Student authentication framework for Online exams outside of school

Alex Kristjan Urosevic

2019 Laurea

Laurea University of Applied Sciences

Student authentication framework for Online exams outside of school

Alex Kristjan Urosevic
Security Management
Bachelor's Degree
January 2019

Laurea University of Applied Sciences **Abstract**
Security Management

Alex Kristjan Urosevic

Student authentication framework for Online exams outside of school

Year 2019 Pages 38

This research projects aim was to find out how institutions can ensure correct identity when exams are done outside of school. The end user was focused on Laurea University of Applied Sciences upcoming full online implementation programme. Throughout the literature review, various authentication methods were gone through, such as: pin code, facial recognition, voice, keystroke, fingerprint, profile-based authentication, as well as hand geometry based recognition. The interviews were conducted using the semi-structured interviews approach, and the outcomes were analysed through thematic analysis. Three interviews were conducted at the Laurea University of Applied Sciences, with the focus group of interviewees having basic and/or fundamental knowledge in IT and authentication in general. The interviewee answers differed from those researched in the literature review to some extent; however, each received was somehow linked to one of the main topics of interest within student identity recognition. The most common topics of the thematic analysis allowed the researcher to identify key concepts and ideas that can be used later in maximizing not only security, but maintaining a peaceful environment for end users to complete exams. Certain trends were pointed out throughout the interviews, the main ones being: biometrics, security, data protection as well as two-layer authentication. Other key points, such as continuous authentication were mentioned, however, linked to for example two-layer authentication hand in hand. With technology advancing and changes being made each day onward, the use of mutli-factor authentication is highly important in order for the adaption to new scenes being made. If one method were to change drastically, the use of another method branching off can work until the other one is stable again. Having various options instead of one is the key to success when it comes to authentication and student identity recognition. With Finland having high tech institutions and good funding from the government, the transition to e-learning and online exams is something that is coming up at a rapid pace and is in good hands. Based on these findings, some recommendations can be made for the school when considering which approaches and methods to take. Keeping it simple, using two-layer authentication and obeying the general data protection regulations (GDPR) is the right path to take.

Keywords: Authentication, security, biometrics, online exams

Table of Contents

1 Introduction

Nowadays we are living in a hectic small world, where people are connecting more and more with each other using tablets, mobile phones, and laptops on the go. The need to keep up to par when it comes to education and ways of learning is becoming vitally important. In the year 2017 alone, there were roughly 23 million new learners online, boosting the total amount of e-learners to 81 million globally (Shah, 2018). The means of artificial intelligence and machine learning increasing at a rapid pace is pushing technology forward in all aspects of our society. Banking is already being done fully online as well as other day-to-day errands. Several setbacks have already been seen in online education due to it being out for not too long as well as the lack of human interaction taking place (Armstrong, 2013). Biometrics have already been implemented in airports, where travellers can pass border control independently with the use of high tech scanners. This shift has taken some time, and therefore represents the potential for online studies being possible. Citizens in this day and age, tend to be more busy and have tighter schedules; the means to educate and learn online is a great path for those lacking time to attend school lectures at a given location and opens gates for many that want to learn but cannot, as specific programmes may not be held in their countries. Within the e-learning environment and whole revolution to online implementations, the whole process involves content from different aspects as well as age groups and different cultures. Different factors such as speed and mobility to adapt to the given situation rely on the hands of the end user (student), to handle. (Sanna et al., 2017, 374). Finland is leading in the field of education, having thousands of international students visit and complete degrees, and has great potential to become the leading country in e-learning. This brings up the important topic of authentication and student identity recognition (Pollari, 2013).

The following research will be based and focused for the Laurea University of Applied Sciences. With the transition to e-learning and online degree programmes offered by the school, the researcher was asked by the school to conduct a research on possible authentication methods that can be used to ensure correct identity in online exams done outside of school. A meeting was held prior to the start of the research, with goals to suggest possible authentication methods that have been used in the past in different schools around the world. The goal was to mention and research about some of the harder possible identity recognition methods, for the school to have a broader picture and greater variety of choices to choose from when creating the infrastructure of given exam environments.

1.1 Research Question

The following research will be conducted and focused around a few main key points with the following being the research question:

How can institutions ensure correct student identity with the use of different authentication methods when exams are done outside of school?

According to Shah (2018), more than 800 universities around the world have implemented online courses and the number is rapidly increasing. The need for teachers and staff to know what is being done at home, as well as monitor and ensure that the correct person is doing the exam, is not only important for the school but also for the students learning path. Doing exams in groups as well as using books or different resources to answer questions, does not show knowledge about a subject, but rather shows the capability to extract information from a small or large text in given time (Littlefield, 2017).

The reason why exams are done alone in classrooms and not in pairs, is simply to determine if a student has understood a given topic, and for them to extract what they have learnt and put it on paper. The same way goes for when trying to implement online exams, and even full time degrees. The need to know if a given person is really the right person doing an exam, is highly important not only for the sake of the examiner knowing, but for the students future. Unethical approaches when learning, can lead to bad approaches in life where going the easy way around might not always be the right way and can lead to bad outcomes. Exams can be conducted in various ways, with differences from one another if in groups or individually. The use of groups allows the teacher to present his/her thoughts faster, rather then going one by one individually (Lelei 2015, 5).

The original idea for this report started during the summer of 2018, and stretched out to mid October, where a supervisor reached out and agreed on working together to bring out the importance of this subject. Roughly a month and a half was given for researching theory and writing the literature review. With the literature review being done, another month to a month and a half was marked to complete all interviews and analyse them as well as write them out in the 'own findings' area. The completion of this thesis is set to be late January 2019.

1.2 Key Concepts and methodology

The research will focus on four different areas of interest regarding online exams done outside of school. Authentication, security, biometrics, as well as online exams all play a key role when thinking about focus key concepts in the report. All of the concepts above link together and paint a bonded picture about the most important fields that are gone through below.

The objectives are to identify the different biometric and authentication methods clearly throughout the literature review, and from there see how we can ensure correct identity for each student completing exams. Each and every key concept somehow links with one anoth-

er, bonding and making a clear picture of what the thesis is broadly about, as well as shows the most important factors that one must follow when reading along.

Methodology used to conduct this thesis is based around the quantitative research framework. The use of audio recordings as well as the interviews being semi-structured clearly wraps up and focuses on qualitative research. The reason behind this being that the subject is quite new to many. Interviewing a large amount of people such as students might not work out, as they will not know possible different authentication methods, compared to experts in for example the IT field.

2 Literature Review

With technology advancing and almost everything being shifted to the Internet, one must understand the need to keep up to date as well when it comes to education. More and more universities and study groups are shifting to the web, not just because of the need to keep up with technology, but the fact that it can be more useful in the near future. Digital material can be updated at all times and edited when online. This brings to the picture that in many cases, information from lectures that are given with the help of textbooks may be out-dated. Various ways of teaching have been implemented already in the online infrastructure, with use of for example podcasts as well as streaming video. (Lehmann et al., 2009, 13).

One of the most important factors of learning in a group or classroom with a teacher is the need to interact. Students must be active learners. In many cases, classrooms are packed with tens of students, and it is a fact that a teacher cannot keep up to date with what each and every student is doing at any given time. On the other hand, with the transition to e-learning and online exams, the student must interact with the database in order for it to know that the student is awake and following what is going on. This is one great factor that is doable with online learning and implementing courses online, that cannot be always done in classrooms. The diversity and need to use different skills is vital when considering being active learners (Anderson, 2017). Critical thinking as well as decision-making is totally different in e-learning compared to learning in a classroom (Pappas, 2015). The key to success comes from hard work and dedication in what is being done, and then later on tested through exams. This brings up the great subject of online authentication and student identity recognition. It is highly important for a student to be able to show and tell what they know in an honest way. Therefore, there are various different authentication methods that can be used by examiners at home, to make the staff and teachers know that the right person is taking the exam and not someone else. Various methods such as blogging, screen casting, as well as the use of audio can help teachers identify and keep track of who is doing an exam at a given time (Kang et al., 2015, 47).

2.1 Authentication methods

Previous decades have witnessed an increased amount of interest and need in authentication in many fields. Passwords being arguably the most commonly used type of authentication, however not being the smartest choice of interest if kept simple and not change frequently. Passwords do not simply provide enough identity check to be stated as a good and authentication that is enough to use by itself (Dacanay, 2017). Hackers on a daily basis try to bypass certain standards and extract information that is not initially meant for them to see in the first place, by using various different methods such as cracking codes or phishing. Various authentication methods can be used to help identify student's completing exams done at home. Pin code, facial recognition, fingerprint, keystroke, profile-based authentication, as well as hand writing biometrics are all examples of good ways to ensure student identity. Security is highly linked to each and every one of the authentication methods above; as there is always a chance that personal information can be leaked or stolen throughout the use of these methods undergone at home. The need to properly educate staff and those on the back end of the degrees given, as well as have strong backup systems to provide in case of the primary ones failing is vital (Mening, 2017).

Establishing the identity of a person is a critical and very important task in almost any scenario on the web. As mentioned in a article called "A framework of Secure Biometric Based Online Exam Authentication: An Alternative to Traditional exams" (Ramu et al., 2013, 53), surrogate representations of identity such as ID cards are not sufficient enough as they can be easily misplaced, shared, or stolen. The biometric system as a whole works simply in a way where one must log in and implement data to a certain standard, multiple times. The data is collected and stored in a database and can be used to scan possible outcomes in later log ins. Algorithms are then used to track and see if similar tracking's are found. Through this we can find and see if they match the individuals physical or behavioural characteristics (Ramu et al., 2013, 54).

