Dissertation

Developing a Data Visualization Tool for the Evaluation Process of a Graphical User Authentication System

Loizos Siakallis

UNIVERSITY OF CYPRUS

DEPARTMENT OF COMPUTER SCIENCE

December 2020

UNIVERSITY OF CYPRUS

DEPARTMENT OF COMPUTER SCIENCE

Developing a Data Visualization Tool for the Evaluation Process of a Graphical User Authentication System

Loizos Siakallis

Supervisor
Prof. Andreas Pitsillides

Co-Supervisor
Dr. Marios Belk

The individual thesis submitted for partial fulfillment of the requirements for obtaining the degree of Computer Science, Department of Computer Science in University of Cyprus

December 2020

Acknowledgments

In spite of the difficulties, we all had to face during such hard times, it was a joy to work on this thesis and the subject around it. For that I would like to thank everyone who managed to support me throughout this journey.

Firstly, I would like to thank my supervisor, Prof. Andreas Pitsillides with whom I had the opportunity to work under his supervision and provided me with the means to carry through with this dissertation project. I would equally want to thank Dr. Marios Belk for his cooperation and inspiration which lead me to work harder and with even more enthusiasm during this thesis.

I also owe special thanks to Argyris Constantinides for the immerse understanding, help and support he has provided. With the use of his Picture Gesture Authentication system, I was able to establish by user study and development of my system.

Finally, I would like to thank my family and my fellow computer science students for the patience they showed during this year and their cooperation and participation of my user study.

Abstract

In this thesis, we will be developing a data visualization and examination tool for the administrators of a graphical user authentication system to use in a user study. For the evaluation of the system a use case of a user study will be executed with the use of an existing graphical password authentication system along with data collected from the system in addition to data recorded using the Emotiv Insight headset during the authentication sessions. For the representation of all the data that was recorded, as stated above, a web application was developed for the administrator of the graphical password authentication system that was previously mentioned and the system that was developed for this dissertation project acts as a subsystem of this parent system. The admin of the system, upon their login, will be able to view general statistics regarding their users' passwords and login sessions. Such statistics will be able to provide the admin with insights relating to the effectiveness of the passwords created.

Since humans are by nature visual learners, it is anticipated that the use of a graphical password as the mean of authentication will eventually constitute in a higher percentage of memorability of the password and higher chances of recall in the long-term. There are many early studies indicating the consequent positive effects of graphical user authentication in the area of both security and usability.

An important factor of a person's individuality is their perception of the world and their reactions to its actuators. During such triggering events, an essential metric and a satisfactory sign of their perception is their emotion. Emotion is an effective authenticator since it cannot be predicted, imitated by a third person nor forced into action. But emotion studies do not stop there. They can be studied for their several effects they can have on the authentication process itself.

Table of Contents

Table of Figures

1 Introduction

In this chapter we will have a deep look into the problem that led us to study this region of user authentication and to develop this interactive dashboard for the visualization of data. Finally, we will offer a scope of this thesis' chapters and sections.

1.1 Definition of problem

Information security has always been, but is also steadily becoming an even more critical part of computer science, and consequently our lives, as the technology progresses in such fast rates. As the users and accounts on the web are increasing exponentially, their insurance of their data and their integrity is becoming a major concerning aspect of today’s studies. Every user nowadays has multiple accounts bound to their identity and this is one of the many reasons that the security of an individual’s credentials is becoming overwhelming for the user. As every account requires a method of authentication, which most of them require the traditional text password, numerous problems are being emerged.

The user’s ability to successfully memorize and recall a text password is becoming even more rare. For that reason, the users might acknowledge this weakness of theirs and submit to compromising means. The users in their effort to remember their credential to various online platforms, might be tempted to create text passwords with a profoundly similarity to one another, or in the worst case, they might even register the same passwords over different accounts online. This unfortunately indicates that in their effort to make the memorability and usability issue, which was emerged with the rising number of accounts per user, less dreadful, they are compromising the security of their passwords. The users now are a target of potential attacks by providing this little friction due to the vulnerability of their online presence.

To state it simply, the problem with today’s user authentication schemes is that they either focus on enhancing the usability and user experience of the user and neglect the security of the user, or they focus so much on the security aspect that it becomes extremely unpleasant for the user to use.

Naturally, to address this problem, several studies have focused on the research and development of another type of user authentication, the graphical user authentication. The benefits of using visual means or cues for the authentication of the user were promising from the start. Users’ engagement during the creation and authentication phases were higher due to the nature of the authentication scheme which appealed in a greater degree since humans are known to be visual learners.

Although there are undoubtedly benefits from using graphical user authentication schemes, the majority of the studies indicated a persistent problem that affected their broaden adoption. That issue revolved around the limited number of user studies.

1.2 Purpose

There is a steadily increasing acknowledgment of the drawbacks of the traditional text passwords, which we so commonly use in our everyday lives. For the past years, researchers all around the world performed various studies around this subject. Many of them even begun suggesting and implementing different schemes for authenticating ourselves in order to decrease and eliminate, to a certain degree, these drawbacks that come with the text password authentication schemes.

As a response to the aforementioned problem, there has been several developments and studies of contradistinctive schemes. The most prominent scheme of authentication that is rising and still currently been studied, is the use of a graphical password as the mean of the user's authentication. By using graphical passwords, or in particular picture passwords, the aim is to enhance the usability and therefore the memorability of the user and its password. This suggestion is based on the research, which states that pictures can elicit emotions to the users based on their experiences with the scenes that are represented in the picture. Although there are many indications from past studies that strengthen this argument, the user studies around this subject are infrequent.

Thus, this study aims to provide a visualization tool for researchers in order to obtain effortlessly the data collected during their user study. Although, this will by no means eliminate completely the problem, it will remove a portion of the friction required to perform a user study. This system will collect and manipulate, where necessary, the data and represent them in predefined groups for the evaluator to examine. For the evaluation of the system developed, a use case of a user study was carried through, in order to gain a better understanding of its performance during a real-word scenario. Ultimately, its goal is to aid in the increase of user studies and to furthermore minimize the required effort.

1.3 Recapitulation

This thesis consists of six chapters. In the first chapter we acknowledged the problem with today’s most used way of user authentication, in addition to the lack of sufficient and conclusive user studies of an equally effective alternatives. Furthermore, it denotes the purpose of this thesis, which is to offer a data visualization tool that can be used during the evaluation phase of a user study in order to obtain effortlessly the data collected and ultimately, to urge a broader adoption of graphical password systems.

In the second chapter, the fundamental concepts of the subject around the study of user authentication are defined as well as the parent fields of science that are examining these concepts.

The third chapter presents past studies that have been realized around the subject of the evaluation of authentication systems, including methods regarding both the aspects of usability and security of a system.

In the following chapter, we discuss the implementation of the data visualization tool developed for the administrator of an existing picture graphical authentication system, which includes the technologies that were chosen to be used, as well as the general flow and structure of information, from the parent system itself to the web application implemented.

Chapter five, consists of the methodology and the evaluation of the interactive dashboard, by implementing a use case of a user study using its parent system. The data during this use case were collected and visualized by the system that was developed during this thesis.

Finally, in chapter six, we exhibit the results of our evaluation and user study which we then attempt to offer an effective conclusion of the aid provided using the interactive dashboard. Furthermore, in this chapter, we offer suggestions and discuss possible future expansions of the system developed.

2 Theoretical Background

In this chapter we will go through the fundamental concepts studied during my research, and my attempt to gain a better understanding of the theory behind many of the past studies and experimentations, as well as to gain a more sharpened perspective of the study we want to carry through.

In this thesis, the system that is being developed will serve as an aiding tool for the evaluation and examination of the data collected during the use of a graphical authentication system. Since its purpose is to increase the number of user studies for graphical authentication systems due to their promising results, it was deemed necessary to research their importance and provide the fundamental concepts that correlate to them in order to better understand them. By studying these following topics, we can understand the significance of graphical authentication, and therefore the significance of its evaluation which will reassure its benefits of adoption.

2.1 Emotion

Our first step towards understanding the importance of user authentication and ultimately its evaluation in order to push it towards a more broaden use across computer systems, was to acknowledge the connection of human nature with the different means of interaction.

Humans are known to be emotion-motivated beings. They make decisions and act based on past and expected experiences. This gives the very special ability that no other living creature has, the ability for the same event to cause different results based on the individual that is experiencing that event. It is only expected that these traits would be passed, on how a user experiences a computer system. Like we stated before, emotion is playing a critical role on the mental processes that occur during a certain event [1], [2], and such events can be the authentication and identification processes during the use of an authentication system.

2.2 Authentication

By definition, authentication is the process of proving one's identity. Since computer systems do not yield the ability to identify a person in the same immediate yet effective way a human can, the search for another mean of verification was emerged. The most common way of verifying the user's identity in today's computer systems is for the claimant to provide a shared secret with the system. This is also known as knowledge-based authentication. There are two more areas of authentication, the token-based and biometric authentication, which together with knowledge-based authentication, comprise the three main ways of verifying a user [3].

2.2.1 Knowledge-Based Authentication

As the name implies, knowledge-based authentication relies on something the user knows i.e., a password. For this method to work effectively it requires the user to be very familiar with the secret he chooses, or the secret is of very simple form. From that, we can already witness some of knowledge-based authentication's flaws. The most secure password is a randomly generated one, although this results in a password that is extremely hard to be remembered by the user and by taking into consideration the fact that today each individual has to remember multiple passwords, if every one of these passwords were randomly generated, it would be nearly impossible for anyone to remember multiple distinct strings of characters without any meaning behind them [4]. In order for the user to create and use a memorable enough secret, it would have to be either obvious enough that an attacker that knows the user would be in a very beneficial position, or it would be a very simple secret, that with enough persistence it could be cracked. The aim here is to have a password that is memorable without compromising security, therefore a password that achieves both security and usability. Knowledge-based authentication systems can be categorized into two distinct categories, the recognition-based systems, and the recall-based systems. We will later go into a deeper explanation of these two types of knowledge-based systems, specifically in our preferred field of study, the graphical user authentication systems.

2.2.2 Token-Based Authentication

Authentication systems that are built based on something that the legitimate user has in its possession at the time of authentication, are called token-based authentication systems. Token-based authentication system's aim, like the others, is to create a more secure verification process. The required token during the verification phase can be anything from a device to a hardware token. The verification process requires the users to have in their presence a certain device, like their smartphone, where they will receive a computer-generated code. With this code, the user will be able to verify the authentication process. Therefore, token-based authentication is mostly used as a verification method rather than a sole authentication scheme. For that reason, token-based authentication can be also referred to as a two-factor authentication (2FA).

2.2.3 Biometric-Based Authentication

At first glance, biometric authentication can seem to be the overall better option, by overcoming many of the drawbacks of the other authentication methods. Biometric authentication is relying on the unique physiological (biological) and behavioral characteristics of an individual, and establishes the authentication process by comparing the biometric data stored with the biometric data captured during the running authentication process [5].

Some of the major technologies for biometric authentication are:

1. Fingerprint Recognition:
   This automated method of identity verification by using an individual’s fingerprints is based on the fact that no two individuals can have the same fingerprints. Some of the disadvantages of fingerprint recognition come from the nature of the finger itself, which lead to degradation of the recognition rate when the finger is wet or wrinkled.
2. Iris Recognition:
   This method of verification implies the analysis of the individual’s iris for patterns by capturing an image of the iris and processing it for authentication.
3. Retinal Recognition:
   Unlike iris recognition, the retinal recognition method is based on the blood vessel pattern within the retina itself. This blood vessel pattern is shown to be unique for every retina.
4. Speech Recognition:
   Another method for biometric authentication is with the use of an individual’s vocal characteristics. During the speech recognition, the individual will speak a pass phrase into a sensor, which then will capture the acoustic signal and convert it into a unique digital code to be processed in order to identify the individual.
5. Face Recognition:
   Face recognition is based on the natural acknowledgment that the plethora of individuals have a unique face. For capturing/scanning the face, high-capacity cameras are used to lay a template of tha face, which will later be used for the

comparison and matching of the face. This type of recognition suffers from various challenges, such as the rotation of the face during the verification process as well as similarities in the faces, in rare occasions i.e., identical twins.

