0.186950483

Table 3: Results of Student's t-test.

Table 3 displays the results of the t-test: the values displayed are the P values derived from the t-test with values for the security portion of the survey on the first row and comfort on the second for each form of authentication. Blank cells indicate no change in answers before and after, invalidating the P value.

Overall the P values are relatively high, indicating a lack of difference between answers before and after the informative passage. The consistent P value of 0.186... indicates a change of one answer by one scale point. The one outstanding exception lies in the values for the ‘Voice recognition’ category which shows the lowest P value out of all categories by a large margin, perhaps indicating that this technology is the least well-understood out of all those presented in this survey – although it is still higher than 0.01 so this cannot be said with any degree of certainty.

The second portion of the survey was split between questions that asked respondents about facts concerning biometric authentication and others that asked their opinion about ethical issues on the topic. Even a brief analysis of Tables 4 and 5 reveals some interesting trends.

	Biometric authentication requires equipment that makes it prohibitively expensive in comparison to other forms of authentication.				
Before	Don't know	FALSE	FALSE	Don't know	TRUE
After	TRUE	FALSE	FALSE	TRUE	FALSE
	If someone stole data from a biometric authentication system I had been enrolled in they could use that data to identify me.				
Before	TRUE	TRUE	Don't know	TRUE	Don't know
After	FALSE	TRUE	FALSE	FALSE	FALSE
	If someone manages to fool a biometric authentication system into thinking they are me that bars me from using it ever again.				
Before	Don't know	TRUE	Don't know	FALSE	FALSE
After	FALSE	TRUE	FALSE	FALSE	FALSE

Table 4: Results for the fact-based questions of the survey.

	I fear that biometrics could be misused by government, law-enforcement, commercial or other organisations to infringe on my human rights.				
Before	I agree	I disagree	I disagree	I agree	I agree
After	I agree	I disagree	I disagree	I agree	I agree
	Collection of my biometric data is necessarily an infringement of my human rights.				
Before	I agree	I disagree	I disagree	I disagree	I disagree
After	I agree	I disagree	I disagree	I disagree	I disagree
	The problem with biometric data collection is less one inherent to biometrics itself and more to do with whether or not one can trust the people collecting it.				
Before	I agree	I agree	I agree	I agree	I agree
After	I agree	I agree	I agree	I agree	I agree
	Should I agree to have my biometric data collected I would want to know what it was being recorded for and be assured that it would not be used for any other purpose.				
Before	I agree	I disagree	I agree	I agree	I agree
After	I agree	I disagree	I agree	I agree	I agree
	I think it should be illegal to gather biometric data on someone without their awareness or consent.				
Before	I agree	I agree	I agree	I agree	I agree
After	I agree	I agree	I agree	I agree	I agree
	I think it should be illegal to gather biometric data on someone without their awareness or consent - even if it may be suspected that the individual in question is a criminal.				
Before	I disagree	I agree	I disagree	I agree	No strong opinion / Don't know
After	I agree	I agree	I disagree	I agree	No strong opinion / Don't know

Table 5: Results for the ethical questions of the survey.

Answers for the purely factual questions tend to vary before and after the informative passage, suggesting that actual technical knowledge concerning biometrics is something that the average user either does not have or is uncertain about. When it comes to the ethical questions, however, there is almost no variance before and after whatsoever – only one respondent changed their answer, for the very last question. Given that ethics tends to be an area of very strong opinion that is based on a lot more than just technical data, it is perhaps not surprising to see such a lack of variation.

Chapter 6: Evaluation

Again, it is necessary to assert that the data collected, while accurately replicated in the results shown, cannot be considered statistically significant due to the small sample size. However, given that this is what we have to work with, one may draw these conclusions:

