**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | **IV** |
|  | **LIST OF FIGURES** | **XI** |
|  | **LIST OF TABLES** | **XII** |
|  | **LIST OF ABBREVIATIONS** | **XIII** |
| **1** | **INTRODUCTION** | 1 |
|  | * 1. THE NEED FOR SECURITY AND AUTHENTICATION SYSTEMS | 2 |
|  | * 1. CIA TRIAD IN SECURITY SYSTEMS | 4 |
|  | * 1. ATTACKS ON SECURITY SYSTEMS | 6 |
|  | * 1. VISUAL HACKING ATTACKS | 7 |
|  | * 1. TYPES OF VISUAL HACKING ATTACKS | 9 |
|  | * 1. SHOULDER SURFING ATTACK | 11 |
|  | * 1. AUTHENTICATION SYSTEM | 13 |
|  | * 1. HISTORY OF AUTHENTICATION SYSTEM | 15 |
|  | * 1. DISADVANTAGES OF TRADITIONAL AUTHENTICATION SYSTEMS | 16 |
|  | * 1. METHODS TO OVERCOME DISADVANTAGES OF AUTHENTICATION SYSTEMS | 18 |
|  | * 1. GRAPHICAL AUTHENTICATION SYSTEM | 20 |
|  | * 1. RISE OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEM | 21 |
|  | * 1. ADVANTAGES OF GRAPHICAL AUTHENTICATION SYSTEM OVER TRADITIONAL SYSTEMS | 22 |
|  | * 1. KEY FEATURES OF GRAPHICAL AUTHENTICATION SYSTEM | 24 |
|  | * 1. TYPES OF ATTACKS THAT CAN BE PREVENTED BY GRAPHICAL AUTHENTICATION SYSTEM | 25 |
|  | * 1. LEADING INDUSTRIES USING GPA | 27 |
|  | * 1. OBJECTIVES | 28 |
|  | * 1. SCOPE | 29 |
|  |  |  |
| **2** | **LITERATURE SURVEY** | 30 |
|  | * 1. REFERENCES | 30 |
|  | * + 1. SHAH, M., NAIK, R., MULLAKODI, S., & CHAUDHARI, S. (2018). COMPARATIVE ANALYSIS OF DIFFERENT GRAPHICAL PASSWORD TECHNIQUES FOR SECURITY. INT RES J ENG TECHNOL (IRJET), 5(4), 1873-1877 | 30 |
|  | * + 1. T. KWON, S. SHIN, AND S. NA, “COVERT ATTENTIONAL SHOULDER SURFING: HUMAN ADVERSARIES ARE MORE POWERFUL THAN EXPECTED,” | 33 |
|  | * + 1. M. MARTINEZ-DIAZ, J. FIERREZ, AND J. GALBALLY, “GRAPHICAL PASSWORD-BASED USER AUTHENTICATION WITH FREE-FORM DOODLES,” IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. PP, NO. 99, PP. 1–8, 2015 | 35 |
|  | * + 1. E. VON ZEZSCHWITZ, A. DE LUCA, AND H. HUSSMANN, “HONEY, I SHRUNK THE KEYS: INFLUENCES OF MOBILE DEVICES ON PASSWORD COMPOSITION AND AUTHENTICATION PERFORMANCE,” IN PROCEEDINGS OF THE 8TH NORDIC CONFERENCE ON HUMAN-COMPUTER INTERACTION: FUN, FAST, FOUNDATIONAL, SER. NORDICHI ’14. NEW YORK, NY, USA: ACM, 2014, PP. 461–470 | 37 |
|  | * + 1. M. MARTINEZ-DIAZ, J. FIERREZ, AND J. GALBALLY, “THE DOODB GRAPHICAL PASSWORD DATABASE: DATA ANALYSIS AND BENCHMARK RESULTS,” ACCESS, IEEE, VOL. 1, PP. 596–605, 2013 | 39 |
|  | * + 1. IRANNA, A. M., AND PANKAJA PATIL. "GRAPHICAL PASSWORD AUTHENTICATION USING PERSUASIVE CUED CLICK POINT." INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ELECTRICAL, ELECTRONICS AND INSTRUMENTATION ENGINEERING 2, NO. 7 (2013): 513-517 | 41 |
|  | * + 1. S. WIEDENBECK, J. WATERS, J. BIRGET, A. BRODSKIY, AND N. MEMON, “PASSPOINTS: DESIGN AND LONGITUDINAL EVALUATION OF A GRAPHICAL PASSWORD SYSTEM,” | 44 |
|  | * + 1. OAKLEY AND A. BIANCHI, “MULTI-TOUCH PASSWORDS FOR MOBILE DEVICE ACCESS,” IN PROCEEDINGS OF THE 2012 ACM CONFERENCE ON UBIQUITOUS COMPUTING, SER. UBICOMP ’12. NEW YORK, NY, USA: ACM, 2012, PP. 611–612. | 46 |
|  | * + 1. AVIV, K. GIBSON, E. MOSSOP, M. BLAZE, AND J. SMITH, “SMUDGE ATTACKS ON SMARTPHONE TOUCH SCREENS,” IN USENIX 4TH WORKSHOP ON OFFENSIVE TECHNOLOGIES, 2010 | 48 |
|  | * + 1. H. ZHAO AND X. LI, “S3PAS: A SCALABLE SHOULDER-SURFING RESISTANT TEXTUAL-GRAPHICAL PASSWORD AUTHENTICATION SCHEME” | 50 |