2.3 Human-Computer Interaction

Human-Computer Interaction (HCI) is an interdisciplinary area that is covered by computer science, psychology, sociology and anthropology, and industrial design[6]. Its main focus comes from the research of the user's interaction with any product, such as a computer system. HCI's goal is developing more interactive and personalized systems that will indirectly help user's with achieving their goals, where their goals could be anything from the actualization of a complex project to the accomplishment of the simplest task. The goal for an interactive system is to be as unintrusive as it can be so that it will allow the user to proceed with their tasks without any obstacles and without interrupting their mental process. For achieving this goal, an investigation of the traits that compile a computer system as interactive and usable is needed. A method of achieving this, is by giving the user a sense of familiarity, and thus allowing them to assume, predict and estimate the result of their actions.

2.4 Usable Security

As stated before, authentication is a very critical part of our computer systems since the beginning. To acknowledge the problem of user authentication we can look into usable security which is a subbranch of Human Computer Interaction, aiming to close that gap of usability and security of user authentication systems. An approach in achieving this, is by making the secret more memorable based on past experiences of the user. As we said before, humans tend to make connections based on their past experiences and an event is much memorable if it triggers an emotional response from the user. Thus said, a password scheme that depends strongly on its users' experiences will not only be more memorable but it will ensure better security due to the fact that it is nearly impossible for a third person to learn or gain the same experience that is needed in order to gain knowledge of the secret.

2.5 Graphical Password

It is no secret that there are problems with the traditional text password schemes. From security, to usability there are trade-offs to be made. As every aspect that we talked about so far, everything comes together to an idea and implementation of a new way of authentication. An authentication that relies on emotion, experiences, and individuality. Although it is not possible to implement the perfect authentication system, due to the limitations of today’s technology and computer systems, there have been multiple attempts for its implementation with promising results that have been gathered for further research and experimentation [7].

We can further categorize graphical authentication systems in the recognition-based systems and recall-based systems.

2.5.1 Recognition-Based Graphical Authentication Systems

In recognition-based systems, the users are presented with a set of choices, in the case of graphical passwords a set of pictures, in which they must decide whether or not the images presented were shown to them during the registration phase of the system and therefore, as the name implies, if they can recognize them. Thus, the decision to be made here is binary; its either yes, the image is known to the user, or no, the image is unknown to the user. Another possible implementation of a recognition-based graphical authentication system is to require the users to click on the correct images in particular order from a set of images that is shown to them.

2.5.2 Recall-Based Graphical Authentication Systems

Recall-based authentication systems, on the other hand requires the user to recreate the password that was created during the registration phase of the authentication. In our case of graphical password authentication, an implementation example is to require the users to register a set of gestures on a specific image and to later recall them and recreate them in order to successfully verify themselves. This example in particular is an implementation of a Cued-Recall password system. There is also another method of implementation, which is the Pure-Recall password system.

2.5.2.1 Cued Recall-Based User Authentication

During the authentication, the users are given some kind of aid, like a hint, in order to recall their password. That aid can be anything from a user assigned hint, to the picture in which they drew a set of gestures on, like in our occasion. Cued recall-based graphical user authentication aims to lighten the burden of the user's memory and enhance the usability of the system.

2.5.2.2 Pure Recall-Base User Authentication

In Pure Recall-Based systems, the users are not presented with any kind of external information. The users themselves have to provided anything that is needed in order to establish a successful verification of their identity with the system. The most common example of a Pure Recall-Based system, is the traditional alphanumerical passwords, where the users have to be able to recall their entire password.

2.6 Cognitive Passwords

Another approach of tackling the problem of usability and security was with the introduction of cognitive passwords. What this method suggests is that the user is presented with a series of questions that are constructed in such way that for the legit user it will be easier to remember but for an unknown claimant it would be extremely hard to guess. This relies in the fundamental ideology, which we discussed earlier, that states that an event that triggers a certain emotion to an individual, or an event that is tied to a certain experience, will highly differ and would be nearly impossible for the impersonator to guess [8]. This is neither a perfect solution, as people close to the legit user are very likely to be able to guess, or even know beforehand this information.

2.7 Cognitive Styles

Cognitive styles was also one of the concepts studied during this thesis' research so that we could gain a better insight on the individuality of a user both in means of processing and perceiving information.

Studies in learning styles were initially being developed as a product from the interest in individual differences. Initially, learning styles were referenced with the use of the term “cognitive styles” up until the 1970’s when the term “learning styles” begun to emerge and become the more commonly used term [9]. Learning was defined by Kolb as a multidimensional process whereby knowledge is created through the transformation of experience. These dimensions of process can be explained as the following four dimensions: 1. Affective; referring to senses and feelings of a person, 2. Symbolic; referring to the cognitive and thinking skills of a person, 3. Behavioral; referring to the actions of a person, and finally 4. Perceptual; referring to a person’s skills of observation. Corresponding to these four dimensions are four learning modes. These four learning modes are perceived as learning abilities and can be identified as the following: 1. Concrete Experience (CE), 2. Reflective Observation (RO), 3. Abstract Conceptualization (AC) and 4. Active Experimentation (AE) [10]. Learning style, based on Kolb, can be defined as the unique learning method presented by the learner during the learning process and situation. Later on, in 2013, it was defined as the unique combination of preferences for the four learning modes that we discussed earlier. From this unique combination a “kite” can be defined based on the relative preferences and since everyone’s learning style is different, everyone’s “kite” will also be unique.

Based on these studies, there have been categorized various groups of learning styles. In the sections that follow, we will explain in more detail two of the fundamental cognitive styles.

2.7.1 Wholist – Analytic Style

In this family the individuals that are better characterized as Wholists process information as a whole, meaning that they perceive the information as a set and not as the distinct bits of information that might be apparent. Individuals who are characterized as Analysts will tend to observe these distinct bits of information and follow specific steps towards the processing and understanding of that information. They will attempt to undertake the challenge they are faced with, by breaking it up into definite parts which they can better perceive.

2.7.2 Verbal – Imagery Style

Individuals who are described as Imagers are often individuals who tend to process information in terms of mental pictures, whilst on the other hand, people who are described as Verbalisers are considered to perceive and process the information in terms of words [9]. In addition, Imagers seem to tend to memorize with ease, content of information that they can assign meaning to it whereas Verbalizers have no problem in the memorization of most content that is of oral or written form.

3 Related Work

There have been various past studies that focus on the evaluation of several graphical password schemes and their comparison to the more traditional text password schemes. In this section we will take a look on previous studies implemented regarding the evaluation methods of several authentication systems, as well as the implementation of graphical authentication systems aiming to enhance different aspect of a user's experience.

As anticipated, evaluation has always been one of the most crucial aspects of a systems adoption. In order to create an evaluation tool, we must first examine the different routes one can follow into a correct evaluation of a system's integrity, and specifically in this case, of an authentication system's effectiveness. The following sections show information gathered during my research of past related work regarding the two main focuses of an authentication system's evaluation; the security of the system and its usability.

3.1 Security Evaluation

There has not been much research done to study the difficulty of graphical password cracking, as stated by some studies. In addition to that, since graphical password schemes are not very widely used, there is little evidence and not that many real reports of attacks on graphical password systems [11].

In the research paper "Security evaluation for graphical password"[12], A. H. Lashkari et al. discussed about the security of several Graphical User Athentication (GUA) algorithms. For the evaluation of the security of GUA algorithms they focused on the three attributes of security: 1) Attacks, 2) Password Space and 3) Password Entropy, which they named as the "Magic Triangle" for GUA security evaluation.

We will now be discussing the attacks on graphical password schemes, as this is the main attribute that is being considered in the aspect of security. Another research paper that delves into the security of GUA's is "Graphical passwords: A survey" [11]. We now can extract a list of 6 different possible methods of attacking with the purpose of acquiring the password.

In the following sections we will discuss those 6 different methods, and how each holds up to a Graphical User Authentication system based on the research composed.

3.1.1 Brute-Force

The first method of attacking is the traditional Brute Force Attack, where every possible combination of password is tried until the genuine password is found. The main mean of defense against this type of attack is the password space. The password space of a conventional text password is 94^N where N is the number of characters in the password (length of the string). It has been shown that there are graphical password schemes that can provide a similar or even larger password space than traditional text passwords.

Regarding the comparisson of the two types of graphical passwords, it is shown that recognition based graphical passwords tend to have a smaller password space than a recall based password. The research on brute-force attacks can be deducted to the conclusion that brute-force attacks, as expected, are more difftcutl to be carried out against graphical passwords, mainly due to the nature of the attack where it would be required for the attack program to generate accurate mouse motions.

3.1.2 Dictionary Attacks

Dictionary attacks are very similarly defeneded like brute-force, as they are a form of brute-force attacks. Since recognition based graphical passwords concern user mouse input, it is not effective to carry out dictionary attacks against these type of password. On the other hand, recognition based graphical passwords are more prone to dictionary attacks, as they are composed of a finite number of passwords. Regardless, dictionary attacks even on recognition based graphical passwords are of much more complexity in comparisson to dictionary attacks on text passwords.

3.1.3 Guessing

Guessing is one of the attack methods that graphical passwords seem to be more prone to than text passwords. This is mainly true, for the reason that graphical passwords often seem to have hotspots, that users focus on, which then leads on more predictable passwords.

3.1.4 Spyware

By taking into consideration the fact that most graphical password system do not require the use of the keyboard, but instead the use of the mouse, key logging or key listening would be completetly ineffective against them. In addition, even with the use of a tool to mouse log the movement and position of the mouse, its performance would be highly afftected be many more factors like the window size and position but also the timing of each click and movement.

3.1.5 Shoulder Surfing

Any form of password scheme that depends on recall of information, assumpts that the password is consistent and the mean of input remains the same in each authentication session. Traditional text password but also recall based graphical passwords are prone to shoulder surfing. Regarding the recognition based graphical password schemes, there has been some research and implementation done, in order to break that consistensy of input and therefore raise the scheme’s resistance to shoulder surfing [13].

3.1.6 Social Engineering

Due to a graphical password scheme’s nature, not only is it extremely odd for a user to give away by accident their password, it is even extremely inconvinient, difficutl and time consuming for an attacker to make the effort to phish for their password.

3.2 Usability evaluation

A major argument from many other researches, in regards to graphical passwords over traditional text passwords, is that they are much more memorable to the user. In an effort to define usability we have derived to the following definitions. From the book “Sustainable design: HCI, usability and environmental concerns” by Pedro Isaias and Tomayess Issa, usability is defined as a quality of the interaction in terms of parameters such as the time taken in order to perform certain tasks, the number of errors made, and the time to become a competent user [14]. Usability is also being defined by the ISO 9241-11 standard as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified content of use [15].

A. Eljetlawi and N. Ithnin did a comprehensive study of the usability features that a recognition-based graphical password scheme should be comprised of [16]. The researchers concluded to four critical features that a recognition based graphical authentication scheme should have:

1. Ease of use
2. Ease of creation
3. Ease of memorization
4. Ease of learning

T. Khodadadi, A. Islam, S. Baharun et al. listed nine categories of the major usability features that can be used for the implementation of a recognition-based graphical password system [17]. The nine categories are as follows:

1. Images that are Meaningful
2. Images Assigned by Users
3. Images Category
4. Easy to Create
5. Fun to Use and Easy
6. Easily Executed
7. Nice and Simple Interface
8. Easily Understood and Learnt
9. Easy to Correct

A common conclusion and aftereffect, that all the studies I have mentioned above have come to, is that graphical passwords and in particular recognition-based graphical passwords require an extensive amount of time for the registration, but also the log-in phase of the system. This observation, S. Xiaoyuan, Z. Ying, and G. Owen have also documented in their research paper “Graphical passwords: A survey” [11]. They commented that due to the long time that is required during those phases, users might find these processes tedious. This statement displays one flaw of recognition-based graphical authentication systems in regards to the usability of the system.

K. Yee has recently listed ten HCI design principles that can be of use when designing a security system in the interest of improving its usability. These ten principles are as follows:

1. Path of Least Resistance
2. Appropriate Boundaries
3. Explicit Authorization
4. Visibility
5. Revocability
6. Expected Ability
7. Trusted Path
8. Identifiability
9. Expressiveness
10. Clarity

4 Description of System

In this chapter we will examine the technologies used for the development of the administrator dashboard, as well as the flow of information from the databased to the user interface and vice versa.

4.1 Introduction

The argument that graphical authentication is enhancing the memorability of the password is the most prominent among the most studies that are being carried out. During my research of graphical user authentication systems, I have observed that although there are numerous suggestions and executions regarding the implementation of an authentication system of this nature, there still is not enough convincing evidence for and user studies to back up this argument. Designing and implementing graphical password systems can be accomplished with several approaches. Currently, the evaluation and experimentation of the existing graphical user authentication systems is of great demand due to the limited number of studies and involvement of users.