- According to the Likert scale portion of the survey, receiving additional data concerning biometric authentication did not greatly change respondents' opinions about the security or comfort of use of various authentication methods. This could mean a number of things: that the respondents were mostly sure of their answers to begin with, which would suggest that they know a great deal concerning the subject matter (unlikely given the next conclusion); that the respondents did their best to answer according to the limited data they already had and in a few cases revised their answers after the passage to something that they felt more closely fit the reality of the situation as it had been presented to them; that the respondents were by and large unwilling to change their answers from before and perhaps resented being asked exactly the same question so soon after the first instance.
- Answers to the technical questions suggest that the informative passage had a significant impact on the respondents' knowledge of technical details concerning biometric authentication. It is only to be expected that the average user would not be particularly well-informed of such details, although this begs the question of why answers to the first portion of the survey varied so little if respondents were so unsure of their technical knowledge.
- The ethical questions showed almost no variance whatsoever. It would seem that respondents were very much made up in their minds concerning the ethical issues of biometrics and that learning more about the technical aspects of biometrics had very little bearing on their ethical decisions. This suggests that the average user draws their ethical judgement from a much wider pool of data than mere technical considerations: the answer to the question 'The problem with biometric data is less one inherent to biometrics itself and more to do with whether or not one can trust the people involved.' which was unanimously 'I agree' indicates that the respondents do not have any innate suspicion of biometrics and rather judge the ethics of using it much as one might judge using any tool or technology.

This data seems to agree with the research on the point that users tend to be ill-informed about the systems they use, seeming to be content merely in their position as end-users without needing to know more about the system than is required to fulfil its function. This is understandable given that most users have other, more pressing concerns and may not have the time or patience to learn everything that they possibly can about the authentication systems that they use everyday, which only further emphasises the importance of educating users – not only about the technical aspects of the systems that they use and how to make them more secure, but also about the importance of learning such lessons in the first place.

As for the ethical aspect concerning biometrics, while it would appear that the respondents had a healthy suspicion for the purposes to which biometrics could be put (as indicated by the majority 'I agree' answer to the questions 'I fear that biometrics could be misused [...] to

infringe on my human rights’ and ‘Should I agree to have my biometric collected I would want to know what it was being recorded for [...]’) they had little fear about biometric technology itself. This reflects the tone of the majority of research on the subject: while it is necessary to be wary about its possible applications, only the most alarmist of parties would try to suggest that biometric identification and authentication is necessarily ethically suspect, shown by the one respondent who claimed that collection of their biometric data was necessarily and infringement of their human rights..

Overall, the responses were much as expected: the assumptions made at the beginning of the project matched up with the larger body of research and reached some very reasonable conclusions from the survey results. There were no notable anomalies to report.

One possible flaw of the survey that it would be advisable to improve before using it again in future is to provide more technical true/false questions and, most importantly, to do a better job of relating the explanatory text to them. In retrospect it has become clear that these questions were perhaps ill-chosen, especially in relation to the points that were actually discussed in the informative passage – linking these more closely would have added more credibility to the idea that the passage had an effect on respondents’ knowledge.

Secondly, a much larger sample size would have been desirable. This was an unfortunate restriction of the time left to complete the project and which, on a better-planned repetition, may be better implemented with more time for respondents and a better plan for attracting them. As it was, the potential respondent pool was fairly low to begin with and the time given to them to respond could not be considered sufficient by any means.

Chapter 7: Conclusions and Recommendations

The aims and objectives of this project have changed significantly from the original plan. That being said, the scaled-down version of this project has still achieved some of the original objectives: research has been conducted into authentication methods, refining the focus of the project from authentication in general to biometric authentication and its ethics in particular; a system has been designed and built, using authentication to emulate a class register logging-in system, albeit not a system that contains biometric authentication; a survey has been conducted into user perceptions of authentication, biometrics and the ethics surrounding them and ascertained that user knowledge of authentication methods tends to be lacking, although the ethical standpoint towards biometrics can be best described as wary but not hostile.

Considering the reduction of this project, the most obvious recommendations for future work are to achieve the original aims and objects primarily set out. The most notable room for expansion lies in the development of the system at the centre of the project: currently it only has knowledge-based authentication, so adding forms of token-based and biometric authentication as well would add to its diversity. Such a fully-featured system could be used in experiments to ascertain both the technical efficacy of these different forms of authentication, opening up more opportunities for comparison with the research, as well as perhaps providing a different avenue for a survey that is instead intended to accompany the system and gather data regarding the user experience.