|  | * + 1. WIEDENBECK, SUSAN, JIM WATERS, JEAN-CAMILLE BIRGET, ALEX BRODSKIY, AND NASIR MEMON. "AUTHENTICATION USING GRAPHICAL PASSWORDS: EFFECTS OF TOLERANCE AND IMAGE CHOICE." IN PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, PP. 1-12. 2005 | 52 |
|  | * + 1. SUO, XIAOYUAN, YING ZHU, AND G. SCOTT OWEN. "GRAPHICAL PASSWORDS: A SURVEY." IN 21ST ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC'05), PP. 10-PP. IEEE, 2005. | 56 |
|  | * 1. EXISTING SYSTEMS | 60 |
|  | * + 1. HYBRID COLOR SHUFFLING | 60 |
|  | * + 1. HUEBOX SCHEME | 62 |
|  | * + 1. COLOR-CODE COMBINATION SYSTEM | 65 |
|  | * + 1. OTHER EXISTING SYSTEMS | 68 |
|  |  |  |
| **3** | **REQUIREMENT ANALYSIS** | 71 |
|  | 1. 1. STAKEHOLDERS | 71 |
|  | * 1. REQUIREMENT GATHERING | 72 |
|  | * 1. REQUIREMENT ANALYSIS | 74 |
|  | * + 1. HARDWARE REQUIREMENTS | 74 |
|  | * + 1. SOFTWARE REQUIREMENTS | 75 |
|  | * 1. PROBLEM STATEMENT | 75 |
|  |  |  |
| **4** | **DESIGN** | 76 |
|  | * 1. PROPOSED SYSTEM | 76 |
|  | * 1. SYSTEM ARCHITECTURE | 77 |
|  | * 1. MODULES | 79 |
|  | * + 1. PASSWORD VERIFICATION MODULE | 80 |
|  | * + 1. COLOR MATCHER MODULE | 83 |
|  | * + 1. PATTERN MATCHER MODULE | 86 |
|  | * 1. SOFTWARE ENVIRONMENT | 89 |
|  | * + 1. JAVA | 89 |
|  | * + 1. INTEGRATED DEVELOPMENT ENVIRONMENT | 90 |
|  | * + 1. APACHE TOMCAT | 91 |
|  | * + 1. MYSQL | 93 |
|  |  |  |
| **5** | **IMPLEMENTATION** | 95 |
|  | * 1. PASSWORD VERIFICATION MODULE | 95 |
|  | * + 1. REGISTRATION SUB MODULE | 95 |
|  | * + 1. LOGIN SUB MODULE | 97 |
|  | * 1. COLOR MATCHER MODULE | 99 |
|  | * + 1. REGISTRATION SUB MODULE | 99 |
|  | * + 1. LOGIN SUB MODULE | 100 |
|  | * 1. PATTERN MATCHER MODULE | 102 |
|  | * + 1. REGISTRATION SUB MODULE | 102 |
|  | * + 1. LOGIN SUB MODULE | 103 |
|  |  |  |
| **6** | **TESTING** | 105 |
|  | * 1. UNIT TESTING | 105 |
|  | * + 1. REGISTRATION UNITS | 106 |
|  | * + 1. LOGIN UNITS | 107 |
|  | * 1. INTEGRATION TESTING | 108 |
|  |  |  |
| **7** | **CONCLUSION AND FUTURE SCOPE** | **110** |
|  | **APPENDIX – 1 (INDUSTRY APPROVAL & COMPLETION)** | **112** |
|  | **APPENDIX – 2 (SCREENSHOTS)** | **115** |
|  | **APPENDIX – 3 (PUBLICATION)** | **120** |
|  | **REFERENCES** | **137** |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **FIGURE NAME** | **PAGE NO.** |
| 1.1 | AUTHENTICATION PROCESS | 2 |
| 1.2 | CIA TRIAD | 5 |
| 1.3 | ATTACK ON SECURE SYSTEMS | 7 |
| 1.4 | TYPES OF VISUAL HACKING | 11 |
| 1.5 | SHOULDER SURFING ATTACK | 12 |
| 1.6 | VARIOUS METHODS FOR AUTHENTICATION SYSTEMS | 19 |
| 1.7 | ATTACKS PREVENTABLE USING GPA | 26 |
| 4.1 | SYSTEM ARCHITECTURE | 77 |
| 4.2 | OVERALL MODULE DIAGRAM | 79 |
| 4.3 | PASSWORD VERIFICATION MODULE | 82 |
| 4.4 | COLOR MATCHER MODULE | 85 |
| 4.5 | PATTERN VERIFICATION MODULE | 88 |
| 1 | USER REGISTRATION PAGE | 116 |
| 2 | COLOR REGISTRATION MODULE | 116 |
| 3 | PATTERN REGISTRATION MODULE | 117 |
| 4 | PASSWORD LOGIN | 117 |
| 5 | COLOR VERIFICATION | 118 |
| 6 | PATTERN VERIFICATION | 118 |
| 7 | LOGIN SUCCESSFUL | 119 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **TABLE NO** | **TABLE NAME** | **PAGE NO.** |
| 2.1 | LITERATURE SURVEY – ANALYSIS | 60 |
| 2.2 | EXISTING SYSTEMS – ANALYSIS | 70 |
| 4.1 | HARDWARE REQUIREMENTS | 74 |
| 4.2 | SOFTWARE REQUIREMENTS | 75 |
| 6.1 | TEST CASE DETAILS FOR REGISTRATION UNITS | 106 |
| 6.2 | TEST CASE DETAILS FOR LOGIN UNITS | 107 |
| 6.3 | TEST CASE DETAILS FOR INTEGRATION TESTING | 109 |