The web application designed and implemented during this thesis, is an interactive dashboard for the administrator of an existing Graphical User Authentication system, that provides the data and statistics of the effectiveness of the user's passwords in terms of usability. In addition, this system aims to aid with the evaluation process a user study, such of the different types of users in respect to the effects that personal or generic pictures have on the usability of their picture passwords. This system is a part of a parent graphical authentication system, "PGA: Picture Gesture Authentication" which was also used during these studies: [18]–[22].

4.2 COVID-19 Repercussions on the Implementation of the System

The current situation of COVID-19 affected a very big part of the development of my dissertation thesis. Since I had no access to the University's facilities, the initial goal to use the Emotiv EPOC headset in order to extract the user's emotional data which would enable me to calculate information such as motivation, attention and memorability was scrapped. Instead, we used raw EEG data from this website [23] which unfortunately was unprocessed and since the preprocessing has to be done with the use of Emotiv's API which I had no access without a headset, I only opted to represent those data rather than calculate the information stated above.

4.3 Tools & Technologies

In this section of Chapter 4 I will be addressing the technologies used in order to collect, manage and manipulate the necessary data in addition to establishing an effective implementation of the administrator dashboard.

4.3.1 Docker

I worked with Docker, an open-source platform, for developing and running my web application. The main reason that Docker is generally chosen for software development is the ability to enclose and package your applications into isolated and secure environments, called containers. These containers can run directly on the host machine's kernel, meaning that they are lightweight enough that it allows you to run more containers than you could if virtual machines were used instead. In simpler words, with Docker I had the ability to develop my web application without the anxiety of it not working on other machines due the different nature of each environment and technologies, since the docker container runs isolated from the environment of the machine.

4.3.2 Python – Django

The programming language used in the development of the web application is Python [24] (v3.6) and specifically Django [25], a high-level open-source Python Web framework hosted by Python's "Python Package Index" (PyPI) [26].

For the structure and manipulation of the data used in my web application, Django provides an abstraction layer, called the "Models" layer. In the models we are able to provide characteristics and specific behavior to individual piece of data. Essentially, each model in Django is a Python class, and each model has its attributes. These attributes basically represent a database field each with its own type (e.g., INTEGER) and options (e.g., null). In order to process the user's request and providing a response Django provides the "Views" layer. In the views layer, I can manage the request from the user (i.e. POST request, GET request) access the database if necessary and then return the corresponding response. In addition, Django also offers the capability to create templates. This function is provided by the "Template" layer of Django, which is characterized by its designer-friendly syntax for rendering the information provided by the designer of the system, that is eventually going to be presented to the end user.

Furthermore, another way of collecting the data provided from the end user to the web application, is with the use of Django’s “Forms”. Forms support the collection and manipulation of the data that is being input into the forms. Some forms examples are the forms existing on the registration page, user login page and admin login page. For each of these forms you can determine and define the required fields and the specific models (from the model layer we discussed above) in order to manipulate the correct information from the form.

4.3.3 PostgreSQL

For the manipulation and management of the data handled by the web application, I used PostgreSQL. PostgreSQL is a free open-source database system that uses and extends the SQL language. PostgreSQL is packed with plentiful features aimed to aid the developers build their applications. PostgreSQL’s high extensibility can be documented from features like defining your own data types, building your own functions and coding in different programming languages without the hustle of recompiling the database [27]. To access the PostgreSQL database I used the docker command line [28].

4.3.4 JavaScript - jQuery

In order to establish a communication between the client and the server JavaScript programming language was used. With JavaScript, we can establish an interactive web application, and in combination with the jQuery JavaScript library the HTML document manipulation etc. is being much easier to be dealt with.

jQuery, as we mentioned above, is a cross-browser JavaScript library which offers various features like DOM element management, handling certain events triggered, animation creation and AJAX application development.

Specifically, I used JavaScript and jQuery to make a call when there is the need, to access certain functions and methods from the server side. The processing is being established on the server side, and afterwards a JSON (JavaScript Object Notation) object is returned. If the call is made with the purpose of receipt of information, the function on the server side will create the JSON object containing all the necessary data.

The functions that I am referring to, in my implementation, are functions located in the “Views” layer of Django, which we discussed earlier about.

4.3.4.1 AmCharts JS Library

For the representation of the data the AmCharts JavaScript library was used [29]. With this library we have access to several functions in order to create graphs and charts. For the data used in the graphs, we are accessing the database of the system containing the needed data and processing the data if necessary, in the functions that we developed. The data passed onto the AmCharts functions are in the form of JSON objects that we created in our functions in the Views layer of the system.

4.4 Database

For the structure and implementation of the database, as stated in section *4.3.3* PostgreSQL was used. During the implementation of the web application and the evaluation of this study, the PostgreSQL was accessed using the docker command line. The following sections will explain in detail only the tables that were created or used during the development of the interactive administrator dashboard, as well as the fields of each table.

4.4.1 Users

This table preexisted along the parent system that I was working on; therefore, I did not create this table. Although I did not create the table, I worked with the data provided by it so that I can extract the important information for the usability evaluation of this system. The “Users” table **web_app_user** is consisted of eleven fields. The first field is the id of the field, named **id**. This field is automatically increased with each new entry to this table. The next fields are the username, email, age, gender, consent and image type of the user, named **username, email, age, gender, consent, image_type** respectively. The data for these fields are filled based on the data that is provided by the users during their registration phase. The **image_type** field represents the type of the user i.e. retrospective or generic user, which is also based on the user’s input on the registration form. The first seven fields are also shown in an example in **Error! Reference source not found.** below. The last four fields on the users’ table are the id of the image that the user selected as their password canvas, the timestamp representing the time and date of the registration, the user’s unique id and the indication of whether or not the user has activated its account. The fields are named as **image_id, timestamp, uuid, is_active** respectively and an example of these four fields' values can be seen in **Error! Reference source not found.** below. The field **uuid** that indicates the user's unique identification is generated using the uuid module for python that provided an invariable UUID object [30] as specified in RFC 4122 [31].

id	username	email	age	gender	consent	image_type
1	name@gmail.com	name@gmail.com	23	Male	Accept	generic

Table 1. Example of the first seven fields of the **web_app_user** table

image_id	timestamp	uuid	is_active
2	2020-12-29 19:33:58.087079+00	2876c0d564054a7d	t

Table 2. Example of the last four fields of the **web_app_user** table

4.4.2 Passwords

The passwords table, named **web_app_password** stores all the data related to the users' passwords. For the implementation of my system, I needed to access and use the data of only some of the fields on this table. The fields that were of my use were the id of each entry, the type of gesture one, two and three, the total time taken to create this specific password, the total times to enter the first, second and third gesture and the total failed attempts to verify the password during the creation of the password. These fields are named as **id, gesture_one_type, gesture_two_type, gesture_three_type, total_time_creation, total_time_first, total_time_second, total_time_third** and **total_failed_attempts** respectively. Each time recorded entry is measured in milliseconds and the types of each gesture can be either "TAP", "CIRCLE" or "LINE". An example of values for these fields is shown in the Table 3**Error! Reference source**

id	gesture_one_type	gesture_two_type	gesture_three_type	total_time_creation
1	LINE	TAP	CIRCLE	3079

total_time_first	total_time_second	total_time_third	total_failed_attempts
1028	1065	986	0

Table 3. Example of values in the specified fields of the **web_app_password** table

not found. below.

4.4.3 Login Attempts

This table contains the data that are captured during each login session of each user. The table is named **web_app_loginattempts** in the PostgreSQL database. This table is consisted of the following fields that were necessary to use and modify for the implementation of the administrator dashboard: the id of the login session, the total failed attempts during that login session, the total time until the user has successfully logged into the system, the time and data of the login attempt and the user's id. These fields can be found by the following names in the database: **id, total_failed_attempts, total_time_until_successful_login, timestamp,** and **user_fk_id.** The primary key of each field is the **id** and the foreign key that makes the relation between the **web_app_loginattempts** and **web_app_user** is the **user_fk_id.** Below, in Table 4, is an example of the values of each data field in this table.

id	total_failed_attempts	total_time_until_successful_login	timestamp	user_fk_id
1	2	4212	2020-12-29 15:17:36.939752+00	2

Table 4. Example of the values in a field in table **web_app_loginattempts**

4.4.4 EEG data

In this table are stored the eeg data that were uploaded by the admin using the administrator dashboard for each user. This table can be found in the PostgreSQL database under the name **web_app_eegdata**. The table consists of these fields: the unique id of the entry which is also the primary key, the fields af3, af4, t7, t8 and pz which correspond to the 5 rows of the csv file uploaded and the location of the electrodes that recorded the eeg data, the time and data of the database entry and the id of the user that the data was collected. The fields can be found by the following names in the database: **id, af3, af4, t7, t8, pz, timestamp, user_fk_id**. Each of the electrode location fields contain a list of decimal number which are the raw eeg data collected from each electrode. Each list contains around 384 values. Due to the size of each list, in the table below the lists are represented in the form of: {i_0, …, i_N} where N = ~384.

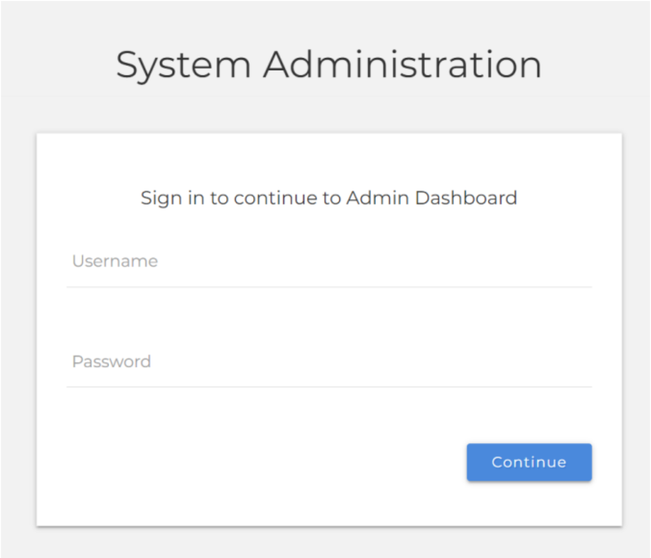
id	af3	af4	t7	t8	timestamp	user_fk_id
1	{4287.03, … ,4576.27}	{4457.03, … ,4315.54}	{4114.23, … ,4347.22}	{4289.43, … ,4257.57}	2020-12-29 15:17:36.939752+00	2

Table 5. Example of the values in the fields of the **web_app_eegdata** table

4.5 User Interface and Implementation

For the sake of simplicity and minimization of redundant steps, the data collected and processed by the system is presented to the administrator in a total of two pages. The first page concerns the data for each user individually, and the second page concerns a generic representation of the data as a whole.

In order for the administrator to access the dashboard, they first have to login to the system, using a regular text password as shown in the figure below.



System Administration

Sign in to continue to Admin Dashboard

Figure 1. Administrator sign in screen

4.5.1 "Per User Stats” Page

After the administrator has successfully signed into the system, they will be prompted with the first page of the Administrator Dashboard. In this page the administrator of the system is presented with a search box, as shown in the figure below, where they can search the users that are registered in the system by typing their usernames. The usernames of the users are the emails with which they used to register in the system.