Chapter 8: Reflections

Possibly the most telling lesson I've learned from this project is that it is impossible to overstate the importance of the critical path. As Doctor Glenn Jenkins pointed out in my interim viva, the success of this project rested almost entirely on the one unknowable quantity in my plan – that is to say, the third-party fingerprint scanner and API that I planned to use. As a result of various complications including a late delivery date, some very odd design decisions on the part of the company that made the API and a lack of any useful documentation, actually integrating the scanner into the system turned out to be beyond my capabilities. Once the critical portion of the plan fell through everything else had to be downscaled accordingly. I will be a lot more cautious about using unknown software or devices in future and where possible will try to research it thoroughly before time commitments are made, while there is still time to correct such mistakes.

A lot of my failures concerning this project have come down to a lack of planning and clear direction on my part. I began the year with such grandiose ideas for what I might achieve. Perhaps this is also a lesson to be somewhat more conservative in my goals, at least until I know what I can realistically do.

On a more personal note, I would like to mention that this past year has not been a particularly easy one for me. My supervising lecturer Tim Bashford is well-acquainted with the problems I've had to face this past academic year and can account for the toll it has taken on me. I take it as a testament to the fortitude I've developed over the past few years that I was able to persevere even in spite of these troubles. If there is a lesson to be learned here, it is that one should never underestimate the value of endurance; the willingness to persevere even in the face of greatly discouraging circumstances. That being said, I would most surely not have made it as far as I have without the constant support of the faculty, whose unrelenting kindness has allowed me to continue even in spite of the misfortunes I have suffered. It is said that experience is the best teacher: from it I have learned that there is no shame in accepting aid from those willing to give it and that the satisfaction one may garner from facing such challenges on one's own is a cold comfort by comparison – if indeed such a task can be completed on one's own at all. I hope that this will help me in any future endeavours that require close co-operation with others and that I will be able to acquit myself with proper consideration when others come to rely on me.

I owe so much to so many, knowing that I may never be able to repay my debts in full. I have heard it said that the best way to repay kindness is to achieve the potential they saw in me, a prospect that I fully intend to realise. Even so, I hope that I have made my gratitude clear to all that deserve it. I will endeavour to ensure that your faith was not misplaced.

Chapter 9: References

- [1] L. Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2020–2021, 2003.
- [2] C. L. Paul, E. Morse, A. Zhang, Y. Y. Choong, and M. Theofanos, "A field study of user behavior and perceptions in smartcard authentication," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6949 LNCS, pp. 1–17, 2011.
- [3] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999.
- [4] M. J. Quinn, "Analysis of Real-World Passwords for Social Media Sites," 2015.
- [5] A. C. Weaver, "Biometric authentication," *Computer (Long. Beach. Calif.)*, vol. 39, no. 2, pp. 96–97, 2006.
- [6] D. Flo Encio and C. Herley, "A Large-Scale Study of Web Password Habits," pp. 657–665, 2007.
- [7] a. Conklin, G. Dietrich, and D. Walz, "Password-based authentication: a system perspective," *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 00, no. C, pp. 1–10, 2004.
- [8] C. Braz and J. Robert, "Security and Usability : The Case of the User Authentication Methods," *Proc. 18th Int. Conf. Assoc. - IHM '06*, pp. 199–203, 2006.
- [9] R. W. Proctor, M.-C. Lien, G. Salvendy, and E. E. Schultz, "A Task Analysis of Usability in Third-Party Authentication," *Inf. Secur. Bull.*, no. April, pp. 49–56, 2000.
- [10] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *Circuits Syst. Video ...*, vol. 14, no. 1, pp. 4–20, 2004.
- [11] F. Monrose, M. K. Reiter, and S. Wetzels, "Password Hardening Based on Keystroke Dynamics," *ACM CCS 99*, pp. 67–76, 1999.
- [12] N. Bartlow and B. Cukic, "Evaluating the Reliability of Credential Hardening through Keystroke Dynamics," *Int. Symp. Softw. Reliab. Eng.*, pp. 117–126, 2006.
- [13] S. T. De Magalhães, K. Revett, and H. M. D. Santos, "Password secured sites - Stepping forward with keystroke dynamics," *Proc. - Int. Conf. Next Gener. Web Serv. Pract. NWeSP 2005*, vol. 2005, pp. 293–298, 2005.
- [14] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, 2006.
- [15] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition," *Ann. Phys. (N. Y.)*, vol. 54, no. ISBN: 978–1–84882–253–5, p. 494, 2003.
- [16] N. Miura, A. Nagasaka, and T. Miyatake, "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Mach. Vis. Appl.*, vol. 15, no. 4, pp. 194–203, 2004.