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **ABBREVIATION** | **EXPANSION** |
| GPA | GRAPHICAL PASSWORD AUTHENTICATION |
| SSA | SHOULDER SURFING ATTACKS |
| CIA | CONFIDENTIALITY, INTEGRITY, AVAILABILITY |
| DoS | DENIAL OF SERVICE |
| RGB | RED, GREEN, BLUE |
| DDoS | DISTRIBUTED DENIAL OF SERVICE |
| MITM | MAN IN THE MIDDLE |
| SQL | STRUCTURED QUERY LANGUAGE |
| 2FA | 2 FACTOR AUTHENTICATION |
| CAPTCHA | COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTERS AND HUMANS APART |
| DAS | DRAW-A-SECRET |
| JDK | JAVA DEVELOPMENT KIT |
| JSP | JAVA SERVLET PAGES |
| HTTP | HYPER TEXT TRANSFER PROTOCOL |
| IDE | INTEGRATED DEVELOPMENT ENVIRONMENT |
| JVM | JAVA VIRTUAL MACHINE |
| GUI | GRAPHICAL USER INTERFACE |
| EER | EQUAL ERROR RATE |
| S3PAS | SCALABLE SHOULDER-SURFING RESISTANT TEXTUAL - GRAPHICAL PASSWORD AUTHENTICATION SCHEME |
| VPA | VISUAL PASSWORD AUTHENTICATION |
| SSO | SINGLE SIGN ON |
| MFA | MULTI FACTOR AUTHENTICATION |
| RBA | RISK BASED ASSESSMENT |