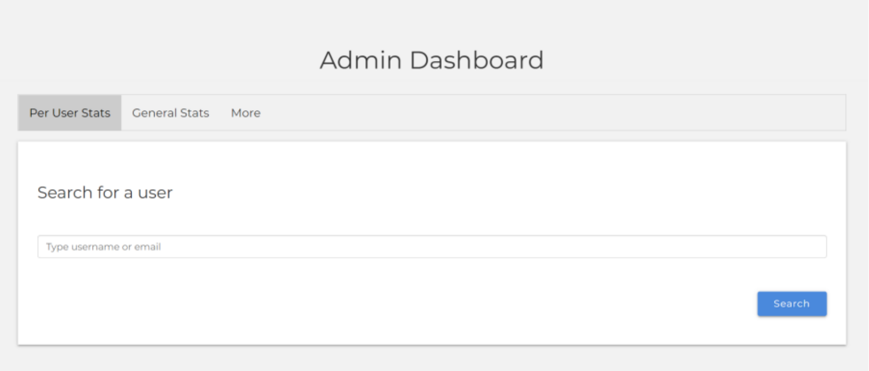
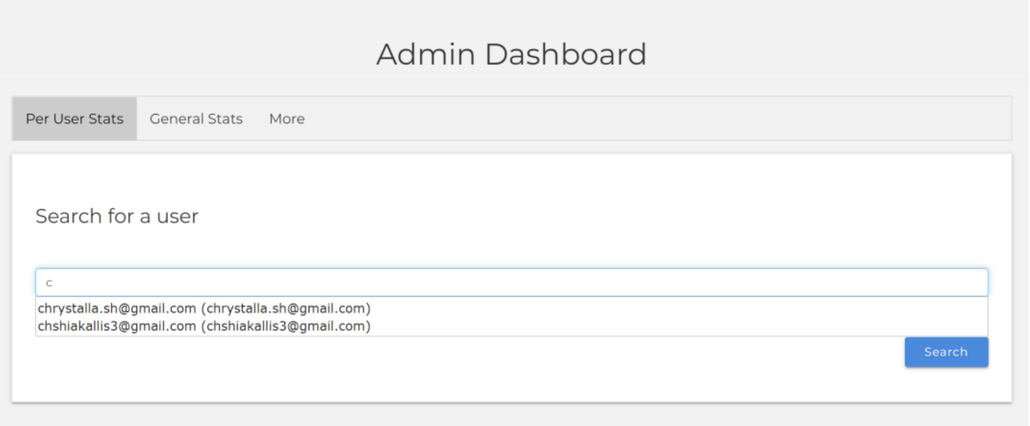


Figure 2. Search box for individual user stats

As the administrator will begin to type the user's username, the system will autofill username suggestions based on the matching characters that the administrator has typed so far.

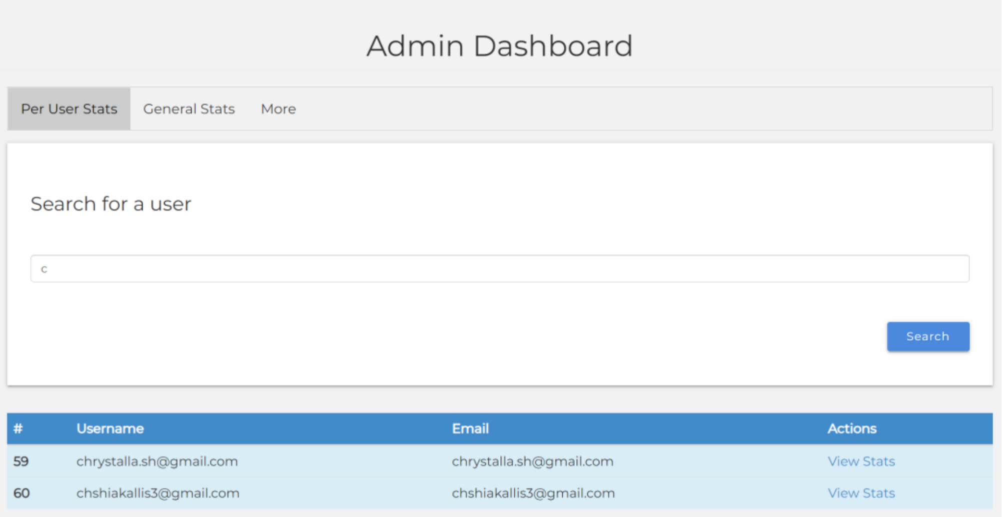


c

chrystalla.sh@gmail.com (chrystalla.sh@gmail.com)
chshiakallis3@gmail.com (chshiakallis3@gmail.com)

Figure 3. Username autofill feature

After the administrator has finished with his search, they can either hit the enter key on their keyboard, or click the "Search" button shown on the interface. With the successful search of a user, meaning if the system has found users with the matching username, a table will appear below the search box with the results as shown in the figure below. The table consists of the user's id, the user's username, the user's email and a "View Stats" action to view statistics about the specified user. The user's id is created and assigned to a user based on the order of its registration. The user's username and email in this occasion are the same, as we have already stated above.



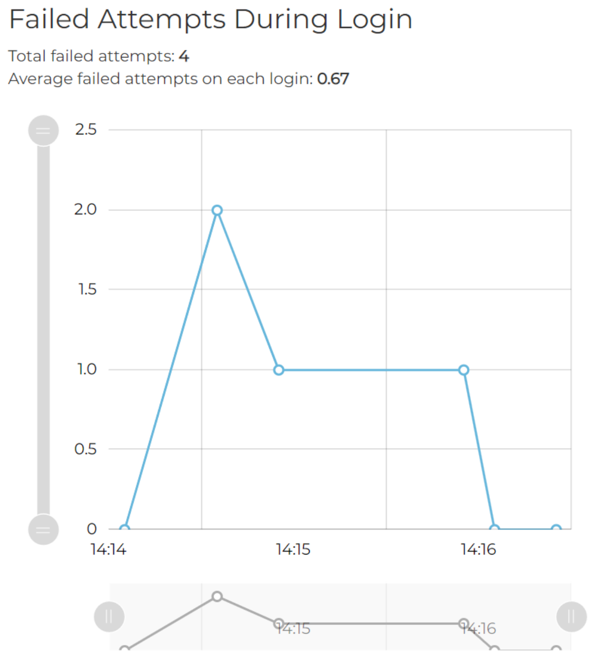
Search for a user

c

#	Username	Email	Actions
59	chrystalla.sh@gmail.com	chrystalla.sh@gmail.com	View Stats
60	chshiakallis3@gmail.com	chshiakallis3@gmail.com	View Stats

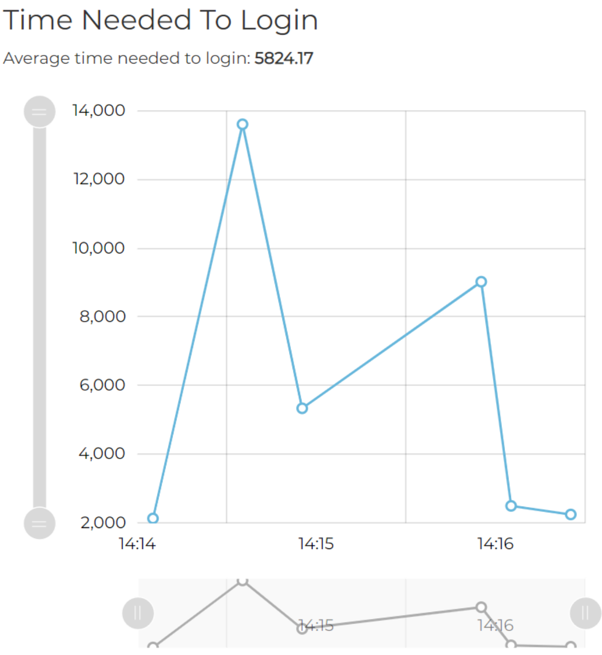
Figure 4. Search results table

By clicking the “View Stats” action button, 2 graphs will appear below the table. The first graph shows the number of failed attempts during each login session, and the second graph shows the time that the user needed in order to successfully login into the system on each session, as shown in the respective figures below. Along with the graphs is shown the total failed attempts and the average failed attempts in each session, based on all the user’s session. The respective values are also shown for the graph presenting the time a user needed to login.


Failed Attempts During Login

Total failed attempts: 4
Average failed attempts on each login: 0.67

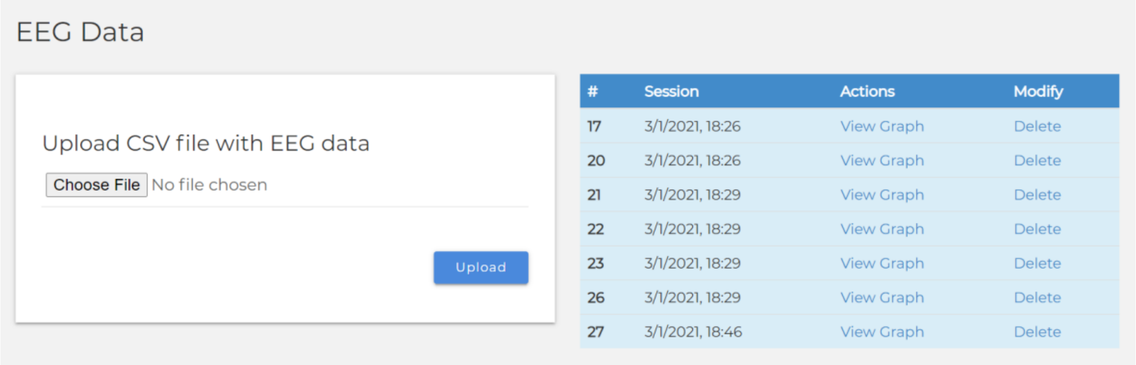
Figure 5. User's failed attempts during each login session


Time Needed To Login

Average time needed to login: 5824.17

Figure 6. User's required time to login during each login session

Below the two graphs there is located a field where the administration can upload a csv file, containing EEG data from that session. The file that is uploaded has to be of certain format and has to have .csv extension. The representation of the data is just visual, so the preprocessing has to be already been established. If the user had already been assigned EEG data then a table will be apparent next to the upload field. From the table the administrator has the option to "View Graph" or to "Delete" the EEG data entry of the table.



EEG Data

Upload CSV file with EEG data

#	Session	Actions	Modify
17	3/1/2021, 18:26	View Graph	Delete
20	3/1/2021, 18:26	View Graph	Delete
21	3/1/2021, 18:29	View Graph	Delete
22	3/1/2021, 18:29	View Graph	Delete
23	3/1/2021, 18:29	View Graph	Delete
26	3/1/2021, 18:29	View Graph	Delete
27	3/1/2021, 18:46	View Graph	Delete

Figure 5. EEG file upload section and EEG data entries in database

When the "View Graph" is selected then below this section appear five distinct graphs, each showing the data that was recorded from a single electrode using the EEG headset.

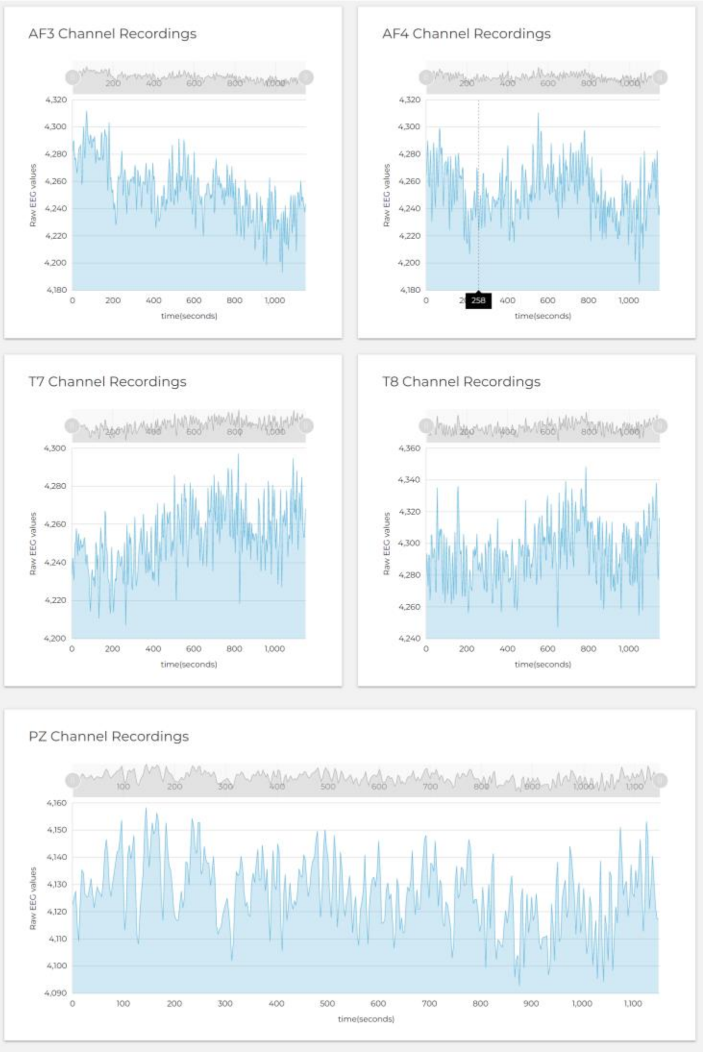


Figure 6. EEG recordings obtained from database

4.5.2 “Generic Stats” Page

To go to the second page, the administrator has to click on the 2nd tab on the sub-navigation pane located beneath the main header of the administrator dashboard page. On this page the administrator is presented with various graphs and charts. The data shown in this page can be divided into three main categories and all in each graph of every category, the values are presented distinctively for the two types of users, which are the retrospective users and the generic users. The data chosen to be collected were done with the system’s usability evaluation in mind. The three categories are as follows:

1. **Password Creation:**

   This category involves the data that was collected from the system’s database appertain to the password creation phase of the graphical user authentication. Each graph shows the metrics and values of the two types of users which as we stated before are the retrospective users and the generic users. This category consists of seven graphs/charts, the average time for each user group to create their picture passwords, the average time for each user group to create each of the three gestures of the picture password, the maximum time that a user from each group needed to create their password, the minimum time that a user from each group needed to create their password, the maximum time that a user from each group needed to create each of the three gestures of the picture password, the minimum time that a user from each group needed to create each of the three gestures of the picture password and finally the total failed attempts of each user group during the password creation phase. The data collection methods will be later discussed in more detail.