- [17] J. Hashimoto, "Finger Vein Authentication Technology and Its Future," *2006 Symp. VLSI Circuits, 2006. Dig. Tech. Pap.*, vol. 00, no. c, 2006.
- [18] W. Zhao, R. Chellappa, P. J. Phillips, and a Rosenfeld, "Face recognition: A literature survey," *Acm Comput. Surv.*, vol. 35, no. 4, pp. 399–458, 2003.
- [19] A. Alterman, "'A piece of yourself': Ethical issues in biometric identification," *Ethics Inf. Technol.*, vol. 5, no. 3, pp. 139–150, 2003.
- [20] M. Sutrop and K. Laas-Mikko, "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics," *Rev. Policy Res.*, vol. 29, no. 1, pp. 21–36, 2012.
- [21] L. a Jones, A. I. Anton, J. B. Earp, and A. I. Antón, "Towards Understanding User Perceptions of Authentication Technologies," *Wpes '07*, pp. 91–98, 2007.
- [22] J. Wickins, "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification," *Sci. Eng. Ethics*, vol. 13, pp. 45–54, 2007.

Appendices

Appendix A

Feature/ Acquisition Device	Pass- words (PW)	PIN	Proxi- mity card	One Time Gener- ators	Chal- lenge Re- sponse	Multi- func- tion card	Pub- lic Key (PK)	Ker- beros	Finger print or Hand or Face	Voice	Sig- nature	Reti- na/ Iris	Key- stroke Rec- ogni- tion	Under- the- skin ID chip
Definition	Know- ledge based 8 to 12 digits	Know- ledge based 4 dig- its	Authen- tication Token	Authen- tication Token	Authen- tication Token	Authen- tication Token	Cryp- togra- phy (PK and PRK)	Key Distri- bution Center	Bio- met- rics User scan- ning	Bio- met- rics User voice when speak- ing	Bio- met- rics Lengt- h/ width h pen- pres- sure	Bio- met- rics Pat- tern of blood vessels	Bio- met- rics User's typ- ing rhyth- m	RHD based
Advantages	Ease of de- ploy- ment	Net- work- less	Last longer (con- tact- less)	PW diffi- cult to guess	No syn- chro- niza- tion	Built- in dy- namic data process- ing	User creden- tials once per login session	Mu- tual Authen- tication	Ease to col- lect	No PWs	High defi- nition graph- ic	Un- chang- eable (life- time)	No en- rolment	Forged, steal chip is pretty hard
Disadvan- tages	Can be for- gotten	Can be for- gotten	Theft, fraud, coun- terfeit	Brute force, dic- tion- ary attack	Users shares their ac- cess permi- ssions	Need of a smart card reader	PK is single point of at- tack	Scal- ability	Crimi- nal affilia- tion	Chan- ges over time	Can change signa- ture at any time	Exces- sive user coop- eration	Mas- quer- ade (spoof- ing)	Mas- quer- ade (spoof- ing)
Security	2	2	3	3	3	5	5	5	4	1	3	5	3	4
Usability	2 ¹	2	3	3	3	3	3	3	3	5	3	2	3	3
Human versus Automa- tism ²	4 ³	5 ³	5	5	5	5	5	5	1	4 ⁴	4	1	1	3
Data collec- tion envi- ronment	Com- puter- based net- work	Com- puter- based net- work	Site- based (Ac- cess Con- trol)	Com- puter- based net- work	Com- puter- based net- work	PK in- fra- struc- ture- based	PK in- fra- struc- ture- based	Distrib- uted- based net- work	Site- based (Ac- cess Con- trol)	Tele- com/ com- puter- based net- work	Com- puter- based net- work	Com- puter- based net- work	Com- puter- based net- work	RFID based
Input Process Time	7-20 secs ⁵	5-10 secs ⁵	2-5 secs ⁶	15s- 5m ⁵	15s- 5m ⁵	7-20 s ^{5,6}	7-20 secs ⁵	7-20 secs ⁵	< 5 secs ⁷	< 5 secs ⁷	5-15 secs ⁷	5secs -15m ⁷	< 5 secs ⁸	< 5 secs ⁹
Industrial Application	Unix [10], Win- dows NT00 /keyC hain	RSA Secur ID ¹⁰	Xy- Loc- Sage- ID, etc.	RSA, Se- cure Com- put- ing, etc.	Crypto Card, Ac- tivCar d, etc.	Ax- alto Gem- plus, etc.	Pretty Good Pri- vacy (PGP)	Ker- beros 5 Re- lease 1,3,2	Digital Per- sonna , Vi- sion- ics	Apple Mac OSX, Voice Secu- rity	Cyber Sign	Pri- vateID, Ex- cic, etc.	Net Nann y's Bio Pass- word	Not yet imple- mented [2]
Accuracy	AAS = 2 ¹⁵ to 2 ²³ (dic- tionary attack) [10]	AAS 13-bit [10]	Up to 10cm of the reader (fre- quency 13.56 mhz) ¹¹	AAS =2 ¹⁹ to 2 ⁶³ [10]	AAS =54 bit [10]	No avail- able data	AAS =102 4 bit PK=2 ⁸⁶ [10]	Clock syn- chro- niza- tion ¹² = 5 m	FRR =1 to 20%; FAR = 0,001 to 5% [10]	FRR =10 to 20%; FAR =2 to 5% [10]	FRR =2- try 10%; FAR =2- try 0,58 % [10]	FRR =2 to 10%; FAR ≥ 0,001 % [10]	Aver- age 98% rate in rec- ogniz- ing indi- viduals ¹³	No data avail- able