**CHAPTER 1**

# INTRODUCTION

Textual passwords have been the standard method for authentication for decades. These passwords usually require a combination of numerals, upper and lower-case letters to fortify resistance against brute force attacks. However, the degree of complexity required to render these passwords truly secure renders them notably arduous to memorize and recall. As a result, users tend to opt for passwords that are either too short or easily derived from the dictionary, rather than employing a random alphanumeric sequence. This is further exacerbated by the fact that individuals frequently reuse login credentials across multiple accounts, creating a security risk that has been evidenced by numerous security teams.

A study conducted by Computer World revealed that nearly 80% of a company's employees' passwords could be cracked in under 30 seconds by means of a network password cracker. In response to the shortcomings of textual passwords, graphical password authentication methods have emerged as a promising alternative. These methods have been designed to overcome the limitations and vulnerabilities of textual passwords. Graphical password authentication methods rely on research indicating that humans are better at memorizing images rather than verbal representations, offering a more intuitive and user-friendly approach to authentication. Image-based passwords have demonstrated an improved ability to be recollected over longer periods of time, even without frequent activation, and can be made complex and secure. However, these methods are also subject to Visual Hacking (SSAs), whereby passwords, PINs, and other sensitive personal information are obtained through direct observation or video capturing techniques.

Considering these issues, it is important to consider the potential security risks associated with all authentication methods, and to develop innovative solutions that prioritize both security and usability. Graphical password authentication methods represent a promising development in this regard, offering enhanced security features while maintaining a high degree of usability. Nevertheless, there is still room for improvement and refinement, and it is important for researchers and developers to continue exploring new approaches to authentication that can effectively address the ongoing challenges and threats to digital security.

## THE NEED FOR SECURITY AND AUTHENTICATION SYSTEMS

The need for security is a fundamental aspect of modern society. As technology continues to advance, so does the importance of protecting sensitive information. Authentication systems play a crucial role in this process by providing a means of verifying the identity of an individual who is attempting to access a particular system or resource.

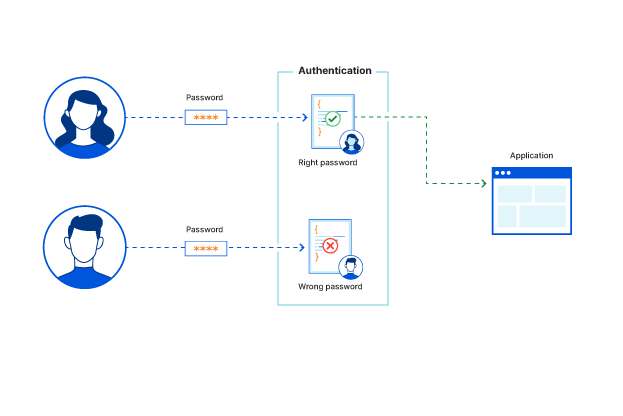


Fig 1.1: Authentication Process

Authentication systems are essential for ensuring that only authorized users are granted access to sensitive information or resources. Without proper authentication mechanisms in place, anyone could potentially gain access to confidential data, putting individuals and organizations at risk of theft, fraud, or other types of malicious activity.