2. **Login Attempts:**

   This category has to do with the data collected during each login attempt of every user. It includes both the successful and failed attempts, if any, of every login session. In this section of the page, the administrator is presented with four charts, regarding the average time that each user group needs in order to successfully log into the system, the maximum time that was recorded for a user of each user group, and the preferred type of gesture for each of the three total gestures for the retrospective users and another one showing the corresponding data for the generic users.

3. Miscellaneous:

In this category, the administrator can view other information not exactly related to the password creation phase nor the login sessions. In this section, the administrator is presented with some more generic information cards. These cards are the most preferred gesture combination (i.e., picture password) amongst retrospective and generic users, the least preferred gesture combination.

A use case of the data collected from this page will be shown in Chapter 5: Evaluation where we used this data for our user study implemented in this dissertation project

5 Evaluation

In this chapter we will discuss the details of the evaluation procedure. The goal of the evaluation was to investigate the effects of retrospective images and to users with past experience of the scenes represented in those images in contrast with generic images where the users had zero knowledge or experience with the portrayed scenes using the system developed during this dissertation project.

5.1 COVID-19 Repercussions on the Evaluation

Due to the current situation of COVID-19, the evaluation of the system and the user study was affected. Since there are limitations to social gatherings, I was not able to work with multiple participants. The individuals that participated were three family members and three fellow computer science students. They were all participating one at a time in order to comply with the current day's laws and of course for our own safety.

5.2 Motivation of Evaluation Study

This evaluation study was implemented as a use case of a user study in order to gain an insight on how the system implemented during this dissertation project will perform in a real-world study.

This example of a study, focused on examining the effects that various categories of pictures have, when used in a Graphical User Authentication system. The two categories of images chosen in this study were retrospective images and generic images. Retrospective images represent scenes with which the users already have an established cognitive connection with them from past experiences and which are highly related to the users. Generic images on the other hand show scenes with no particular context and that have no meaning for the user. Specifically, in this study, we chose to present the users which are currently studying at University of Cyprus, pictures taken on the campus or in the universities various areas, such as the cafeteria, labs etc. To the users who are not students at UCY we chose to present pictures totally unrelated to any past experiences and fully unknown. This distinction was decided so that we can test the polar opposites of the possible user-image pairs. In addition, we were motivated to implement this study in order to test in real use, the tool developed during this dissertation project, and how efficiently collects and presents the data.

Research Question

Can the use of retrospective images as a cue in a picture gesture authentication system enhance the usability and security of the system?

Hypothesis

H1: The users with retrospective images are going to need less time to create their password due to their possibly existing prior connections with the scene represented in the picture.

H2: The users with generic images are going to need more time to create their password due to the time they will possibly need to observe the image and find candidate gesture spots on the picture.

H3: The users that are assigned with retrospective images are going to create more complex passwords due to their possibly existing prior connections with the scene represented in the picture and their more detailed observation of the scene.

5.3 Evaluation Tools

To accomplish an evaluation of the performance of the tool developed in this project, we used the existing Picture Gesture Authentication system that was discussed in the earlier passwords for the generation of the data during the password creation, and the login sessions for each type of images. In addition, for the visualization and analysis of the results we used the administrator dashboard that was developed during this project.

5.3.1 PGA System

The Picture Gesture Authentication system that was used for the creation of passwords and login attempts by the users was the one that we already mentioned in the Chapter 3: Related Systems. This authentication system is a Cued Recall-Based Graphical User Authentication system in which the participants are presented with nine images to choose one from, which will then act as the cue to create their gestures one. The possible gestures supported by this authentication system are “tap”, “circle” or “line”.

5.3.2 Administrator Dashboard

The administrator dashboard was developed so that the researcher, or simply any administrator of the system can gain a more comprehensive and easy view of the data related to the passwords created by the users of the system. This tool acts as aid to the administrator and gives him an insight of the data that was recorder by representing them visually in the pages of the dashboard.

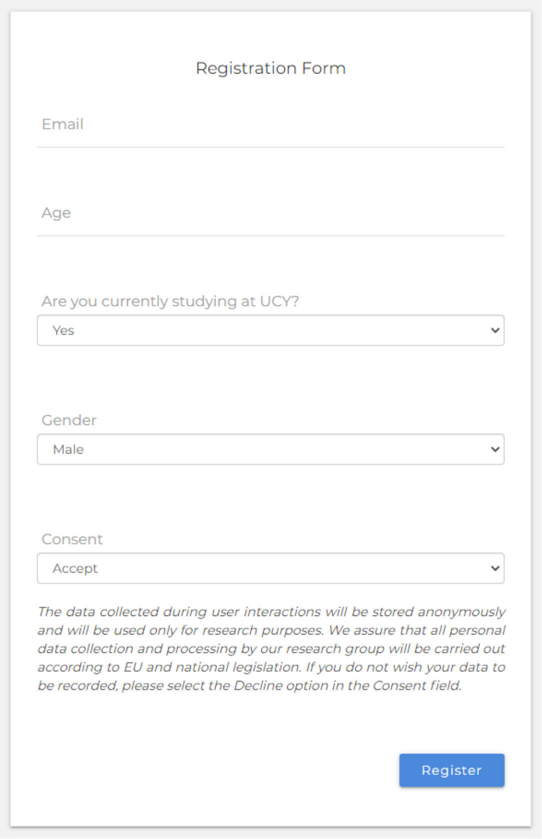
5.4 Participants

A total of six individuals participated in this study (five males and one female) and their age ranged between 23 and 62 years old. Three of the participants had no prior experiences with University of Cyprus and the remaining three were currently studying at UCY. Those who were currently studying at UCY were given retrospective images (showing scenery/classrooms from UCY) as their cue and those who had no prior experience, were given generic images. The participants with no prior experience, although they could have also gotten UCY related images, they were instead given generic images in an attempt to enhance the contrast and consequently the possible effects to be observed.

5.5 Procedure

5.5.1 Registration Phase

For the registration phase, the users had to fill in a form with their demographic characteristics. The fields that each participant was required to fill for this evaluation study, was their email, age, whether or not they are currently studying at UCY, their gender and their consent, as it is shown in Figure 7. Afterwards, based on whether or not they are currently studying at UCY they were presented with a total of nine retrospective images if they were currently studying or nine generic images if they were not. From those nine images they were requested to choose one of them which will then act as the cue during the password creation and login sessions. When a picture is selected, they were then prompted to create three gestures which will compose their password. The types of each of the three gestures can be either tap/click on the screen, draw a straight line or create a circle. During the registration phase the users can see on the picture a representation of their password gestures in order to make sure that the system registered the correct password. In the case that they decide to change the password during the registration phase they have the option to press the restart button and start all over. Once they are sure for their password, they need to enter it once again, in order to verify their password. The participants were all using the same Dell Latitude laptop for both the registration and verification phase (login session).



Registration Form

Email

Age

Are you currently studying at UCY?

Yes

Gender

Male

Consent

Accept

The data collected during user interactions will be stored anonymously and will be used only for research purposes. We assure that all personal data collection and processing by our research group will be carried out according to EU and national legislation. If you do not wish your data to be recorded, please select the Decline option in the Consent field.

Figure 7. Registration Form

5.5.2 Login Sessions

This phase took place over the course of five days. A login session consisted of the participants firstly entering their email and then when they were presented with the picture, that they selected as their cue during the registration phase, to attempt and log into the system with their picture gesture password. During this phase there are no indications on the image for each of the three gestures. If a user entered the password incorrectly, a prompt appears to inform them to try again.

The first day that they requested to login was at the day of the registration, right after they were registered to the system. The users were requested to login in a total of three times in the span of five days with one day gap each time. So, their second login session was held two days after their first, and accordingly the third and last login session was held two days after their second session. During these procedures I was present and observing each participant in case of any questions or difficulties might had pop up.

5.6 Results Analysis

By using the interactive dashboard, we were able to easily have an insight of the user data collected during our use case and if necessary, we could further examine the data of the users individually, using the search function of the dashboard.
In the following sections, the graphs and charts shown were generated and presented in the dashboard automatically, removing any friction between the collection and examination of the data during the user study.

5.6.1 Registration Phase

For the observation of the results during the registration phase (password creation) we direct to the General Stats page on the administrator dashboard. On the first section are presented all the data regarding the password creation phase. The data that will be discussed in the next sections of this thesis are: the average time that users with retrospective image cues required to register to the system in comparison to the required time that user with generic image cues required, the average time that users with retrospective image cues required for the assignment of each gesture of their password in comparison to the respective times that users with generic images required, the comparison of the maximum time a user of each image type required to complete the password creation, the comparison of the minimum time a user of each image type required to complete the password creation, the comparison of the maximum/minimum time that each gesture of the password needed to be assigned for each of the image groups, the total failed attempts that were made during the password creation, the total restarts of the password creation for each group, the maximum restarts from a user of each group, the minimum restarts from a user of each group, and the number of times that each type of gesture type was selected as the third, second, or third gesture of the password, for both image type user groups.

5.6.1.1 Average Time to Create Password

From the administrator dashboard we can observe the following graph (Figure 8 & Figure 9) which shows that the users with retrospective images required on average 8568 milliseconds to create their password in comparison with the average of 11380 milliseconds that users with generic images needed. This time only includes the time taken to successfully create their passwords i.e., if a user restarted the creation process, the time restarted as well.

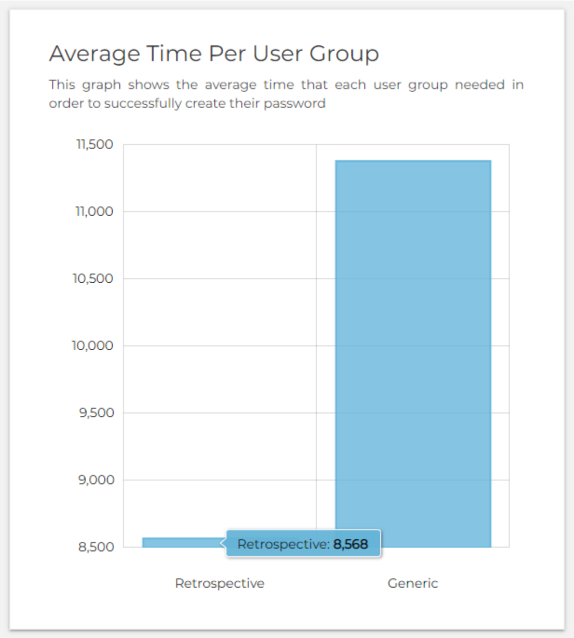


Figure 9. Average time to register for users with retrospective images

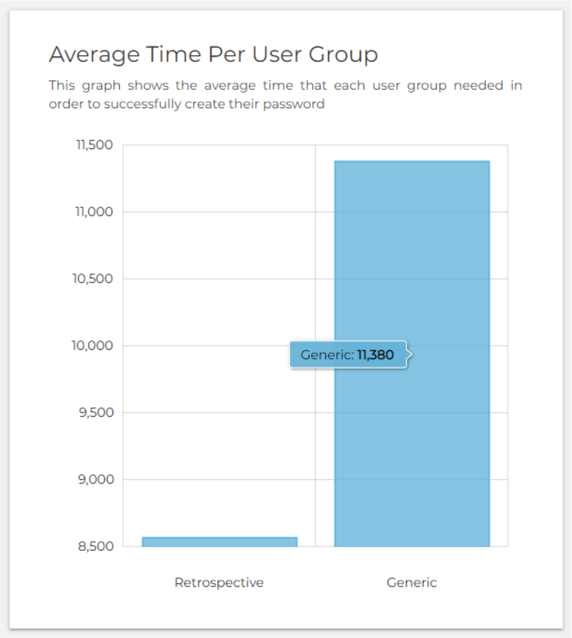


Figure 8. Average time to register for users with generic images

Observations

The users with retrospective images required less time to create their passwords in comparison to the users with generic images. Specifically, they required approximately 3 seconds less to create their password. Although this difference is not such a significant one, it complies with our hypothesis that users with generic images would require more time to create their password because they would need time to observe and process this new scenery presented to them and then decide on the spots and type of their password.