2.1.1 PIN Code

Each pin code that one has, must be of a kind that is not easy to access. With modern day hackers and people spoofing around for other people's information, having a simple pin code will get one nowhere. In many cases, passwords have been left out and instead pin codes have been used. A 4-digit number can mean the world to someone, with all of their personal information stored behind it, or even important business' or school projects. Pin codes can seem very simple and easy to guess, and therefore one should never use significant dates, any part of their address, or social security number, as it can help guess what the code could be (Pritchard, 2019). When considering online exams and multi layer authentication, it is highly important to start off from the basic authentication methods such as PIN Codes and passwords, and slowly work your way up to more difficult ones. The more layers of authentica-

tion, means the likelihood of having your information leaked to someone else decreases as security increases. “The use of PINS has grown with the popularity of mobile devices” (Keeper security, 2017). Exams are being done in this day and age on tablets and even mobile phones, and the need for good PINS and not simple ones is increasing drastically. Something that many people do not take into consideration when thinking about pins is the fact that only a certain amount of entry’s can be attempted before locking the system for safety reasons (Keeper security, 2017).

Variations of pin codes in this day and age exist through two-layer usage, with the help of modern day phones. The pin codes that are asked to enter are at the second layer of authentication are found through a text message received by the third party security provider. The reason behind the hand held message four digit pin code is the fact that the first set of pin codes one may enter can be easily guessed in many cases, therefore having the second set of numbers always generated randomly through a text message (Oberhaus, 2018). If such third party security is used for double layer pin code authentication, one must understand the need to have a mobile device at hand at all times. Security being at stake with a security code at access through the message, the pin code received will only last in most cases for two to three minutes before being blocked. The given pin and both layers of access must be at all times linked to a same device in order to not have problems with data protection. If a given laptop or mobile device that the pin is set to is stolen for example, total productive maintenance (TPM) anti-hammering protection lock kicks in for an additional security level of protection. Various other plug ins are for free on the web and these can also be used to secure additional layers. All in all, pin codes are a great way to ensure security, do not require much set up, and are cost sufficient (Halfin et al., 2017).

2.1.2 Facial Recognition

Facial recognition plays a vital role when trying to identify a student working outside of school on an exam. Cheating by doing exams in a group is something that is highly occurring on a daily basis around the world. One can be doing an exam on their own, according to them, but in reality there can be someone next to them helping them out and giving them suggestions on what could be the possible answer. Gallery size, consistently using the same camera, as well as the surrounding environment where the video camera is being held, all play a vital role when trying to identify a student in different exam sessions (Introna, et al., 2010, 3). A survey conducted by Fayyoummi, showed that with the implementation of facial recognition, the likelihood of cheating would decrease (Fayyoumi et al., 2014, 15). With the survey branching off to seek facial monitoring with the main focus on virtual classroom attendance, users tended to focus and stay recognizable in the camera to get a grade as being present. The survey in general showed that students wanted to do exams in a honest way, and therefore mitigate the chances of getting caught by looking at their own paper and not

left or right when having the camera on. The quality, lighting and imaging process must be up to standards at all times when undergoing facial recognition procedures. It is doable to complete facial recognition under ease with cheap cameras, however the outcome will be in many cases not as good and harder for the algorithms to match together and identify a given student (Serra 2017, 8).

With the development of cameras in phones as well as computers and ipads, the use and capability of using such facial recognition is becoming slightly easier. Facial recognition programmes and systems have been made in the past years by many companies, with most following a similar procedure on how to recognize faces. Four essential steps are used in the process, feature analysis, neural work, eigenfaces as well as automatic face processing. Each and every procedure is done with care, as a slight mistake in capturing an imagine can give wrong results. Each human having roughly eighty different unique features in their face, makes it even harder for accurate outcomes. Fortunately technology is so up to date that it can use algorithms and trends in past implementations to help in current facial monitoring (Liao et al., 2016, 2-3). Quality of imaging as well as recognition with ease has developed in the previous years and is still increasing at a rapid pace. Previously 2D imaging was used for facial recognition in almost every field; now technology is increasing the likelihood and capability of screening with 3D imaging, thus getting a larger and broader picture of a face. Emotional status can determine ones facial expressions, with various facial landmarks and variations possible. Each and every scenario must be recognizable, with different situations where a student may be happy, sad, or just with no expression on their faces (Ayvaz et al., 2017, 98-99).

2.1.3 Fingerprint

Authentication has always been a major issue, ever since the first release of online exams. The verification of a student's identity is not an easy process, and requires time and several procedures to conduct. The design and initial idea of the fingerprint based hall authentication is to scan a given students finger and only pass those accepted and deny all others (Ingashitula, 2017, 1). The cost and deployment of many techniques used to identify a student's identity are not cheap, and the lack of fixed standardization in many methods can easily lead to different algorithm results, making it very difficult to be compatible. Fortunately, this has advanced and the means to increase security measures has drastically become a bigger concern for software developers. Hygiene, as well as culture differences and ethical issues bring up a huge concern when considering fingerprint recognition in public. Fortunately with the shift to online implementations of studies, each student has their own fingerprint scanner that is connected to their home or portable devices, cancelling out such problems that may be in place if many people use a shared scanner (Saheed et al., 2017, 47). Since the start of online exam implementations, fingerprint recognition was used as it was easy to implement

and cost effective, not only for students but as well as the institutions providing the exams (et al., 2010, 93). Fingerprint recognition has also been so high tech in the past that there have been keyboards that have fingerprint recognition implemented in them. The need for an external fingerprint recognition scanner is unnecessary, as everything is in one set on a keyboard (Alotaibi 2010, 5).

Fingerprint scanners can be found in various different sizes, as well as quality differences, leading to major variations in costs between each product. Optical scanners are the first type of fingerprint scanners that have been used, and can still be used in the future for student exam identity recognition. Such scanners are used in for example, phones to gain access and unlock a code, and have been sufficient so far in that others cannot bypass such passwords. More up to date variations of fingerprint scanners are the captive scanners that are seen more these days. Some high tech and new phones use these scanners as well, making them more accurate due to not only creating a traditional imagine of a finger, but digging deeper and using time arrays to seek more detail images of a finger (Triggs, 2018).

2.1.4 Key Stroke

Keystroke recognition has become a commonly used biometric authentication method throughout many different fields online. Research on keystroke recognition has drastically become a more important matter in the last decade, as experts have realised that it is economical as well as the fact that it can be integrated in modern day computers easily. With keystroke not having anything external and it being a software implementation used, it is one that can be used with ease (Teh et al., 2013, 1). In order for such recognition to take place, information must be gathered through previous inputs in the system, in order for recognition to work in later sessions. Keystroke dynamics or recognition refers to an automated method of identifying a person through the rhythm of typing. Enough inputs must be implemented as many students in this day and age type at similar paces. Multi-factor authentication has been used in the past with keystroke recognition for online exams, mostly being combined with the more basic biometric type such as passwords, pin codes, as well as continuous profile based questions throughout the exam time. Keystroke recognition has been proven to be an ideal implementation for online exams as it works in two parts to extract the most out of its security matters. Dwell time, as well as flight time provides the whole infrastructure of the concept. Dwell time meaning the time and duration a key is pressed, and the flight time being the duration in between releasing a key and pressing the next one. Interestingly enough, key stroke recognition can also spot out the use of the frequency and use of other functions on the keyboard such as the number pad or function keys (Das, 2004).

Machine learning techniques have been implemented and used in keystroke recognition as well. The new way of identifying trends by implementing enough data to a system where it can later on seek specific patterns and make outcomes, is a newly developing infrastructure

that can take e-leanring to a whole other level when it comes to student identity recognition. Possible facial recognition as well as voice recognition can be bypassed, and not used if machine learning is set to develop in e-learning in the near future. The use of such trends and ways one writes can easily be detected by a system. Machine learning techniques have been already set and used to some extent, however, at the moment are quite limited as to what trends they can capture and render (Tsimperidis 2018, 1).

2.1.5 Profile Based Authentication

With the rapid increase in online users, universities and course makers must choose different methods to implement in their study groups, on how one will identify them throughout the elapsed time an exam takes. Using such methods as facial recognition as well as fingerprint or key stroke recognition can be a financial burden for many, and therefore other methods such as profile based authentication can be used. Depending on what the topic is, in many cases, profile based authentication can be enough and higher-level security measures may not necessarily be implemented. The execution and use of reliable and secure approaches is extremely important to ensure stakeholders trust in the final assessment process of the exam (Ullah, 2012).

Profile based authentication is one of the more simple methods used to authenticate students doing exams, where they possess user ids, passwords, as well as challenging questions (Ullah 2014, 220-221). To begin, a user can simply log onto their account using a password or Pin. The next phase is where the profile-based authentication kicks in; it is initially during the learning environment at unknown times. The database asks the student during the learning process profile questions in order to proceed with studies. At each given time when the student wants to access an online exam profile, more difficult questions are asked and collected and stored in the user profile interface. From one challenge and question to another, the profile is slowly grown and can be expanded drastically to increase questions that can be asked in the future through this authentication method. The questions asked are not directly about the exam, but can rather be related to the student's interests, hobbies, or other personal related topics. A research conducted at the University of Hertfordshire, showed that after having a certain amount of students undergo a exam with profile based authentication happening throughout the exam, many failed to provide correct identity. The reason behind this being that the initial information that was gathered in the system did not connect with the syntax of the questions. Problems occurred when students answered longer questions using more words than just one, mixing up the infrastructure and not having the database understand their answers (Tryfonas et al., 2015, 133-135). Without doubt, profile based authentication is still up to date one of the most frequently used ways when trying to identify an individual online (Salameh 2015, 169-170).