One of the main reasons for the need for authentication systems is the growing trend towards digitalization of information. As more and more sensitive data is stored in digital format, the risks associated with unauthorized access or data breaches increase. Authentication systems provide a way of controlling who has access to this data, ensuring that only authorized individuals can view, modify, or delete it.

Moreover, authentication systems are essential for protecting online transactions and financial data. When individuals make purchases online, they need to be assured that their financial information is secure and that they are not at risk of identity theft or other forms of fraud. Authentication systems help to provide this assurance by ensuring that only authorized users have access to financial data and transaction systems.

Authentication systems are also necessary for compliance with regulations and industry standards. Many industries are subject to strict regulatory requirements regarding the protection of sensitive information. Authentication systems can help organizations comply with these regulations by providing a means of controlling access to sensitive data and ensuring that only authorized individuals are granted access. The need for security and authentication systems is critical in today's digital world. As technology continues to evolve, the risks associated with unauthorized access and data breaches will only increase. Authentication systems provide a necessary layer of protection by ensuring that only authorized users have access to sensitive information and resources.

## CIA TRIAD IN SECURITY SYSTEMS

The CIA triad, also known as the information security triad, is a model designed to guide organizations in implementing and maintaining a robust and effective information security program. The CIA triad stands for Confidentiality, Integrity, and Availability, which are three essential pillars of information security. These three components are the foundation of any security framework, and they work together to provide a comprehensive approach to securing data and information systems.

Confidentiality refers to the protection of sensitive or confidential information from unauthorized access. This includes data such as personal information, financial information, and intellectual property. Confidentiality ensures that only authorized individuals can access sensitive information, and unauthorized individuals are prevented from accessing or viewing it. The need for confidentiality arises from the increasing number of cyberattacks, data breaches, and the value of sensitive information. Confidentiality is achieved through measures such as access controls, encryption, and data classification.

Integrity refers to maintaining the accuracy and consistency of data and information systems. Data integrity ensures that data remains complete, accurate, and reliable throughout its lifecycle. Integrity ensures that data is not tampered with or modified in any unauthorized manner. The need for integrity arises from the increasing number of malicious attacks aimed at altering data for fraudulent purposes. Integrity is achieved through measures such as data validation, error checking, and data backups.

Availability refers to the ability of authorized users to access the information they need when they need it. This includes the availability of hardware, software, and data. Availability ensures that authorized users can access systems and data when needed and that systems and data are not affected by disruptions, outages, or other factors that may cause unavailability. The need for availability arises from the increasing reliance on technology for business operations and the potential impacts of system outages on operations. Availability is achieved through measures such as redundancy, fault tolerance, and disaster recovery planning.

The CIA triad is a crucial concept in information security, and it is often used as a framework for developing security policies, procedures, and practices. The CIA triad provides a holistic approach to information security, covering all aspects of information security, including data protection, access control, risk management, and disaster recovery. The CIA triad ensures that information security measures are aligned with business goals and objectives, and that they are effective in protecting critical information assets.