5.6.1.2 Maximum/Minimum Time to Create Password

The following charts (Figure 10) show the maximum time that a user from each image assigned group needed to create their password and the minimum time respectively. The maximum time needed for a user with retrospective image to create their password was 17456 milliseconds whereas the maximum time needed for a user with a generic image to create their password was 14379 milliseconds. The minimum time for a user with retrospective image to create their password was 3947 milliseconds whereas the maximum time needed for a user with a generic image to create their password was 6974 milliseconds.

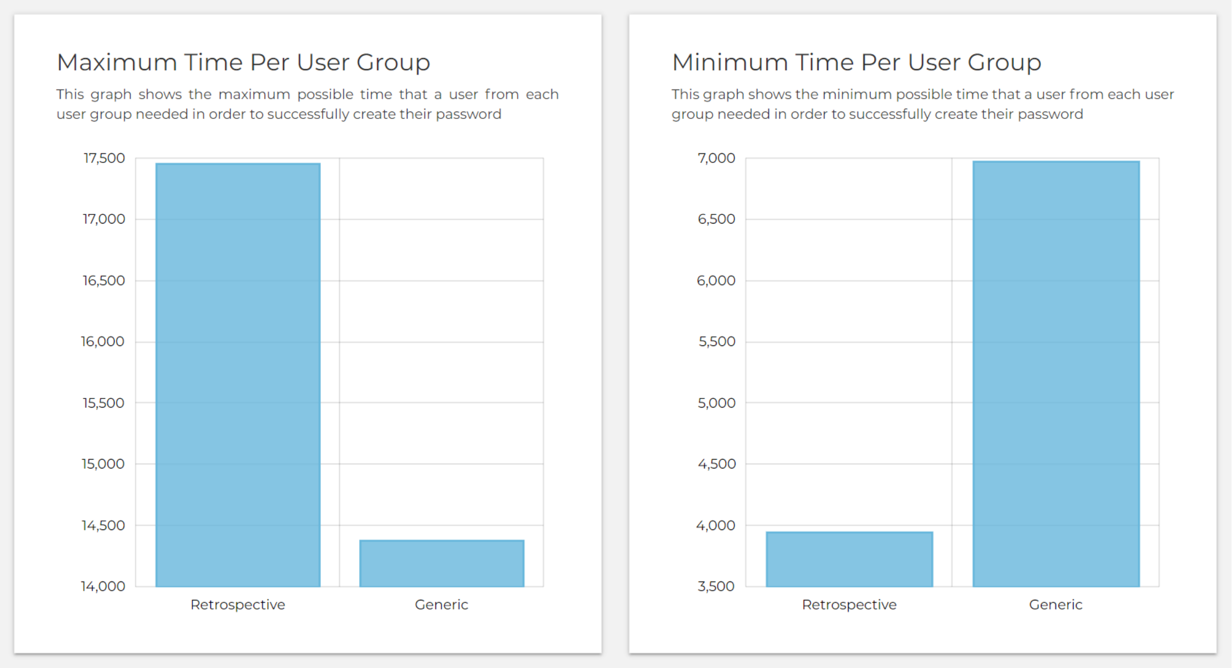


Figure 10. Maximum and Minimum time for a user of each group to create their password

Observations

From the charts above we can obtain the information that the user with the maximum time required to create its password using a retrospective image, needed approximately 3 seconds more than the user with the maximum time required to create its password using a generic image. From the observation of the password creation process the "retrospective" user that required this much time was creating a more complex password and this resulted in restarting the creation process which we will see afterwards in a later chart. This observation also complies with our hypothesis that "retrospective" user will tend to create more complex passwords.

5.6.1.3 Maximum/Minimum Time per Assigned Gesture

The following charts (Figure 11) show the time taken for each gesture that comprises the password. From the charts we can see that the maximum time to create the first gesture for a user with a generic image was more than a second higher than the time needed for a user with a retrospective image, although the minimum time for a user with a generic image seems to be slightly lower than that of a retrospective.

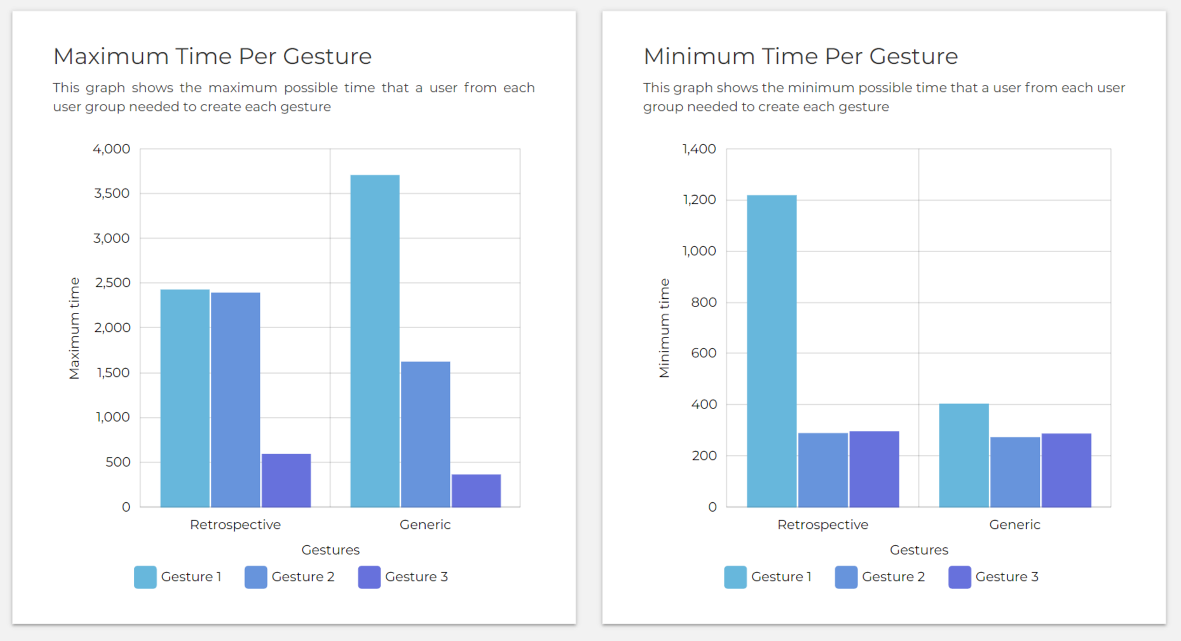


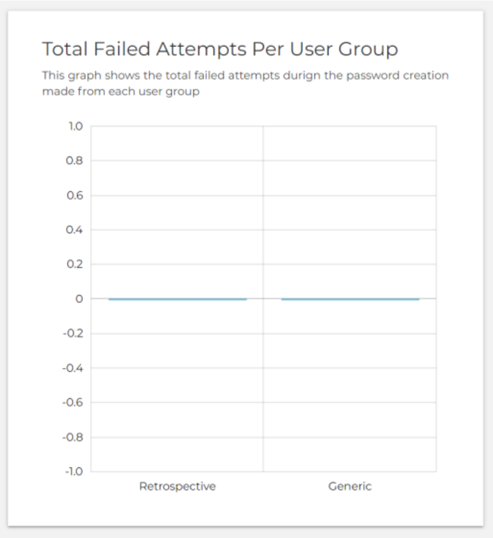
Figure 11. Maximum and Minimum time for each gesture to be assigned from a user of each image group

Observations

The maximum time for a user with a generic image is 3708 milliseconds and for a user with a retrospective image is 2429 milliseconds. For the user with the generic image, it took more than a second to create the first gesture. Although this is not a significant difference, if we had to address this difference it would be due to the initial observation and process that the user with the generic image had to go through. The rest gestures were created with not a very significant difference.

5.6.1.4 Total Failed Attempts During Password Creation

From the graph on the right, we can see that none of the users failed at the recreation phase of their password.



Observations

The fact that no user failed to verify their password shows that the system registered correctly their gestures and they themselves had not made any unnoticed personal mistakes during the password creation.

5.6.1.5 Total Restarts of the Password Creation Process

From the data collected and shown in Figure 12 we can observe that "retrospective" users restarted their password creation process in total of four times, whereas the none of the "generic" users restarted the process at all.

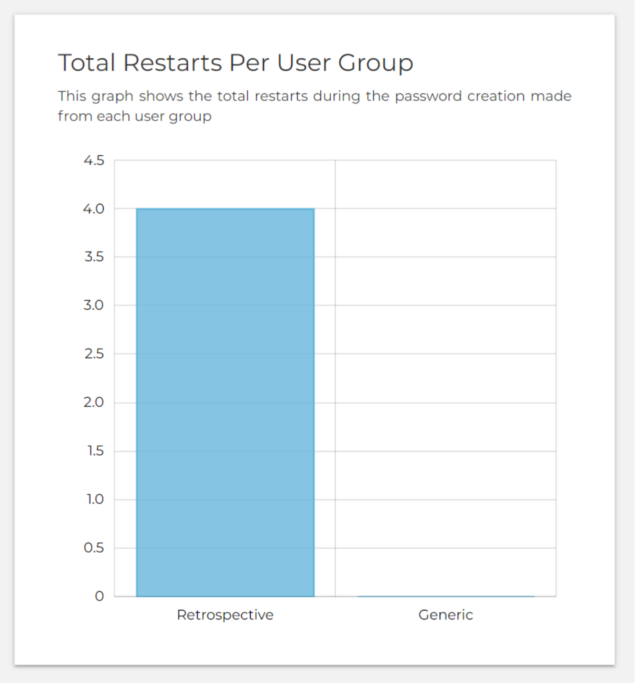


Figure 12. Total Restarts per User Group

Observations

Using this chart, we can come to the following assumption. The users with retrospective images chose to restart the password creation process either because they were unsatisfied with their selection or they made a different gesture from that they were trying to create. Either way this assumption is now backing the hypothesis we made earlier, which we also referenced in section *5.6.1.2 "Maximum/Minimum Time to Create Password"*, where we stated that the users with retrospective images will be more likely to create more complex passwords.

5.6.1.6 Maximum/Minimum Restarts During the Password Creation

From these charts () we can see the maximum times a user from each user group restarted their password creation process. A user with retrospective image is shown to have restarted the process three times whereas none of the users with a generic image attempted to restart and create from the start their password. The minimum times a user has restarted the process is zero for both groups.

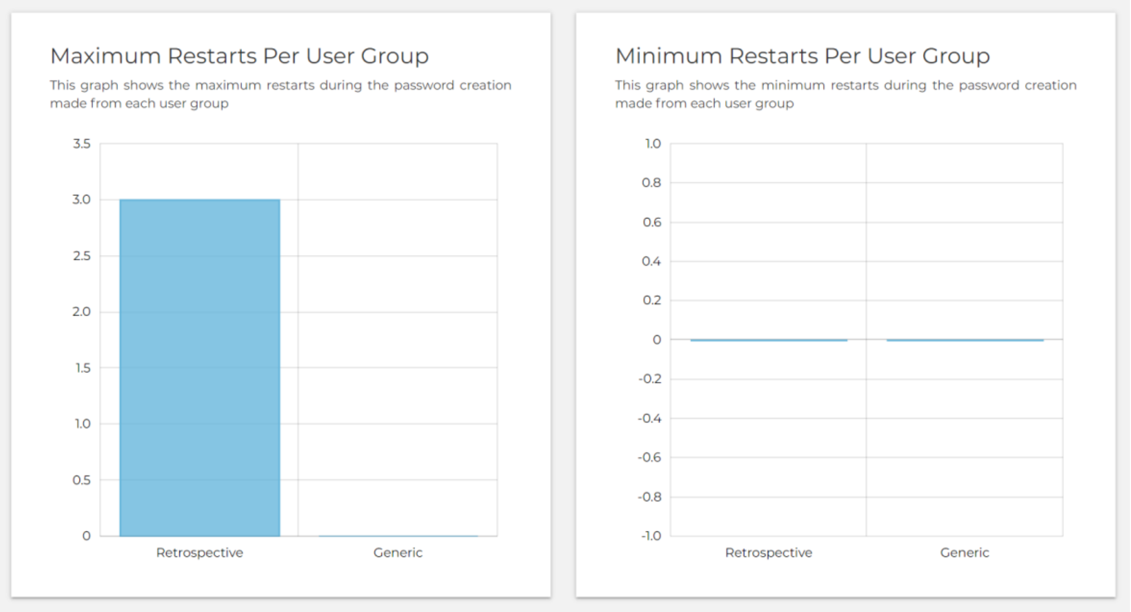


Figure 13. Maximum and Minimum times a user has restarted the creation process for each user group

Observations

The observations for the maximum number of restarts underlay those of the total restarts that we have commented on the previous section. The minimum number of restarts show that during the password creation there was at least one user for both user groups, which did not have the need to restart the password creation process.