2.1.6 Hand geometry based biometrics

Verification and identification are two different parts in regard to the big picture. Verification meaning authentication, the problem of denying or confirming a person's identity. Identification being in other words "who am I", the challenge being establishing a given persons identity. With there being no specific correct way of identifying anyone while doing an exam, linking methods together can be more effective, especially when doing an exam. Continuous or on off authentication is vital. The fact that hand geometry and recognition is not that complicated and the geometry measurements easily collectible, helps play a key role in considering the most applicable authentication methods for examiners. Having a flexible approach and easily implemented with different biometrics, hand geometry based biometrics can be linked with fingerprints to pursue a great and secure method of identity recognition while doing exams. Fingerprints can be used for infrequent identification, where as on the other hand geometry based biometrics can be used for more frequent checks (Ross, 2007). The use and power of implementing two biometric systems not only increases the means of authentication, but gives a diverse approach in case one method does not work for example due to a technical error. All in all, the base and use for hand-geometry devices is quite simple. (Struc 2015, 2).

Multi-touch enabled touchscreens on ipads, and different high-tech phones have been used in the past to help identify citizens when in need. Length being an important aspect of hand based geometry recognition, repetition as well as consistency in similar swipes is ideal and vital for correct identity recognition (Song et al., 2017, 359). The finger, width, thickness, as well as curvatures distinguish each human from one another. Each human having certain trends and ways of writing differentiates one another from each other. The use of such system operation that can detect if one student is linked to their hand based geometry profile is highly in construction and in need of new implementations and lots of data gathering capabilities. Certain setbacks drain the chances of institutions using this type of authentication as geometry scanners, good cameras, as well as good lighting all cost a lot and require great deal of attention when setting up (Zunkel et al., 2017, 2-4). Hand geometry systems have the longest implementation of biometrics in the history of recognition. The procedure of identifying a hand is accurate, however, requires more time than some other biometric methods. Hand geometry system uses the camera while a hand is placed on a plate palm down, guided by five different pegs that sense a given hand. This type of authentication method is therefore not as good as some other methods to identify student's hands online in online exam environments. Such a method can be easily implemented and used however with other methods to form a solid structure and multi-authentication base (Mayhew, 2012).

2.1.7 Voice Recognition

Voice recognition is defined as the ability and use of computer analysis to interpret words and phrases meant to identify an individual's voice (Oxford Dictionary). Voice recognition has been a vastly growing field, spanning in different areas such as computer science as well as mathematics in order to reach its main purpose of recognizing the correct persons voice. The reliability of programmes speech recognition has shown to be a problem for many companies; however, experts have been able to reach good accuracy when testing programmes (Rudrapal et al., 2012, 6). The imagination and interpretation of secure systems regarding voice recognition has advanced greatly in the previous years, combining superior digital as well as mathematical knowledge to identify humans through voice patterns (Koirala 2013, 3). Google has already imbedded many voice recognition tools into their tablets as well as phones. The implementation of voice recognition is doable in this day and age for exams online, however, with googles services that can be used, the amount of words in specific subjects may be limited. Home and wellness category being the leading field, as google first focused on home based gadgets that can be used through voice recognition. Science and education being the last place down, a whopping four times less words found in this category known by googles voice recognition programme. With Google updating these modules, voice recognition can work with ease, as new punctuational models are being developed each day (Lardinois, 2018). Other companies such as Microsoft have also created software to help develop automated speech recognition (API). Various problems emerge when considering authentication matters regarding voice recognition. A person's voice may change from day to day if one gets a flu, changing the way they pronounce words. In order for voice recognition to work, a numerous amount of voice profiles must be implemented in order for the system to easily identify who is speaking at a given time. Grammar can also effect the way a system understands what a student is telling, making it difficult and in many cases, slowing down the pace of the exam. Voice recognition being a bit of a tricky biometric method used for recognition, can still have great potential when considering the vastly growing field of Artificial learning as well as machine learning (Rai et al., 2017, 2938-2939).

2.1.8 Two-factor authentication and its importance

The use of digital devices and the internet creates a gap for those who are in the will or need to exploit the school rules and bypass the traditional and correct way of completing exams (Kigwana 2018, 2). Education institutions around the globe have tried to already make it harder for students to not cheat and use others help, however, results show that current efforts have been unsuccessful in most cases (Hylto et al., 2016). Many may consider student profiles in school databases not to be important, however, many hackers today tend to target unsuspected fields just to cause harm. Two-factor authentication plays a key role as it a system that creates additional security for an online account (Douthit, 2018).

When looking at the broad picture of the transition to online studies and exams, student authentication plays one of the key roles when considering security. The time and span where a hacker can take over what someone is doing is exactly when the procedure of authentication is being done, in case of vulnerability within the system. Passwords are arguably in many cases the leading cause of accounts being hacked or fraud occurring. Passwords are for many users a easy to remember set of strings, and for hackers in this case, a easy password to take over and guess (Dacanay, 2017).

The likelihood of something going wrong is much higher when only having one authentication method such as a PIN code when logging onto a system. The need to look around our surroundings and protect information as well as the infrastructure that we are working around is greatly in need of attention in our society. Teachers and staff in school must know that they are dealing with the correct examiner and exam at a given time; therefore, multi authentication methods come into place (Maring, 2018). PIN codes provide one layer of authentication when trying to access a database, and from there onwards one can be free with what they want to do when logged in. Without having a second layer of continuous or on/off authentication, possible results of cheating may occur. Just like working in a classroom on an exam, teachers walk around to see if people are looking only at their paper. This is repeatedly done throughout the take of the exam, and therefore the same approach must be implemented in online exams with the use of continuous authentication methods. One must consider that online exams can also have so called hick-ups and bypass a certain checkmark with an authentication method, leading to free access within the database or exam stage. Errors can occur within the framework of one particular authentication method, therefore, having access and control as an administrator of the exam, as well as capability to authenticate using a different method helps and brings a dynamic approach to security matters and student identity (Violino, 2017).

Time stamps when logging into a system have played a very important role when securing a users account. The factors that are mostly spoken about when considering multi factor authentications are the following: your memory, what you posses, as well as yourself (Ihalainen, 2016). With the shift to online studies and e-exams, the need to provide such possibilities for students to identify them in various ways and procedures, plays a key role in not only protecting the information of the end user, but also to keep the material of a possible exam secret. Multi-factor authentication can be easily implemented in online studies by including passwords, a possible multiple-choice question, as well as a fingerprint recognition identification stage. With identity fraud and possible unethical conduct still being a problem even with the use of multi-factor authentication, staff and teachers from schools can bump up security measures and decrease the chances of such problems coming into play with the use of many authentication methods (Bachmann, 2018).

2.1.9 Advantages and disadvantages of different authentication methods

Companies and organisations, as well as institutes, are considering using biometric authentication methods more and more as we speak. The need to secure the employees, staffs, as well as end users information is extremely important as private information may be leaked. The capability and use of voice recognition as well as fingerprints has emerged globally, with having identity recognition even working through tablets and hand held phones (Alton, 2018). PIN codes as well as profile based authentication methods have more positive than negative factors when considering simplicity and effectiveness, compared to the high tech biometric methods (Sukadarmika et al, 2016). Facial, hand, as well as voice recognition have been and will be always more accurate than authentication methods where biometrics are not involved (Advantages and disadvantages of Biometrics, 2018). Device limitations, modifications needed to be done, resets, as well as system limitations are all possible setbacks when biometric methods are used. With everything requiring technology as well as maintenance, not one device in our world can work with no error. The fact that there is space for error, can setback an examiner or student trying to complete something in a given time. Online exams in most cases have time limits, and the last problem a student wants to have is something to do with a technical error (Student and academic services, 2015). Advantages always come into play if the provider, as well as the end user agrees upon the use of biometric recognition methods such as facial recognition and voice recognition. As studies have shown, the use of biometric authentication measures at a multi-factor level, tend to provide very accurate identification of the end user as well as increase security measures (Cmarsden, 2015).

2.1.10 Matters concerning Data Protection Regulations

The General Data Protection Regulation is a legal regulation framework that sets rules and guidelines regarding personal data for individuals within the European union (Beattie, 2018). The increase in security and importance of securing data for schools has increased within the measures set by GDPR. Schools are in much better position fortunately at the moment compared to some companies and organisations, as they already store personal information about students, as well as are aware of who they are allowed to send information to and whom not to. Leaping a step forward, the new GDPR will set even more accurate regulations that schools must obey, with a big focus on what programmes to use and what not to use for students when attending courses. This will base a major effect on online studies and exams, as the programmes used must be accepted and meet the standards of data protection (Baines, 2017).

2.1.11 Costs

Online proctoring and the shift to online exams has boomed in the past years, many not being aware that the eLearning industry is now over a 100-billion-dollar business (Jose, 2018). E learning has as well shown to set unquestionable benefits to those willing to learn, creating

the opportunity for one to learn in flexible environments. In order for this to function properly, there are numerous amounts of concerns such as costs (Andriotis, 2017). The face to face environment has been implemented online, where students have lectures with teachers in a virtual online environment, however having it lack many structural models that could work much better, such as communication as a group (Bartley et al., 2004, 167). With the advances in technology and web-based monitoring, companies such as ProctorU provide services as a third party host while an exam is being completed. The use of a webcam, microphone, as well as an internet connection can seem easy to purchase, however, branch off to addition expenses each time a user needs to take an exam. ProctorU working as a third party user in exam environments, charge from 8 dollars up for a half an hour monitoring service (Kolowich, 2013).

2.1.12 Security Matters

An online exam system is a set of multiple or single software's used to assess a student's performance during the elapsed time of an examination. E-exams is not a simple system, compared to the standard way of writing exams in a classroom, involving various stakeholders such as the examiner itself, and the corrector in many cases the teacher (Sukadarmika et al., 2016). One may not understand the principle behind online exams, and the importance that security plays when undergoing exams. Different biometric systems may sound useful, however, implementing them and making sure data is secured is a whole different section to the ball game. The biggest threat while doing online exams or any work online in general, is the use of impersonation. (Karim, et al., 2015) Impersonation means the act of pretending to be another person for the purpose of fraud, in this case identity. According to research done at the Purdue University Global in 2009, with technology being not as advanced as today, teachers and staff already then realized that the implementation of various biometrics increased the grades that students got, however, also increased the amount of cheating. Another research conducted in 2013, at a university in the United States showed that the grades that students got were better online than those that they got at school, however, still did not meet the expected requirements for authenticating students as what the board had insisted (Sarrayrih et al., 2013, 440).