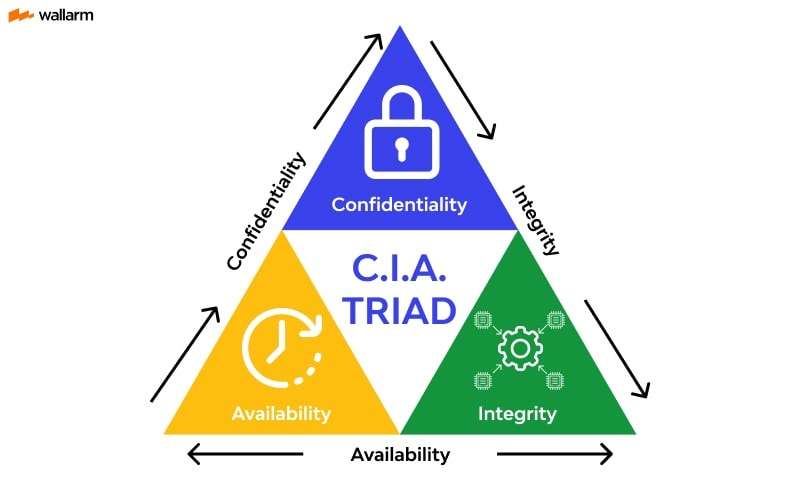


Fig 1.2: CIA Triad

## ATTACKS ON SECURITY SYSTEMS

In the context of cybersecurity, an attack refers to any deliberate or unauthorized attempt to breach the security of a computer system, network, or device. The goal of an attack may vary, from stealing sensitive information, gaining unauthorized access, causing damage to the system or network, or disrupting normal operations. Attacks can take different forms, and they can be launched by a wide range of actors, including cybercriminals, hacktivists, state-sponsored actors, insiders, or even unintentionally by legitimate users.

There are several types of attacks that can be launched against a computer system or network. Here are some common examples:

* **Malware attacks:** Malware is a type of software designed to infiltrate or damage a computer system or network. Malware attacks can take various forms, such as viruses, Trojans, ransomware, spyware, or adware. Malware attacks often involve tricking users into installing or executing malicious software that can steal data, encrypt files, or take control of the system.
* **Phishing attacks:** Phishing is a social engineering attack that involves tricking users into revealing sensitive information, such as passwords, credit card numbers, or social security numbers. Phishing attacks often use emails, phone calls, or fake websites to lure victims into providing their information.
* **Denial-of-service (DoS) attacks:** DoS attacks involve overwhelming a system or network with traffic, making it unavailable to legitimate users. DoS attacks can be launched using various techniques, such as flooding the network with traffic, exploiting vulnerabilities in the system, or using botnets.
* **Man-in-the-middle (MitM) attacks:** MitM attacks involve intercepting the communication between two parties and eavesdropping or manipulating the data exchanged. MitM attacks can be launched by exploiting vulnerabilities in the network, such as unsecured Wi-Fi networks, or by using phishing techniques.
* **Password attacks:** Password attacks involve attempting to guess or steal passwords to gain unauthorized access to a system or network. Password attacks can take various forms, such as brute-force attacks, dictionary attacks, or password phishing.
* **SQL injection attacks:** SQL injection attacks involve exploiting vulnerabilities in web applications that use SQL databases. SQL injection attacks can allow attackers to steal data or manipulate the database by injecting malicious SQL commands into the input fields of the web application.
* **Zero-day attacks:** Zero-day attacks refer to attacks that exploit vulnerabilities in software or hardware that are not yet known to the public or the vendor. Zero-day attacks can be particularly dangerous as they can allow attackers to take control of a system or network without being detected.

Fig 1.3: Attacks on Secure Systems

## VISUAL HACKING ATTACKS

Visual hacking refers to the practice of acquiring sensitive, confidential, or private information by exploiting visual aids such as computer screens, paper documents, or even conversations. It is a type of hacking that does not rely on technical means but rather on human error, negligence, or carelessness.

Visual hacking can take many forms, such as shoulder surfing, tailgating, or dumpster diving. Shoulder surfing is the act of looking over someone's shoulder while they are typing their password or viewing confidential information on their computer screen. Tailgating involves following an authorized person into a restricted area without permission, while dumpster diving entails rummaging through garbage or recycling bins for sensitive documents.

Visual hacking is a significant threat to both individuals and organizations as it can result in the theft of sensitive data, financial loss, reputational damage, and legal consequences. In addition, visual hacking is often difficult to detect and prevent as it involves exploiting human vulnerabilities rather than technical flaws in systems or software.

One common form of visual hacking is through the use of cameras or other recording devices. For example, an attacker may use a hidden camera to capture a victim's login credentials or personal information as they enter it on their computer screen. Alternatively, an attacker may use a smartphone to surreptitiously record conversations or capture images of sensitive documents.