Table 6: Comparison of wide range of user authentication methods. [8]

Appendix B

Please indicate how strong you think each form of authentication is (1 = very strong, 5 = very weak).								
Password	Smartcard	PIN	Smartcard + PIN	Face recognition	Fingerprint scanning	Voice recognition	Iris scanning	
1	3	3	2	1	1	2	1	
3	1	3	1	2	2	2	1	
3	3	4	5	5	5	5	5	
3	2	3	1	2	3	3	1	
4	3	4	4	4	3	4	5	

Table 7: Results for the strength of security question before reading the passage.

Appendix C

Please indicate how strong you think each form of authentication is (1 = very strong, 5 = very weak).								
Password	Smartcard	PIN	Smartcard + PIN	Face recognition	Fingerprint scanning	Voice recognition	Iris scanning	
1	3	3	2	3	1	3	1	
3	1	2	1	2	1	3	1	
3	1	3	4	5	5	5	5	
3	2	2	1	4	2	4	2	
4	3	4	4	2	4	4	5	

Table 8: Results for the strength of security question after reading the passage.

Appendix D

Please indicate how comfortable you would be using each form of authentication (1 = very comfortable, 5 = very uncomfortable).								
Password	Smartcard	PIN	Smartcard + PIN	Face recognition	Fingerprint scanning	Voice recognition	Iris scanning	
1	3	3	2	1	1	2	1	
1	1	1	1	3	2	3	3	
3	3	4	4	5	5	5	5	
1	1	1	1	3	3	3	2	
5	3	4	4	3	3	2	4	

Table 9: Results for the comfort of use question before reading the passage.

Appendix E

Please indicate how comfortable you would be using each form of authentication (1 = very comfortable, 5 = very uncomfortable).								
Password	Smartcard	PIN	Smartcard + PIN	Face recognition	Fingerprint scanning	Voice recognition	Iris scanning	
2	3	3	2	3	1	3	1	
1	1	1	1	3	2	4	3	
3	3	3	4	5	5	5	5	
1	1	1	1	2	2	3	2	
5	3	4	3	2	5	3	5	

Table 10: Results for the comfort of use question after reading the passage.