Issues concerning security evolve throughout the course of the exam, and therefore it is necessary to implement multi factor authentication and continuous biometrics in order to know the end user at all times (Perrin et al., 2012, 5). In order for the whole concept and idea of online exams to work, there must be participation as well as trust and motivation to use such services and programmes to complete exams (Chen, 2014). The main privacy concerns associated with biometrics relate to three different factors. The circumstances which biometric information is obtained, retained, as well as stored, bring up a big concern when it comes to Data Protection. The fact that many colleges and universities share information with one an-

other regarding student's participation in exam and the exams themselves, it is important to note that important student data is being sent across a large platform. In the United States of America, there is bill of rights and cause of action for the invasion of another person's privacy (Mann et al., 2017).

2.1.13 Unethical conduct in online exams

Unethical behaviour can be defined as going against what is set to be the correct way, breaking the law in some situations (Joseph, 2018). The best way to avoid any possible unethical conduct manners prior to and during the exam time is to think and take action with an honest mind-set at all times. Keeping ones eyes on their own task and not wondering around the room seeking for answers, as well as not having peers helping will lead to honest and morally acceptable answers. In case of possible open book exams conducted from home or outside of school, the look out and use of one's own thoughts is to be followed and to not have any signs of plagiarism (Iorga 2013, 55-56).

With the growth of technology and almost everything becoming more international, the unfortunate push towards unethical behaviour has drastically increased, especially in online exams or home based assignments in general. The fact that many universities and colleges provide online studies as well as exams, makes many pupils think that it is morally acceptable to cheat from others or plagiarize. Plagiarism has become one of the most noticeable parts of online exams for staff and teachers grading. Fortunately, with more and more surveillance being implemented, and the use of plagiarism detection, many tend to complete exams in an honest way (Martin et al., 2011, 88).

2.2 Third party surveillance

Solutions have been implemented in the past years for students to complete exams online in an honest way with the use of a third party programme. One company that provides these types of services is ProctorU (Kolowich, 2013). Many citizens around the world that are involved in the shift to online education are not aware of the fact that identity fraud is a highly important area of interest for hackers, and the fact that 100% correct identity recognition is only possible with the use of multi-factor biometric authentication. Within the past ten years, numerous amounts of universities and colleges around the globe have established online courses, later getting to know and realise that many students are taking advantage of this and cheating and causing fraud related problems (Bergstein, 2012).

2.2.1 Positive Sides to third party surveillance

Many are not aware that third party hosts are being implemented during exams; the tasks of identity recognition are divided to these professionals. A professional in a field knows what to look out for, when to interact, as well as fix possible problems. With technology advancing

and biometric solutions being implemented in certain areas, the need to know how to fix problems at given times increase. Students have one objective when undergoing exams, which is to successfully complete the exam in a given time. The use of authentication methods when taking an exam can easily slow down the pace, set a student off track, or even confuse them and mislead them in the wrong direction. ProctorU, a company that provides these services, has a setup that is simple and easy to follow which may wake up concerns for users as certain procedures must be gone through in order to establish and enter the database (Kolowich, 2013). Scheduling exams is simple with the aid of such third party companies such as ProctorU; this means that exams can be taken place at any given time during any day of the week. In order to proceed with the examination, one must calibrate the webcam and microphone, providing evidence to the person monitoring that one is alone in a given room and that nobody else is helping throughout the exam (ProctorU 2018, 3-5). The most important factor and how the person watching one do an exam can excel, is by watching the motion of ones eyes when doing an exam. In many cases, the students have also a monitoring sharing system, where the person monitoring can see what they are doing on the computer as well as watch their eye motions for possible suspicious activity through the webcam service (Jose, 2018).

2.2.2 Negative sides to third party surveillance

With each and every aspect of a given third party surveillance service being the newest technology, there are several setbacks and negative sides to the whole concept. Financial disadvantages in the long run, as well as problems with technical devices can setback one from doing an exam properly. The focus on one student and what they are doing cannot be seen at every given moment, as a employee at a third party surveillance monitors up to six students at a given time (Eisenberg, 2013). Manual monitoring still must be done as of now, however, with the rapid growth of artificial intelligence as well as machine learning, robots can soon spot every gesture a human does and interpret a move in a specific way. Technology being as it is, can have hick ups and not always work at a given time. This brings us the big topic of slowing down completion of exams as well as frustrating the student and in the worst-case scenario, complicating their exam and getting them off track. As easy as it may sound, the use of facial recognition can have its setbacks; as well controlled light is needed in order for the database to recognize one's face. Several technical challenges face Facial recognition as one can have a bandage, cut, or even facial characteristic changes from one date to another, making the recognition sometimes impossible (Rodchua 2011, 3-4).

3 Research Methodology

Research methodology is a systematic way to solve a problem, studying the way a research is carried out and conducted. Qualitative as well as quantitative research can be conducted, differing from one another in various ways. Qualitative meaning the focus on smaller amounts as well as human behaviour, opinions, themes, as well as motivation. Quantitative methodol-

ogy having different characteristics such as the use of statistical, mathematical, or numerical analysis to proceed in what is being done (Labaree, 2009). The research conducted in this thesis is based around qualitative research methodology, as trends and thoughts as well as opinions can be extracted at ease, diving deeper into the problem and extracting the most out of what is one looking for.

Qualitative methods having four different categories: observations, analysing texts and documents, interviews and focus groups, as well as audio and video recording (Silverman 2006, 18). In order to conduct successful research regarding authentication and student identity in online exams, a chosen method within the qualitative methods was chosen to take and dig deeper, which was semi-structured interviews. The need to get deeper into the topic as well as to gain different views and perceptions on the topic was to shed light on different perspectives on various problems (Justpaste, 2015). The will and capability of uncovering a targets behaviour, engaging them into the topic to get a deeper understanding of what is being talked about, as well as the results showing descriptive approaches, all show assets of why the qualitative approach is capable and fitting for this research. The use of semi-structured interviews in the research can be backed up by several ideas:

- Informal and unstructured
- Follows a list of topics and areas that need to be covered in a certain order
- The capability to merge off into topics that may come to mind, and not being so called " fixed" as in for example structured interviews

Recording semi-structured interviews, with the use of a guided paper by the interviewer, allows later analysis being easier as open-ended questions may lead to further discussion within the topic (Cohen, 2006). Making sense of complex situations, learning from participants about their previous experiences, as well as construct a clear hypothesis and/or theory from the data gathered (Shukairy, 2017).

3.1 Thematic Analysis in semi-structured interviews

The interviews conducted in this research were based around semi-structured interviews at school. Staff and teachers that had general knowledge about authentication and information technology were interviewed and asked eleven questions related to the topic. Easy to understand and straightforward questions were asked in order to get a clear picture of the given topic, shifting from one question to another with ease. Thus, it made analysing the data easy as it was within a systematic order. Analysing qualitative data can be challenging from time to time, however, a very important and necessary procedure in an innovation process. Thematic analysis is one method of analysing data, used by many when considering qualitative

data (Olivia, 2018). Familiarization in thematic analysis works in the process of becoming familiar with the given data through reading interview transcripts, looking for common themes, as well as key concepts. Generating the initial code once the interviews are done one by one, helps organize and manage what data has been collected. The whole procedure of generating each code per one interview helps the interviewer at the end sort out certain trends and common topics of interest from each interview, merging ideas in groups where common trends are seen. Once each category is fit with certain trends and themes, as well as key concepts, one can start classifying and naming the given defined themes, to get a better picture of the whole picture (Nowell, 2017).

The given choice and use of thematic research fits this research around authentication and student identity, especially when semi-structured interviews were used to conduct own research. The interview elapsing certain areas such as authentication methods, security matters, as well as unethical conduct in exams, can be easily classified and categorized through thematic analysis, interpreting and finding common themes. The research conducted around authentication and student identity is quite broad, covering different topics. A different methodology would have been used, had the subject been not so broad, only covering for example one topic. The fact that it reaches out to specific fields, strikes a key path to dividing the data into different categories, exactly what thematic analysis strives for. The coding phase of thematic research may be the most difficult one, as it structures where everything sits into play in each interview, and must be organized in order for the next phase of creating each theme to work well (Olivia, 2018).

Thematic analysis as mentioned is the process of identifying patterns or themes within qualitative data. Certain trends and ideas were processed with ease throughout the interviews, with hot topics and more important and key concepts being highlighted. Throughout the procedure of analysing this data, certain steps were taken to fully understand and make professional conclusions on the topic.

Data collection within the qualitative research while using the thematic analysis approach has several different approaches to collect data, some being the following:

- Field Diaries
- Observational Data
- Historical Data
- Audio Recording

The method used to collect data was found with ease after the topic was set and research question was polished. Audio recording was the best-fit way to go when collecting data, as everything that was spoken about and possible sub-questions merged off to, were able to be listened to later on so that nothing was left out from the interviewee's answers. The interviewers phone was used to record the interviews as well as a field diary was used to help later analysis with hot topics and key concepts being jotted down at a fast pace.

The given questions asked specifically within the semi-structured interviews can be found in the appendix section of the thesis (Appendix 1). An overview is explained as well briefly before the questions are listed with the target group interviewed as well stating the semi-structured approach used.