5.6.1.7 Number of Times Each Gesture Was Selected

These two charts below (Figure 14) show how many times a type of gesture was used as the first, second and third gesture of the users' passwords during the creation of the password. We also took into consideration that some gestures are more complex than others e.g., the “CIRCLE” gesture is a bit more complex to perform and recreate than the “TAP” gesture. This is due to the fact that not only it is physically harder to perform repeatedly a circle using the mouse, but a circle can be of different size in contrast with a tap/click of a mouse.

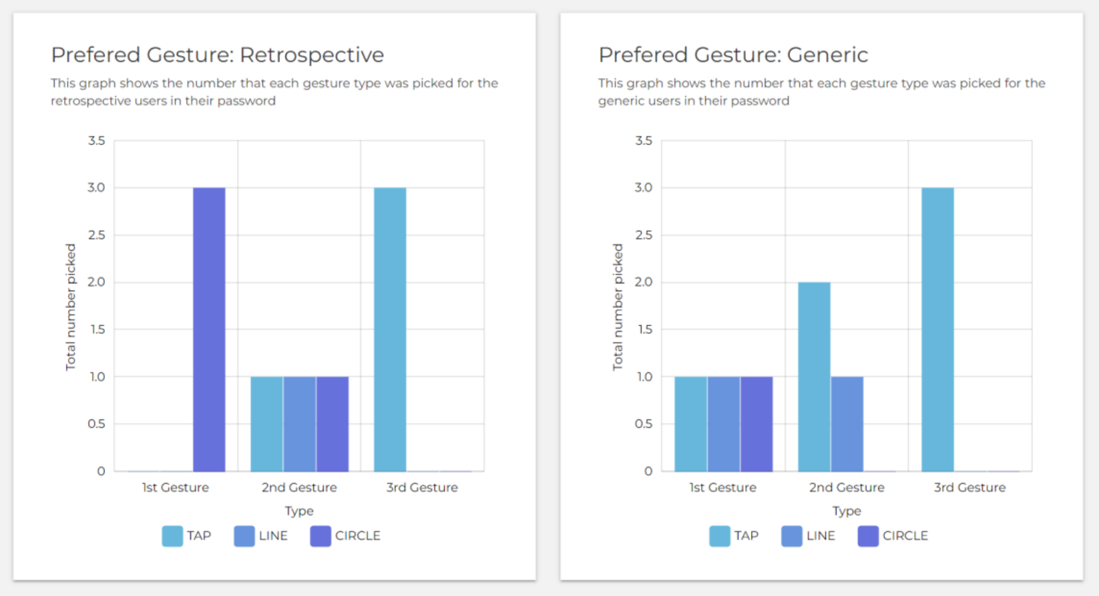


Figure 14. Number of Uses for each Gesture type from each user group

Observations

Knowing that there were three participants with each image group we can clearly see that every one of the users with retrospective images selected as their first gesture the "CIRCLE". As we stated above, the circle is a more complex gesture to perform, so we can make an assumption that all the "retrospective" users started with a high intention of creating a complex password, which also complies with one of our earlier hypotheses. In total, the circle gesture was chosen four times in all of the three passwords of the "retrospective" users, whereas for the "generic" users it was only selected once. A last observation that could be made is that users with generic images started off with totally different gesture types and slowly moved towards the same choice of the simpler ones. Other than that last minor observation, not much is left to be commented on, since there no other patterns to be noticed regarding the type of gestures selected.

5.6.2 Login Sessions

In order for the administrator/researcher to see the results during the login sessions of the users they will have to scroll to the next section of the "General Stats" page, named "Statistics regarding login attempts". In this section the administrator is presented with the following charts: the average login time of the users of each image group during the span of those five days, the maximum time that a user from each image group needed to login to their account, the corresponding minimum time a user needed to login during a single session, the total failed attempts to login during all of the sessions and the maximum and minimum failed attempts occurred in the duration of a single session.

5.6.2.1 Average Login Time for each User Group

The following chart (Figure 15) represents the average time that was required for every user of each group to successfully login to their accounts over the login sessions established in those five days. The average login time for the users with retrospective images was 9341 milliseconds whereas the average login time for the users with generic images was 6555 milliseconds.

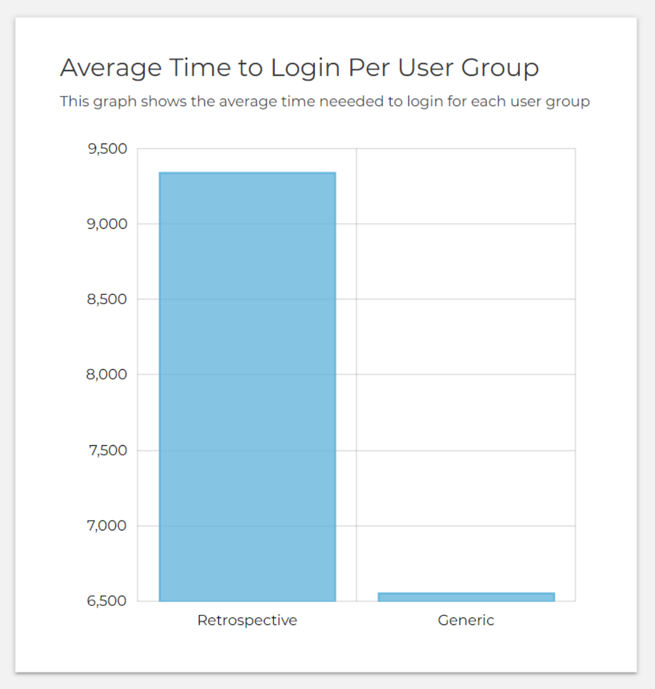


Figure 15. Average Login Time for each User Group

Observations

Initially, the data seem surprising because it would be expected for the users with retrospective images to be able to login faster. This result may be an outcome of a more complicated password. We will be discussing this in more detail in the following sections where we will also take a look at the failed attempts of the login sessions.

5.6.2.2 Maximum and Minimum Login Time for a Single Session

Using these two generated graphs we will gain a better understanding of the results shown above. The maximum login time for a "retrospective" user during a single login session was 44017 milliseconds and for a "generic" user was 11100 milliseconds. The minimum login time was 2094 milliseconds and 4212 milliseconds for the "retrospective" and "generic" users respectively.

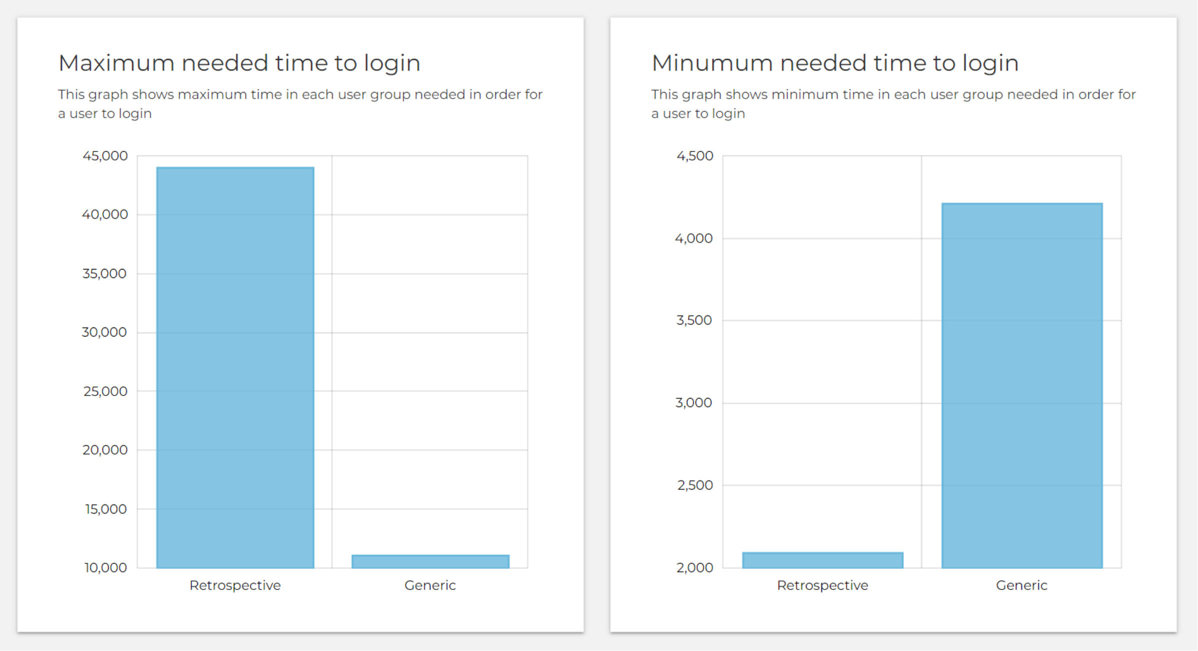


Figure 16. Maximum and Minimum Login Times of a Single Session

Observations

By taking a closer look at the graphs we can see the big difference of the maximum login times for the two user groups. On the other hand, by observing the data on the minimum login times we can see something very different. The minimum login time for a "retrospective" user is almost half the time of that of a "generic" user. That maximum login time is much higher even than the average login time, which was 9341 milliseconds. Taking that into consideration, we can assume that that maximum time was established by a minority of the "retrospective" users, possibly due to a failed attempt.

5.6.2.3 Total Failed Login Attempts of each User Group

In this section we will gain a better perceptive of the results we extracted on the previous sections. As the chart show () none of the generic users made a failed attempt to login to their accounts. The retrospective on the other hand made in total 5 failed attempts.