Appendix F

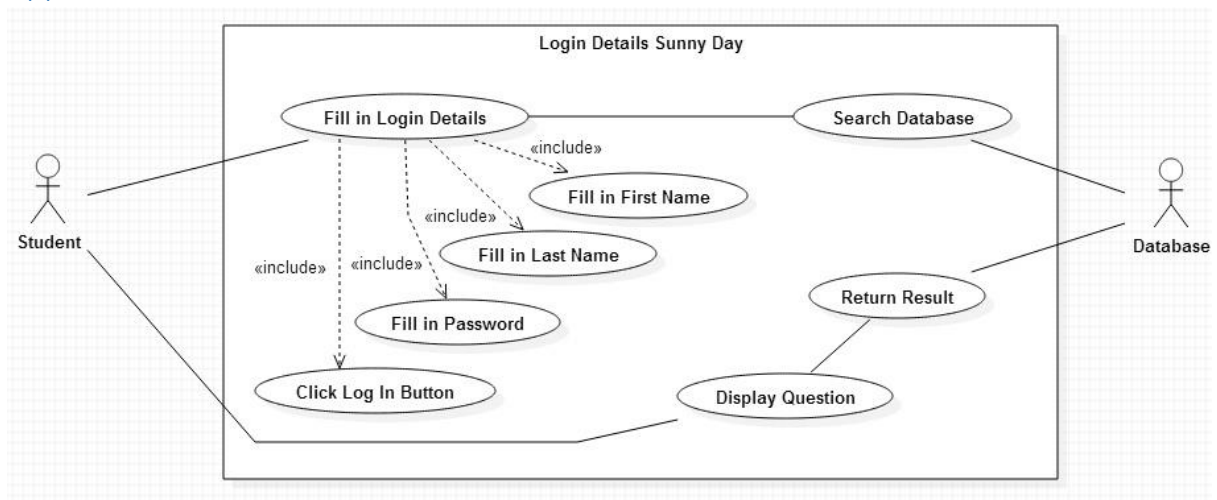


Figure 11: A decomposition of the login use case showing ideal operation.

Appendix G

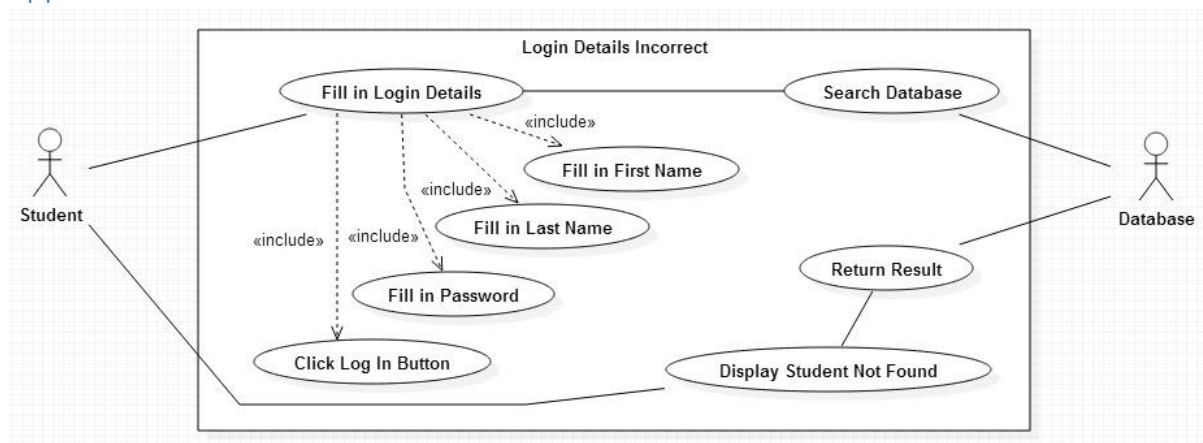


Figure 12: A decomposition of the login use case showing the 'Student Not Found' error.