3.2 Backing up chosen qualitative method

Research was conducted throughout this thesis using the qualitative research method approach. Within the qualitative research approach, data is analysed through numerical comparisons and statistical inferences. The research throughout followed a qualitative approach, which aims to seek and show how, as well as, why a particular behaviour, phenomenon works in a given context (Mcleod, 2017). One on one interview, focus groups, as well as recording the keeping all show very good examples of qualitative research. The qualitative research approach is defined as a market research method that focuses on gaining data through a more so called open ended and conversational communicational style (Bhat, 2018). After the data was collected from the interviews, a wide scale of information was gathered and quite unstructured. Fortunately, with the help of the thematic analysis approach, following easy steps and procedures to digest and analyse the information, various conclusions were made based on what was found.

The chosen method of qualitative research was based around the fact that experts were in the means and key focus to be interviewed. Deep understanding as well as the capability to merge off from some questions and link ideas with one another, was vital and would have only been capable with interviewees that had at least fundamental knowledge of the authentication and student identity topic. Each and every interview were based around the semi-structured interview approach, with eleven different questions asked by the interviewer to the interviewees. The interviews spanning roughly from 15-20 minutes each, depending on the length of given answers. From the start until the end of each and every interview, recording was done on notepads, with the key focus to look out for possible key concepts, themes, and trends in the interviewee's answers. With the help of good structure from each and every question, following what the interviewee was saying was easy as well as categorizing answers was not hard. Qualitative data fitting into this thesis research in various different ways, with the purpose of organizing data, using the data to interpret different ideas, as well as seek common pattern identification. The tying of field data to the research objective can be easily

shown throughout the literature review, as well as own findings (semi structured interviews). It as well forms the basis for informed and well-organized conclusions as to what should be done in order for student identity to work out well and fill out possible vulnerabilities within data protection, student privacy, as well as various security matters.

3.3 Choosing the interviewees and why exactly them

The reason behind choosing the interviewees to be from Laurea was simply the fact that from the researchers perspective, it was best to take into consideration answers from those that work at the institute where the implementation will be added. The diversity and need to have people's opinions on such a matter from two different perspectives was what the researcher was aiming for. All three staff/teachers that were interviewed had fundamental knowledge on authentication and the transition to online learning. Two out of the three were teachers that teach in the IT field, with one of them doing their PHD in cyber security at the moment. Security in general as well as networking and cyber security is something that both teachers excel in and teach online. With some of the courses even being fully implemented online that they hold, however, slightly lacking behind on authentication and study identity recognition when it comes to taking the exams. Lastly, the third person interviewed was a staff member that runs different projects within the school. The reason behind this was to have an interesting perspective from someone that is ready to implement such matters, however, does not teach. The need to have ideas and stand points as well as suggestions from those that teach, as well as those that manage programmes and degrees is vital for future possible implementations. Teachers may think in one way, and therefore it is good to have a diverse standpoint from two different sides. All in all, the answers from all three members did not differ from one another, however, the researcher did see certain trends that were not mentioned within the interviews but were mentioned within the literature review.

4 Findings of the Research

Findings of the research were conducted through the semi-structured interviews. Three of the experts interviewed all answered questions with a similar approach to the subject, as all of them had a similar background as a teacher at the Laurea campus and not a part of the online programme. Eleven questions were asked from start to finish, with common topic being found the most important as well as certain security matters being highlighted as well as possible biometric implementations that would be almost impossible to include in the coming years online degree programme. With possible obstacles to certain biometric implementations, the interviewer still found it highly important to ask such questions as it is technology that is coming in the near future. The interviews were conducted from the first interviewee onward, wit the goal to stop the interview amount to a point where new information was not collected anymore, but rather the same type of answers heard. In order to conduct this research and analyse it with ease, the thematic analysis approach was used.

Coding the data was a very interesting part of the whole procedure, as it marked a key role when preparing for themes and framework identification in later stages. When going back to the interviews after they were complete, certain trends and codes were conducted and extracted. Certain topics from each interview rose above others, them being:

- Biometrics is the only way to successfully identify students in online exams
- Security measures increase drastically as more layers of authentication are added
- Data protection regulations come into the picture when storing data increases with the use of profile based authentication
- Two layer authentication is important, however, it is not always doable with possible technical errors or too long setup prior to the start of a given exam

The topics above mentioned in the bullet points are the main topics extracted from the interviews. Certain trends and topics of interest can easily be seen as being the most important. Biometrics, security, data protection as well as two-layer authentication being the most talked about points. Even though the unethical conduct in exams was asked in the interviews, it did not point out a drastic concern when listening to the interviewee's answers. Unethical conduct is a problem that has been addressed in schools where exams are taken place within the facility, and therefore, do not show a bigger concern when working online. The difference between the unethical conduct online versus in school was, according to the interviews, a different way of cheating and going around to get the answers. It played a small role in the answers provided, however, was not such a big concern such as data protection and security of the student's personal information.

4.1 Classification and main concerns

Themes and framework identification within the interviews was undergone with classifying the questions into categories such as: biometrics, security, preparation, as well as continuous authentication. Two thirds of the interviews conducted brought up matters concerning biometrics being the key focus in online exams. One of the interviewees mentioned that biometric use in online exams has been used in the past, and is possible to be used in the future. The interviewee that mentioned biometric not being a problem to be used did mention only something about fingerprint recognition, and nothing about possible facial and voice recognition that would need more attention with data protection and storing information on a schools database.

Security was a concern for all of the three interviewees as everything conducted online must be stored somewhere. Two out of the three interviewees mentioned that information between schools is transmitted online, and therefore, a concern would be in the future how the

information is stored and with who's approval as everything is online. A key factor that was mentioned in all of the interviews was that students doing exams all around the world, using different internet service providers and internet speeds, might not be able to connect to the online service and conduct exams at given times.

Preparation and setup for exams is a major concern for all of the interviewees, as it requires time and everything to work technically correct at a given time. Compared to the traditional way of attending a classroom and completing an exam with a pen and paper, online exam using various authentication methods require more procedures to work. One of the interviewees suggested two-layer authentication with possible fingerprint recognition as well as profile based authentication to work out for student identity, as well as to at the same time not to go against data protection regulations and technical errors. Two out of the three interviewees suggested more time for preparation for the exam and trying to implement biometric recognition, with the school stating and giving certain criteria prior to the exam about data protection, and possible technical errors regarding the software used to identify students.

Continuous authentication was played a key role in each and every interviewee's answers, as it is something that must happen otherwise unethical conduct can arise. Each and every interviewee mentioned that it is a must to have authentication from the start of an exam to the finish, at checkpoint times, but not necessarily at all times. One of the interviewees mentioned that facial recognition as well as voice recognition is a must in order to monitor and know that one is doing an exam alone. Two out of the three interviewees stated that continuous authentication is a must with checkpoints at given times throughout the exam. According to them, possible checkpoints could use profile based authentication or fingerprint recognition to quickly identify and know that the same person is still doing the exam and not someone else.

4.2 Main concerns from literature review not addressed in interviews

Various concerns were seen when comparing what the interviewees wrote to what the literature review mentioned. Highly important matters in regard to the use of multi-factor authentication being important and the quality that it can produce was something mentioned within the research in the literature review, however, was not mentioned in the interviewee's answers. Fingerprints can be used for infrequent identification, where as on the other hand geometry based biometrics can be used for more frequent checks (Ross, 2007). As Ross mentions, the use and merging of two different authentication methods at various times throughout a exam input can help increase security measures, and give a example of checkpoint verification of a student doing an exam.

The fact that the interviewees are aware of the transition to online learning and have fundamental knowledge on possible authentication methods, do not however understand the possi-

ble realistic unethical approach that many students take when completing exams online. As mentioned in (Bergstein, 2012) report, many universities have implemented possible online courses in the past, but do not tend to interact well when it comes to unethical conduct. The reason and thought behind the interviewees mentioning the use of biometrics in online exams for students a must, shows that they do really intend to try and implement such needs into the schools academic programme. GDPR was a concern for the interviewees, however, nothing related to the increase in regulations and standards becoming more accurate was mentioned. According to (Baines, 2017), the regulations set for obeying certain criteria and standards have increased even more recently, putting a major burden the institutions to choose the right methods of online identity recognition.

A major concern regarding costs and the use of possible profile based authentication or biometrics was seen when asked about the following question: Will it be very expensive you think to implement this for Laurea and do you think students are aware of the possible transition? Short and simple answers were given regarding the costs of online exams, however, were not backed up by any other statements such as the use of two more cheaper authentication methods. All of the answers given were that it would be expensive to implement such measures. Compared to the literature review and for example what Kolowich mentioned in his article, there are various different systems and even third-party companies that can help with monitoring exams with costs not being possibly as high as many would think (Kolowich, 2013). Lastly, something that was spotted by the researchers mind was the fact that interviewees did not mention anything regarding the risks and vulnerabilities that might be seen when using different stakeholders to help online authentication. As mentioned by Sukadarmika, even without the use of third-party surveillance companies, but just programmes that are written by others, various different concerns rise when the use of different platforms and programmes increase (Sukadarmika et al., 2016).

5 Comparison to Existing literature

With technology advancing at a rapid pace, there is not one correct way to correctly identify a student identity in a online exam environment, but rather several ways that can be merged together and/or duplicated to not only increase security measures but also to really know who is completing the given exam (Kang et al., 2015, 47). Each of the interviewees had a similar opinion as what was mentioned in the literature review regarding correct identity in online exams. Several implementations can be used, however, depending on the exam type as well as duration, an institution can pick which of the authentication methods would be best suitable. As mentioned in (Pritchard, 2019) report as well as the interviewee's answers, PIN codes make up a very important structure when considering the use of two-layer authentication and the start of basic first layer identification. Both sides agreed upon the fact that it is important to have the basic PIN code recognition at the beginning of an exam. In order to get

into the system that the exam is done in, one must provide a four-digit code to gain access and enter the exam field. According to the interviewees as well as Pritchard, it is something that is always necessary and must not be related to ones personal information such as street address, date of birth, or social security number.