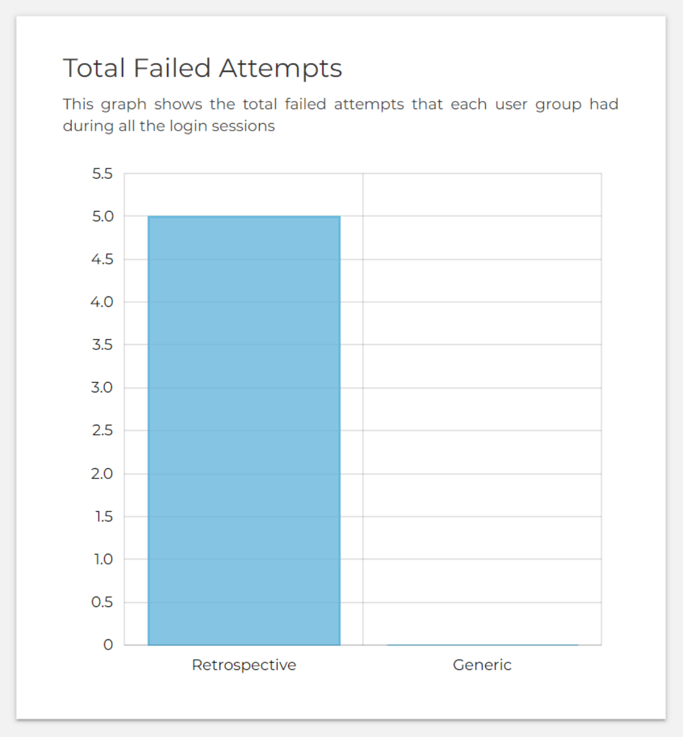


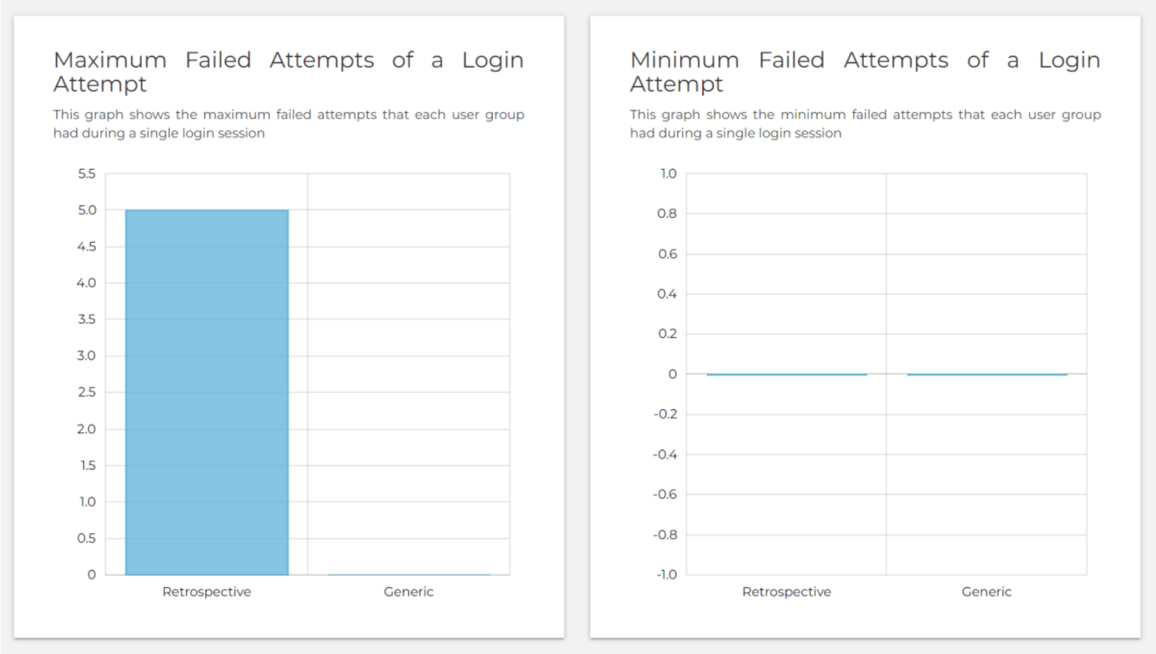
Figure 17. Total Failed Login Attempts for each User Group

Observations

There have been recorded five failed login attempts during the login sessions of the retrospective users. Based on the previously presented data, we can assume that this might be possibly due to a password of higher complexity. If this is correct then it complies also with the hypothesis that users with retrospective images tend to create more complex passwords.

5.6.2.4 Maximum and Minimum Failed Login Attempts

The following graph shows that the maximum times that a user failed to login during a single login session was five for the retrospective users and none for the generic users. The second graph shows that there was at least one user of each user group that succeeded to login during a session.



Maximum Failed Attempts of a Login Attempt

This graph shows the maximum failed attempts that each user group had during a single login session

Minimum Failed Attempts of a Login Attempt

This graph shows the minimum failed attempts that each user group had during a single login session

Figure 18. Maximum and Minimum Failed Login Attempts

Observations

We can now clearly see that all the failed attempts of the retrospective user group were done by a single user in a single session. By the data alone it is not quite clear whether this is due to solely a user or a system error. Although, we can make the safe assumption that whether it was a user or a system error, it could possibly have been caused due to a more complex password which resulted in a higher difficulty of recreation and verification.

6 Conclusion and Future Work

In this chapter we will conclude on the effectiveness of the administrator dashboard regarding its aid in the evaluation process of this use case of a user study and its representation of the results collected. In addition we will offer a summary of this thesis and finally we will point out different ways of future expansion of a system of this nature and further research.

6.1 Conclusion

In this thesis, after the research of the importance of graphical user authentication and specifically the evaluation of such systems, we aimed to implement an effective and efficient evaluation tool by providing the researcher the aid of automatic data collection and visualization. We tested the implemented system's performance by carrying out a use case of a study, in which we examined briefly the effects of a user's choices and goals regarding their authentication with use of the Picture Gesture Authentication system. More particularly, regarding the ways a retrospective image can influence the strength and complexity of an individual's password, in the scope of creating a more secure and usable way of authentication. In the beginning of our evaluations, we attempted to make our assumptions and hypothesis revolving this matter, as we would in a real-word user study. These hypotheses were that with the use of a retrospective image which consequently elicit stronger emotions due to past experiences that a user has with the scene represented within the image, would have made it easier for the user to create and remember its password, whilst being a strong and complex enough password.

With the results collected using the administrator dashboard that was developed, the evaluation study and specifically the collection of the data was fairly frictionless. Using this data, we managed to take a brief look into the effects of the users' prior experiences during the registration and authentication phases of a picture password system. More specifically, we succeeded to respond to our initial hypothesis, but more importantly we succeeded in minimizing the time required to collect the data and visualize them, since these processes were established automatically by the interactive dashboard.

Although the user data is far from sufficient in order to create a comprehensive look into this matter, they were sufficient enough in order to acknowledge the usefulness of this data visualization tool. With this dashboard we were able to immediately observe and develop a small sample of observations of our user study test, as we discussed in the previous chapter. In the case that a further inspection of the data was needed, we had the option to individually view and examine the statistics regarding a certain user, with the search feature of the dashboard.

6.2 Future Work

A future expansion of this system would be the implementation of a function that would process the EEG data provided, so that an approximation of emotional data would be extracted and presented along with the data collected regarding both the retrospective and generic users. In addition, in the dashboard there could be additional features implemented, like storing each group of login sessions, based on the date they were carried out, as an individual user study, so that the administrator could have several user studies saved in the database.

The field of Graphical User Authentication is becoming even more promising as the number of studies grow. Since we as humans are mostly visual learners, and are emotion driven beings, the exploration of the effects of human emotion in the area of authentication is naturally expected to be the next step into the development of cognitive intelligent technologies and tools.

References

[1] P. Saariluomaand and J. P. P. Jokinen, “Emotional Dimensions of User Experience: A User Psychological Analysis,” *Int. J. Hum. Comput. Interact.*, vol. 30, no. 4, pp. 303–320, 2014, doi: 10.1080/10447318.2013.858460.

[2] C. E. Izard, “Emotion theory and research: Highlights, unanswered questions, and emerging issues,” *Annu. Rev. Psychol.*, vol. 60, pp. 1–25, 2009, doi: 10.1146/annurev.psych.60.110707.163539.

[3] L. Kraus, J. N. Antons, F. Kaiser, and S. Möller, “User Experience in Authentication Research: A Survey,” no. May, pp. 34–38, 2016, doi: 10.21437/pqs.2016-12.

[4] J. Yan, B. Alan, R. Anderson, and A. Grant, “Password memorability and security: Empirical results,” *IEEE Secur. Priv.*, vol. 2, no. 5, pp. 25–31, 2004, doi: 10.1109/MSP.2004.81.

[5] K. Dharavath, F. A. Talukdar, and R. H. Laskar, “Study on biometric authentication systems, challenges and future trends: A review,” *2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013*, 2013, doi: 10.1109/ICCIC.2013.6724278.

[6] T. Hewett *et al.*, *ACM SIGCHI Curricula for Human-Computer Interaction*. 1992.

[7] B. D. Payne and W. K. Edwards, “A brief introduction to usable Security,” *IEEE Internet Comput.*, vol. 12, no. 3, pp. 13–20, 2008, doi: 10.1109/MIC.2008.50.

[8] M. Zviran and W. J. Haga, “Cognitive passwords: The key to easy access control,” *Comput. Secur.*, vol. 9, no. 8, pp. 723–736, 1990, doi: 10.1016/0167-4048(90)90115-A.

[9] R. Riding and I. Cheema, “Educational Psychology : An International Journal of Experimental Cognitive Styles — an overview and integration,” *Educ. Psychol. An Int. J. Exp. Educ. Psychol.*, vol. 11, no. 3–4, pp. 37–41, 1991.

[10] J. J. Koob and J. Funk, “Kolb’s learning style inventory: Issues of reliability and validity,” *Res. Soc. Work Pract.*, vol. 12, no. 2, pp. 293–308, 2002, doi: 10.1177/104973150201200206.

[11] S. Xiaoyuan, Z. Ying, and G. S. Owen, “Graphical passwords: A survey,” *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, vol. 2005, no. May, pp. 463–472,

2005, doi: 10.1109/CSAC.2005.27.

[12] A. H. Lashkari, A. Abdul Manaf, M. Masrom, and S. M. Daud, “Security evaluation for graphical password,” *Commun. Comput. Inf. Sci.*, vol. 166 CCIS, no. PART 1, pp. 431–444, 2011, doi: 10.1007/978-3-642-21984-9_37.

[13] A. Shah, P. Ved, A. Deora, A. Jaiswal, and M. D’Silva, “Shoulder-surfing resistant graphical password system,” *Procedia Comput. Sci.*, vol. 45, no. C, pp. 477–484, 2015, doi: 10.1016/j.procs.2015.03.084.

[14] T. Issa and P. Isaias, “Sustainable design: Hci, usability and environmental concerns,” *Sustain. Des. Hci, Usability Environ. Concerns*, pp. i–iii, 2015, doi: 10.1007/978-1-4471-6753-2.

[15] “ISO (International Organization for Standardization),” 1997. https://www.iso.org (accessed Dec. 28, 2020).

[16] A. M. Eljetlawi and N. Ithnin, “Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods,” *Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008*, vol. 2, pp. 1137–1143, 2008, doi: 10.1109/ICCIT.2008.20.

[17] T. Khodadadi, A. K. M. M. Islam, S. Baharun, and S. Komaki, “Evaluation of recognition-based graphical password schemes in terms of usability and security attributes,” *Int. J. Electr. Comput. Eng.*, vol. 6, no. 6, pp. 2939–2948, 2016, doi: 10.11591/ijece.v6i6.11227.

[18] A. Constantinides, A. M. Pietron, M. Belk, C. Fidas, T. Han, and A. Pitsillides, “A Cross-cultural Perspective for Personalizing Picture Passwords,” *UMAP 2020 - Proc. 28th ACM Conf. User Model. Adapt. Pers.*, pp. 43–52, 2020, doi: 10.1145/3340631.3394859.

[19] A. Constantinides, C. Fidas, M. Belk, and A. Pitsillides, “‘I recall this picture’: Understanding Picture Password Selections based on Users’ Sociocultural Experiences,” *Proc. - 2019 IEEE/WIC/ACM Int. Conf. Web Intell. WI 2019*, pp. 408–412, 2019, doi: 10.1145/3350546.3352557.

[20] A. Constantinides, M. Belk, C. Fidas, and A. Pitsillides, “An eye gaze-driven metric for estimating the strength of graphical passwords based on image hotspots,” *Int. Conf. Intell. User Interfaces, Proc. IUI*, pp. 33–37, 2020, doi: 10.1145/3377325.3377537.

[21] A. Constantinides, M. Belk, C. Fidas, and G. Samaras, “On cultural-centered

graphical passwords: Leveraging on users' cultural experiences for improving password memorability," *UMAP 2018 - Proc. 26th Conf. User Model. Adapt. Pers.*, pp. 245–249, 2018, doi: 10.1145/3209219.3209254.

[22] A. Constantinides, M. Belk, C. Fidas, and A. Pitsillides, "On the accuracy of eye gaze-driven classifiers for predicting image content familiarity in graphical passwords," *ACM UMAP 2019 - Proc. 27th ACM Conf. User Model. Adapt. Pers.*, pp. 201–205, 2019, doi: 10.1145/3320435.3320474.

[23] "MindBigData the MNIST of Brain Digits." http://www.mindbigdata.com/opendb/imagenet.html (accessed Jan. 04, 2021).

[24] "Python.org." https://www.python.org/ (accessed Dec. 31, 2020).

[25] "The Web framework for perfectionists with deadlines | Django." https://www.djangoproject.com/ (accessed Dec. 31, 2020).

[26] "PyPI · The Python Package Index." https://pypi.org/ (accessed Dec. 31, 2020).

[27] "PostgreSQL: The world's most advanced open source database." https://www.postgresql.org/ (accessed Dec. 31, 2020).

[28] "Dockerize PostgreSQL | Docker Documentation." https://docs.docker.com/engine/examples/postgresql_service/ (accessed Dec. 31, 2020).

[29] "JavaScript Charts & Maps - amCharts." https://www.amcharts.com/ (accessed Jan. 15, 2021).

[30] "uuid — UUID objects according to RFC 4122 — Python 3.9.1 documentation." https://docs.python.org/3/library/uuid.html (accessed Dec. 31, 2020).

[31] "RFC 4122 - A Universally Unique IDentifier (UUID) URN Namespace." https://tools.ietf.org/html/rfc4122.html (accessed Dec. 31, 2020).