Appendix H

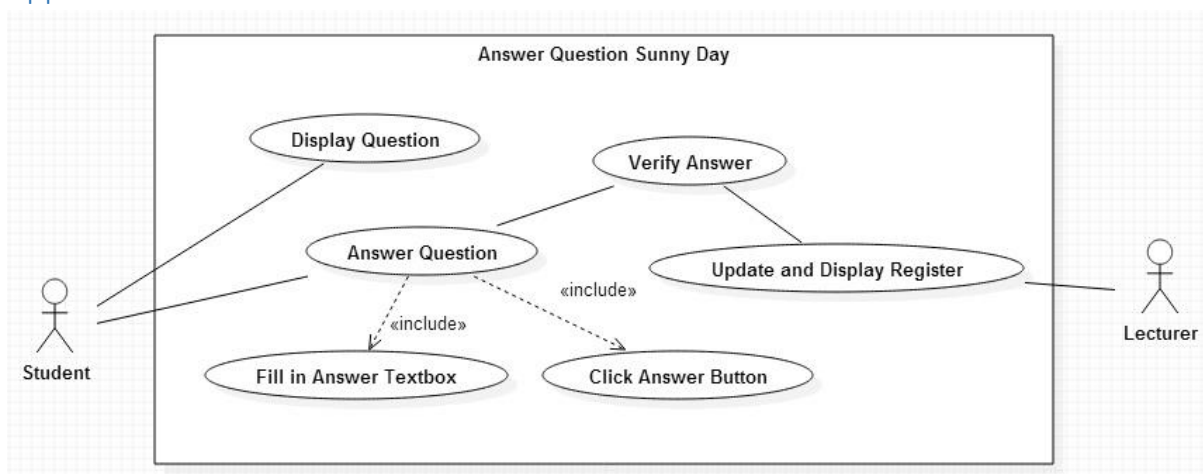


Figure 13: A decomposition of the security question use case showing ideal operation.

Appendix I

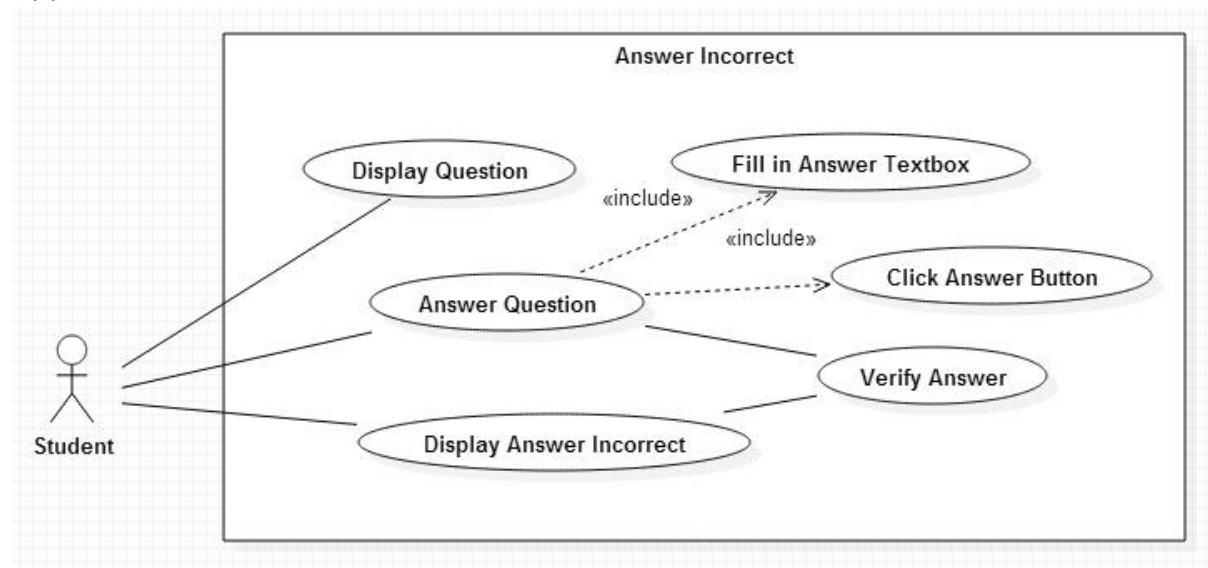


Figure 14: A decomposition of the security question use case showing 'Answer Incorrect' error.