According to Fayyoumi, the use of facial recognition in online exams decreased the likelihood of cheating happening (Fayyoumi et al., 2014). Compared to the interviewee's answers, the answers were slightly different. All three of the interviewees did not have a opinion on the fact that cheating would decrease with the use of facial recognition, backed up with facts such as: screen sharing not being mentioned if in use, is facial recognition on all the time or at given checkpoints, as well as technical errors can cause exams to continue even with the camera not in use. With every type of situation being considered by the interviewees when it came to facial recognition, they did however state that with the use of continuous facial recognition from the start of an exam to the finish, the likelihood of cheating would possibly decrease.

From the given comparison of the literature review and interviews conducted, the interviewer noticed a similarity in answers when it came to fingerprint recognition. The use of fingerprint scanners is one of the simplest ways of biometric recognition, and at the same time does not require lots of time and has a major advantage when considering financial costs compared to other biometric methods (Ingashitula 2017, 1). The staff interviewed at Laurea had a similar approach, considering the fingerprint recognition something that can be implemented with greater ease. The interviewees thus had concerns about storage capacity as well as data protection matters.

Two-layer authentication creates a security additional layer of security, in case one of the authentication methods has vulnerability and is bypassed (Douthit, 2018). In order for exams to be conducted with ease by the students, according to the interviewees, an appropriate and stable method must be chosen by the institution to mitigate any possible problems. Continuous authentication was a subject mentioned numerously throughout the interviews conducted at school, and that can be justified by Cmarsden stating that it is possible to get accurate results with the use of biometric implementations (Cmarsden, 2015). In order for possible voice and face recognition to be implemented, the institution providing the studies must make clear and straightforward rules about the use of such authentication methods. According to the interviewees, a possible introduction lecture prior to the degree programme starting would be a good idea, where every procedure of used biometrics is gone through as well as data protection regulations are addressed.

Understanding the shift and principles of online studies may tend to be difficult, however, it sets a futuristic path when keeping up to par with technology (Sukadarmika et al., 2016).

Security matters according to Sukadarmika have been a problem for institutions that have previously used the online exam methods. Impersonation, or in other words the cover up of someone else doing the exam for a peer, is a major concern for teachers and staff grading the student's exams. (Karim, et al., 2015). According to the interviewees, security was a major concern more when it came to storing data. Each and every time a student logs into a system and uses possible biometric or profile based authentication, the information is stored for later use of identification. The teachers and staff brought up a common recommendation concerning the security matters, which was to limit the amount of security levels to the needed amount only, and not to add any additional layers. According to one interviewee, the need to find a common and trustworthy two-layer authentication is ideal and in need for Laurea, which is only double by troubleshooting various possibilities. Finding the correct solution is not easy, and requires time and effort. Within the past ten years, numerous amounts of universities and colleges around the globe have established online courses, later getting to know and realise that many students are taking advantage of this, cheating and causing problems related to fraud (Bergstein, 2012).

When comparing the literature review and interviews conducted, certain trends were found, similar to the ones extracted from the thematic analysis. Biometrics, security, preparation for exams, as well as continuous authentication playing a key role in both the theoretical approach as well as semi-structured interviews. With the topic being quite new to everyone, possibilities and capabilities mark sky as the limit, however, time will tell when 100% accurate authentication in online exams can be seen.

6 Conclusion

In conclusion, the objectives and research question were justified and explained throughout the literature review and later on compared and contrasted to the results found conducted in the semi-structured interviews. The research question: **How can institutions ensure correct student identity with the use of different authentication methods when exams are done outside of school?** was looked at through various different authentication methods. Justified with the rapid increase in technology and possible implementations of machine learning and artificial intelligence in e learning, institutions must keep up with what is going on around the globe. As seen throughout the literature review, possible outcomes and online exams have already been implemented, however, may lack in security measures as well as fully monitored services. With roughly 23 million new learners online in only 2017, and with a total of 81 million globally, the need to keep security measures and unethical conduct out of play marks a key role for institutions and/or others trying to set up exams online. With the shift and usage of more biometrics and other high tech implementations, the need to focus on security as well as the needs of the students is key. Students must have examination time to focus on what they are doing, and not to shift off and deal with possible problems with for example third

party surveillance providers. With citizens even more busy in this day and age with possible hobbies and/or double degree programmes, exams must be set up so that vulnerabilities are fixed prior to the exam take, as well as hot fixes being placed at given times. When considering the unethical concerns, even though the unethical conduct in exams was asked in the interviews, it did not point out a drastic concern when listening to the interviewee's answers. Unethical conduct is a problem that has been addressed in schools where exams are taken place within the facility, and therefore, do not show a bigger concern when working online.

As Pollari mentioned in his article, Finland has thousands of students coming each year to study or do courses around the country (Pollari, 2013). With great technology experts and high speed Internet, the country has great potential to be a great leader in e learning, providing great education fully through the web. If biometric choice and/or other authentication methods are chosen correctly by Laurea, the possibilities being the sky as the limit, taking into account GDPR regulations being met. As mentioned by Shah, more than 800 universities already have used online courses, and is increasing at a very rapid pace (Shah, 2018). Other stakeholders come into play however with many factors needed to be looked at, the main aim is to have students present knowledge that they have learnt through online exam in a given time, alone in a empty room with know one else in helping out.

Going through the semi-structured interviews and using the thematic analysis approach, gave the researcher great ease to seek the most common topics and trends mentioned. The location of the interviews being done in one single institute, with all teachers having no prior experience in giving online exams using authentication methods, caused possible setbacks in more in depth answers. Time consumption played as well throughout the process of the thesis, having the researcher focus on each part of the literature review with no problems. All in all, with the use of possible biometrics and continuous authentication, there is a great chance that the upcoming degree programmes fully implemented online can work out of Laurea. Trial and error with what methods to use, that are cost efficient, exist and are out there for use.

References

Printed sources

Smith, M. (2016). DNA Evidence in criminal appeals and post-conviction inquiries: Are new forms of review recuired? *Macquarie Law Journal* 2, 141.

Electronic sources

Alotaibi, S.J. (2010). Using biometrics Authentication Via Fingerprint Recognition in E-exams in E-learning Environment. [online], availible at:https://eprints.soton.ac.uk/271453/1/USING_BIOMETRICS_AUTHENTICATION_VIA_FINGERPRINT_RECOGNITION_IN_E-EXAMS_IN_E-LEARNING_ENVIRONMENT.pdf (Accessed: 4.12.2018)

Alton, L. (2018). *Are Biometrics Good or Bad for Digital Security? [online],* available at:https://www.informationweek.com/strategic-cio/security-and-risk-strategy/are-biometrics-good-or-bad-for-digital-security-/a/d-id/1331991 (Accessed: 10.12.2018)

Anderson, K. (2017). *5 Key Reasons Why eLearning is Essential and Not Overrated. [online],* available at: https://elearningindustry.com/elearning-is-essential-not-overrated-5-key-reasons (Accessed: 20.11.2018)

Andriotis, N. (2017). *The Hidden Costs Behind eLearning. [online],* available at:https://elearningindustry.com/hidden-elearning-costs (Accessed: 14.11.2018)

Ayvaz, U., Guruler, H. and Devrin, M.O. (2017). *Use of Facial emotion recognition in E-learning Systems. [online],* available at:https://www.researchgate.net/publication/320307642_USE_OF_FACIAL_EMOTION_RECOGNITION_IN_E-LEARNING_SYSTEMS (Accessed: 18.11.2018)

Bachmann, L. (2018). *Multi-factor authentication: More Important Now Than Ever. [online],* available at : https://blog.lastpass.com/2018/07/multi-factor-authentication-important-now-ever.html/ (Accessed: 18.12.2018)

Bailie, J. (2009). *Online Learner Authentication: Verifying the Identity of Online Users. [online],* available at:https://www.researchgate.net/profile/Jeffrey_Bailie/publication/292156270_Online_Learner_Authentication_Verifying_the_Identity_of_Online_Users/links/56ab906308aeadd1bdce53e3.pdf (Accessed at: 2.12.2018)

Bartley, S.J., and Golek, J.H. (2004). *Evaluating the Cost Effectiveness of Online and Face-to-Face Instruction. [online],* available at:https://pdfs.semanticscholar.org/12e9/bf795f70026404c3fa6603e494f8abf77412.pdf (Accessed: 26.11.2018)

Bergestein, B. (2012). *In online exams, Big Brothers Will be Watching. [online],* available at:https://www.technologyreview.com/s/506346/in-online-exams-big-brother-will-be-watching/ (Accessed: 18.12.2018)

Bhat, A. (2018). *Qualititative Research: Definition, Types, Methods and Examples. [online],* available at: https://www.questionpro.com/blog/qualitative-research-methods/ (Accessed: 4.1.2019)

Biometric Online Authentication Provider System, (2009). *Method and System for Providing Online Authentication Utilizing Biometric Data. [online],* available

at:https://patentimages.storage.googleapis.com/96/e6/73/7d225ebd12ede7/US7502761.pdf (Accessed: 5.12.2018)

Biometric Solutions, (2016). *Keystroke Dynamics. [online],* available at:http://www.biometric-solutions.com/keystroke-dynamics.html (Accessed: 1.12.2018)
Chen, R.S. (2014*). Information Technology Journal. [online],* available at:http://docsdrive.com/pdfs/ansinet/itj/2014/2674-2681.pdf (Accessed at: 3.11.2018)

Chen, Y. and He, W. (2013). *Security Risks and Protection in Online Learning. A Survey. [online],* available at: http://www.irrodl.org/index.php/irrodl/article/view/1632/2712 (Accessed: 6.1.2019).

Cmarsden, (2015). *4 Reasons Why Biometric Security is the Way Forward. [online],* available at: http://www.digitus-biometrics.com/blog/4-reasons-why-biometric-security-is-the-way-forward/ (Accessed: 18.12.2018)

Cohen, D., Crabatree, B.B. (2008). *Semi-structured interviews. [online],* available at:http://www.qualres.org/HomeSemi-3629.html (Accessed: 23.18.2018)

Dacanay, M. (2017). *Benefits of Implementing Multi-Factor Authentication. [online],* available at: https://www.globalsign.com/en/blog/benefits-of-multi-factor-authentication/ (Accessed: 18.12.2018)

Das, R. (2004). *An application of Biometric Technology: Keystroke Recognition. [online],* available at:http://web.science.mq.edu.au/~isvr/Documents/pdf%20files/biometrics/Keystroke%20Recognition%20Biometrics%20-%20find%20BIOMETRICS.htm (Accessed: 20.18.2018)

Douthit, C. (2018) *Two factor Authentication (2FA) Is Important to Protect Your Cryptocurrency Investments. Heres Why. [online],* available at: https://www.investinblockchain.com/importance-two-factor-authentication/ (Accessed: 2.1.2019)

Eisenberg, A. (2013). *Keeping an eye on Online Test-Takers. [online],* available at:https://immagic.com/eLibrary/ARCHIVES/GENERAL/GENPRESS/N130302E.pdf (Accessed: 18.12.2018)

Epignosis LLC, (2014). E-learning Concepts, Trends, Applications. [Online], available at:https://www.talentlms.com/wp-content/uploads/2018/09/elearning-101-concept-trends-applications.pdf (Accessed: 13.11.2018)

Fayyoumi, A. and Zarrad, A. (2014). *Novel Solution Based on Face Recognition to Address Identity theft and Cheating in Online Systems. [online],* available at:https://file.scirp.org/pdf/AIT_2014042816334195.pdf (Accessed: 12.12.2018)

Frankenfield, J. (2018). *General Data Protection Regulation (GDPR). [online],* available at:https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp (Accessed: 3.12.2018)

GDPR Report, (2017*). How can schools ensure they are GDPR compliant? [online],* available at: https://gdpr.report/news/2017/12/05/can-schools-ensure-gpdr-compliant/ (Accessed: 17.11.2018)

Halfin, D., Poggemeyer, L., Hall, J. (2017). *Why a pin is better than a password. [online],* available at: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password (Accessed: 9.1.2019)

Hylton, K., Levy, Y., and Dringus, L. P. (2016). *Utilizing webcam-based proctoring to deter misconduct in online exams. Computers & Education, 92,* 53-63. https://doi.org/10.1016/j-compedu.2015.10.002 (Accessed: 8.1.2019)

Ihalainen, P. (2016). *What is Multi-Factor Authentication (MFA)? [online],* available at:https://www.globalsign.com/en/blog/what-is-multi-factor-authentication-mfa/ (Accessed: 18.12.2018)

Ingashitula, M.S. (2017). *Fingerprint Based Exam hall Authentication. [online],* available at:https://www.researchgate.net/profile/Mathew_Ingashitula/publication/320856056_Designing_Fingerprint_Based_Exam_Hall_Authentication_A_PROJECT_REPORT_BACHELOR_HONOURS_DEGREE_IN_DIGITAL_COMMUNICATION_TECHNOLOGY_IN_SIGNATURE_SIGNATURE/links/59fea0f9a6fdcca1f29c0041/Designing-Fingerprint-Based-Exam-Hall-Authentication-A-PROJECT-REPORT-BACHELOR-HONOURS-DEGREE-IN-DIGITAL-COMMUNICATION-TECHNOLOGY-IN-SIGNATURE-SIGNATURE.pdf (Accessed: 6.12.2018)

JustPaste.it (2015). *Why choose qualitative Research over Quantitative Research? [online],* available at: https://justpaste.it/WhyChooseQualitativeResearch (Accessed: 4.1.2019)

Fayyoummi, L. and Nissenbaum, H. (2010*). Facial recognition Technology. A survey of Policy and Implementation Issues. [online],* available at:http://eprints.lancs.ac.uk/49012/1/Document.pdf (Accessed: 18.12.2018)

Iorga, M., Ciuhodaru, T. and Romedea, S.N. (2013). *Students and the unethical behaviour during academic years. [online],* available at: https://ac.els-cdn.com/S1877042813032540/1-s2.0-S1877042813032540-main.pdf?_tid=8b1e51c1-b9b4-4b28-aaaa-468e76b8e9b9&acdnat=1545297140_b93276d276a2d44f443e0e5fc6cb9cde (Accessed: 20.18.2018)

Jose, S. (2018). *Online proctoring is Trending: Here is All You Should Know About It. [online],* available at: https://blog.talview.com/a-complete-guide-to-online-remote-proctoring (Accessed: 18.12.2018)

Joseph, C. (2018*). Examples of Unethical Behavior in an Organization. [online],* available at:https://smallbusiness.chron.com/examples-unethical-behavior-organization-13629.html (Accessed: 20.18.2018)

Kang, B.H and Kim, H. (2015). *Proposal: A design of E-learning User Authentication System. [online],* available at: https://pdfs.semanticscholar.org/6293/5229a5b3666237f963ba8656048c35c7a090.pdf (Accessed: 11.1.2019)

Keeper Security, (2017). *PIN vs. Password: What's the Difference? [online]*, available at: https://keepersecurity.com/blog/2017/03/07/pin-vs-password-whats-the-difference/ (Accessed: 11.12.2018)

Kigwana, I. and Venter, H. (2018*). A digital Forensic Readiness Architecture for Online Examinations. [online],* available at: http://www.scielo.org.za/pdf/sacj/v30n1/02.pdf (Accessed: 22.12.2018)

Koirala, J. (2013). *Identity Verification with Speech Recognition. [online],* available at:https://www.theseus.fi/bitstream/handle/10024/62229/thesis.pdf?sequence=1 (Accessed: 8.12.2018)

Kolowich, S. (2013). *Behind the Webcams Watchful Eye, Online Protoctoring Takes Hold. [online],* available at: https://www.chronicle.com/article/Behind-the-Webcams-Watchful/138505 (Accessed: 18.12.2018)

Labaree, R.V. (2009). *Organizing Your Social Sciences Research Paper: Quantitative Methods. [online],* available at: http://libguides.usc.edu/writingguide/quantitative (Accessed: 23.12.2018)

Lardinois, F. (2018). *Google launches an improved speech-to-text service for developers. [online],* available at: https://techcrunch.com/2018/04/09/google-launches-an-improved-speech-to-text-service-for-developers/?guccounter=1 (Accessed: 6.12.2018)

Lehmann, K. and Chamberlin, L. (2009). Making the move to eLearning. [online], available at: https://books.google.fi/books?id=c9LGBtALAqUC&printsec=frontcover&dq=shift+to+online+learning&hl=en&sa=X&ved=0ahUKEwjK16bh_oXfAhWB_SwKHW5fBXw4ChDoAQgmMAA#v=onepage&q&f=false (Accessed: 6.11.2018)

Lelei, F. (2015). *The Benefits of Individual, Paired, and Group Lessons in a Montessori Childrens House. [online],* available at: file:///Users/alexurosevic/Downloads/Lelei.pdf (Accessed: 19.12.2018)

Levy, Y. and Ramim, M.M. (no date). *A theoretical Approach for Biometrics Authentication of e-Exams. [online],* available at: http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf (Accessed: 3.12.2018)

Liao, W., Vanorsdale, C. (2016). *Facial recognition and its Applications in Distance Learning Environment. [online],* available at:https://pdfs.semanticscholar.org/7eba/8590558148759b0aeebb0772e19ae50edb3c.pdf (Accessed: 4.1.2019)

Littlefield, J. (2017). *10 Reasons to Choose Online Education. [online],* available at:https://www.thoughtco.com/reasons-to-choose-online-education-1098006 (Accessed: 19.12.2018)

Maring, J. (2018). *Put Password in the Past with Multi-Factor Authentication. [online],* available at: https://www.securitymagazine.com/articles/88848-put-password-pain-in-the-past-with-multi-factor-authentication (Accessed: 21.11.2018)

Martin, D.E., Rao, A. and Sloan, L.R. (2011). *Ethnicity, Acculturation, and Plagiarism: A criterion Study of Unethical Academic Conduct. [online],* available at:https://www.jstor.org/stable/44150979?seq=1#page_scan_tab_contents (Accessed: 20.12.2018)

Mayhew, S. (2012). *Explainer: Hand Geometry Recognition. [online],* available at:https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition (Accessed: 2.1.2019)

Mening, R. (2017). *4 Security tips to Help You Secure Your Online Learning Platform. [online],* available at: https://elearningindustry.com/secure-your-online-learning-platform-4-security-tips-help (Accessed: 4.1.2019)

Mcleod, S. (2017). *Qualitative vs Quantiative Research. [online],* available at:https://www.simplypsychology.org/qualitative-quantitative.html (Accessed: 27.12.2018)

Nowell, L.S, Norris, J.M. and White, D.E. (2017). *Thematic analysis: Striving to meet the trustworthiness Criteria. [online],* available at:https://journals.sagepub.com/doi/full/10.1177/1609406917733847 (Accessed: 24.12.2018)

Oberhaus, D. (2018). *What is two-factor Authentication Recovery Code? [online],* available at: https://motherboard.vice.com/en_us/article/evknva/what-is-a-two-factor-authentication-recovery-code (Accessed: 1.1.2019)

Olivia, 2018. (2018). *Thematic Analysis. [online],* available at:https://www.statisticssolutions.com/thematic-analysis/ (Accessed: 24.12.2018)

Oxford Dictionary, (no date). *Voice Recognition. [online],* available at:https://en.oxforddictionaries.com/definition/voice_recognition (Accessed: 4.12.2018)

Pappas, C. (2015). *Active Learning in Online Training: What eLearning Proffesionals Should Know. [online],* available at: https://elearningindustry.com/active-learning-in-online-training-what-elearning-professionals-should-know (Accessed: 10.1.2019)

Perrin, D.G, Perrin, E., Muirhead, B. and Betz, M. *Instructional Technology and Distance Learning. [online],* available at:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.694.4322&rep=rep1&type=pdf#page=7 (Accessed: 13.11.2018)

Pollari, M. (2013). *Information and Inspiration on e-learning from Finland. [online],* available at: https://www.luma.fi/en/news/2013/09/09/information-and-inspiration-on-e-learning-from-finland/ (Accessed: 3.1.2019)

ProctorU, (2018). *How it Works. ProctorU. [online],* available at:https://www.proctoru.com/downloads/howitworks.pdf (Accessed: 18.12.2018)

Pritchard, J. (2019). *Personal Identification Number (PIN) Security Tips. [online],* available at: https://www.thebalance.com/pin-number-definition-and-explanation-315344 (Accessed: 2.1.2019).

Rai, A., Khan, A., Bajaj, A. and Khurana, JB. (2017). *An efficient online examination system using speech recognition. [online],* available at:https://www.irjet.net/archives/V4/i4/IRJET-V4I4715.pdf (Accessed: 9.12.2018)

Ramim, M.M. and Nova, Y.L. (2007). Towards a Framework of Biometric Exam Authentication in E-learning Environments. [online], available at: http://www.irma-international.org/viewtitle/33131/ (Accessed: 15.11.2018)

Ramu, T. and Arivoli, T. (2013). *A framework of secure Biometric Based Online Exam Authentication: An Alternative to Traditional Exam. [online],* available at:https://pdfs.semanticscholar.org/e11f/74e9427a94d82302630c0127b1e316a35999.pdf (Accessed: 27.11.2018)

Rodchua, S., Boakye, G.Y. and Woolsey, R. (2011). *Student Verification System for Online Assesments: Bolstering Quality and Integrity of Distance Learning. [online],* available at:https://cdn.ymaws.com/www.atmae.org/resource/resmgr/Articles/Rodchua-Student-Verification.pdf (Accessed: 17.12.2018)

Ross, A. (no date). *A prototype Hand Geometry-based Verification System. [online],* available at: https://paginas.fe.up.pt/~ee03106/Relatorio/Referencias/1.pdf (Accessed: 14.11.2018)

Rudrapal, D., Debbarma, S.S. and Debbarma, N.K.N. (2012*). Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H People. [online],* availbile at:https://www.researchgate.net/profile/Dwijen_Rudrapal2/publication/258650671_Voice_Recognition_and_Authentication_as_a_Proficient_Biometric_Tool_and_Its_Application_in_Online_Exam_for_PH_People/links/54ddae400cf25b09b91465ff/Voice-Recognition-and-Authentication-as-a-Proficient-Biometric-Tool-and-Its-Application-in-Online-Exam-for-PH-People.pdf (Accessed: 6.12.2018)

Saheed, Y.K., Hambali, M.A., Adeniji, I.A. and Kadri, A.F. (2017). *Fingerprint Based Approach for Examination Clearance in Higher Institutions. [online],* available at:file:///Users/alexurosevic/Downloads/46-1032-1-PB.pdf (Accessed: 1.11.2018)

Salameh, N. (2015). *Review of user authentication methods in online examination. [online],* available at:https://www.researchgate.net/profile/Nader_Salameh/publication/284895765_Review_of_user_authentication_methods_in_online_examination/links/56f62b0d08ae95e8b6d1e204/Review-of-user-authentication-methods-in-online-examination.pdf (Accessed: 3.11.2018)

Sanna, P, Marcialis, G.L. (2017). *Remote Biometric Verification for Elearning Applications: Where we Are. [online],* available at:https://www.researchgate.net/publication/320362029_Remote_Biometric_Verification_for_eLearning_Applications_Where_We_Are (Accessed: 2.1.2019)

Sarrayrih, M. and Ilyas, M. (2013). *Challenges of Online Exams, Performance and problems for Online University Exam. [online],* availible at:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.304&rep=rep1&type=pdf (Accessed: 1.12.2018)

Serra, X. (2017). *Face Recognition using Deep Learning. [online],* available at:http://sergioescalera.com/wp-content/uploads/2017/02/TFM-Xavier-Serra.pdf (Accessed: 2.11.2018)

Shah, D. (2017). *By the numbers: MOOCS in 2017. [online],* available at: https://www.class-central.com/report/mooc-stats-2017/ (Accessed: 25.11.2018)

Shukairy, A. (2017). *9 Tips to Conducting Accurate Qualitative Research. [online],* available at: https://www.invespcro.com/blog/9-tips-to-conducting-accurate-qualitative-research/ (Accessed: 23.12.2018)

Silverman, D. (2006*). Interpreting Qualitiative Data. [online],* available at: https://books.google.fi/books?id=uooz4p82sDgC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (Accessed: 5.1.2019).

Song, Y., Cai, Z. and Zhang, Z.L. (2017). *Mulit-touch Authentication Using Hand Geometry and Behavioural Information. [online],* available at:https://www.computer.org/csdl/proceedings/sp/2017/5533/00/07958587.pdf (Accessed: 3.1.2019)

Struc, V., Pavesic, N. (2015). *Hand-Geometry Device. [online],* available at:https://www.researchgate.net/publication/228851322_Hand-Geometry_Device (Accessed: 4.11.2018)

Student & Academic Services, (2015). *How to deal with technical Problems During an online exam. [online],* available at:http://registrar.athabascau.ca/exams/online/invigilator/tech_problems.php (Accessed: 13.11.2018)

Sukadarmika, G., Linawata, L., Sastra, N. and Setiawan, I. (2016). *Proposed model for e-exam availability in WLAN environment. [online],* available at:file:///Users/alexurosevic/Downloads/Proposed_model_for_e-exam_availability_in_WLAN_env.pdf (Accessed: 6.11.2018)

Teh, P.S., Teoh, A.B.J. and Yue, S. (2013). *A Survey of Keystroke Dynamics Biometrics. [online],* available at:https://www.researchgate.net/publication/259115430_A_Survey_of_Keystroke_Dynamics_Biometrics (Accessed: 15.11.2018)

Triggs, R. (2018). *How fingerprint scanners work: optical, capative, and ultrasonic variants explained. [online],* available at: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/ (Accessed: 8.1.2019)

Tryfonas, T., and Askoxylakis, I. (2015*). Human Aspects of Information Security, Privacy, and Trust. [online],* available at:https://books.google.fi/books?id=nrQ0CgAAQBAJ&pg=PA133&lpg=PA133&dq=profile+based+authentication&source=bl&ots=iEI8dksKBm&sig=TX0WTr6Gwdbi0J5xcSCclu8jYWo&hl=en&sa=X&ved=2ahUKEwiNtZHp957fAhUjqlsKHTq0Cdk4ChDoATACegQICRAB#v=onepage&q=profile%20based%20authentication&f=false (Accessed: 13.11.2018)

Tsimperidis, L., Yoo, P., Taha, K. and Mylonas, A. (2018). *An adaptive model for keystroke-Dynamics-Based Educational Level Classification. [online],* available at:https://www.researchgate.net/publication/327949049_RBN_An_Adaptive_Model_for_Keystroke-Dynamics-Based_Educational_Level_Classification (Accessed: 10.1.2019)

UKessays, (2013*). Advantages and Disadvantages of Biometrics. [online],* available at:https://www.ukessays.com/dissertation/examples/information-systems/advantages-and-disadvantages-of-biometrics.php (Accessed: 26.11.2018)

Ullah, A., Xiao, H., Lilley, M. and Barker, T. (2012). *Usability of Profile Based Student Authentication and Traffic Light System in Online Examination. [online],* available at:https://www.researchgate.net/profile/Abrar_Ullah/publication/261466127_Usability_of_Profile_Based_Student_Authentication_and_Traffic_Light_System_in_Online_Examination/links/55ee975a08aef559dc43c4d4/Usability-of-Profile-Based-Student-Authentication-and-Traffic-Light-System-in-Online-Examination.pdf (Accessed: 26.11.2018)

Violino, B. (2017). *Continuous authentication: Why its getting attention and what you need to know. [online],* available at:https://www.csoonline.com/article/3179107/security/continuous-authentication-why-it-s-getting-attention-and-what-you-need-to-know.html (Accessed: 24.11.2018)

Zunkel, R.L. (2017). *4 Hand Geometry Based Verification. [online],* available at:http://mer.chemia.polsl.pl/biometrologia/materialy/biometrics/handgeometry.pdf

Appendices

Appendix 1: Interview questions conducted at Laurea

The following questions were asked in the Semi Structured interviews conducted at the Leppävaara campus at Laurea University of Applied Sciences. The staff and teachers interviewed were all in the IT field and had basic fundamentals knowledge on matters regarding authentication and the shift to online learning.

- What are different authentications methods that you know of that can help and which are the most secure ones?
- How can we ensure correct identity in online exams? And is it even possible?
- Why is using biometrics important when trying to seek correct identity in online exams?
- Any other security related matters that you may know of?
- Is there a need of more complex biometric authentication or is profile-based authentication important?
- Unethical conduct?
- Is two factor authentication or more layers important or is one enough? And how can such an implementation work?
- Is continuous authentication a must?
- Will it be very expensive you think to implement this for Laurea and do you think students are aware of the possible transition?
- Is it possible to have good biometric authentication but be portable and not stationed always at a given desk?
- What is the most important? Pin code, facial recognition, fingerprint, keystroke, profile-based authentication, hand geometry based biometrics or voice recognition? Or is there a most important?