Another form of visual hacking is through social engineering ics such as phishing scams, pretexting, or baiting. In these scenarios, an attacker may eat a trusted source, such as a co-worker, IT support, or vendor, in order to gain access to information or convince a victim to take a particular action that puts them at risk.

To prevent visual hacking attacks, individuals and organizations should implement a range of physical and technical security measures. For instance, they should ensure that confidential documents are stored securely and shredded when no longer needed. They should also limit access to restricted areas and use security cameras to monitor activity. Additionally, they should implement data encryption, two-factor authentication, and other technical security measures to protect against unauthorized access to systems and data.

Moreover, education and awareness programs can also help to mitigate the risk of visual hacking. Training employees to recognize and respond to visual hacking attempts, such as detecting suspicious behavior, verifying the identity of visitors, and reporting any security incidents, can go a long way in preventing successful attacks.

## TYPES OF VISUAL HACKING ATTACKS

Visual hacking attacks are a form of cyberattack that relies on visual means to steal sensitive information from an individual or an organization. These attacks are carried out through direct observation, video capturing, or other visual techniques to obtain confidential information. Visual hacking can be classified into different types based on the methods used to gain unauthorized access to sensitive information. Some common types of visual hacking attacks include:

* **Shoulder Surfing Attack:** Shoulder surfing is a type of visual hacking attack in which an attacker tries to steal sensitive information by observing the user's actions, such as entering a password, PIN, or other confidential data on a device. The attacker typically stands close to the victim, either behind them or beside them, and observes their actions while pretending to engage in some other activity.
* **Screen Capture Attack:** A screen capture attack involves taking a screenshot or a photograph of the victim's device screen without their knowledge or consent. The attacker can then use this information to steal sensitive information such as usernames, passwords, credit card numbers, or other personal data.
* **Dumpster Diving Attack:** Dumpster diving is a type of visual hacking attack that involves searching through the victim's discarded documents, such as bills, invoices, or other documents containing sensitive information. The attacker can use this information to steal personal data, commit identity theft, or carry out other fraudulent activities.
* **Eavesdropping Attack:** An eavesdropping attack is a type of visual hacking attack that involves listening in on a private conversation or overhearing a sensitive discussion in a public place. The attacker can then use the information obtained to carry out fraudulent activities or gain unauthorized access to sensitive data.
* **Social Engineering Attack:** A social engineering attack involves tricking the victim into revealing sensitive information by pretending to be someone they trust, such as a friend, colleague, or service provider. The attacker can use various techniques, such as phishing emails, pretexting, or baiting, to gain the victim's trust and obtain confidential information.
* **Video Camera Attack:** A video camera attack involves using a hidden camera or a smartphone camera to record the victim's activities without their knowledge or consent. The attacker can then use this information to steal sensitive information such as passwords, credit card numbers, or other personal data.
* **Tailgating Attack:** A tailgating attack involves gaining unauthorized access to a restricted area by following an authorized user without their knowledge or consent. The attacker can then gain access to sensitive information, steal valuable assets, or commit other fraudulent activities.

Fig 1.4: Types of Visual Hacking

## SHOULDER SURFING ATTACK

Shoulder surfing is a type of social engineering attack in which an attacker observes or records the actions of an individual in order to obtain sensitive information such as passwords, PINs, or other sensitive information. This technique has been used for many years by criminals to gain unauthorized access to systems or facilities. Shoulder surfing can be executed either directly, by physically looking over someone's shoulder, or indirectly, by using optical tools or cameras to record the victim's actions from a distance.

In the context of information security, shoulder surfing is often used to obtain user credentials or other sensitive information that is used in authentication systems. This type of attack can be particularly effective against traditional textual passwords, as attackers can often deduce passwords from the pattern of keystrokes observed. With the increasing prevalence of mobile and web-based applications, the risk of shoulder surfing attacks has increased significantly, as users are frequently accessing sensitive information from public spaces or in the presence of others.

To counteract shoulder surfing attacks, several security measures have been proposed and implemented. One such measure is the use of graphical passwords, which employ images or patterns in place of traditional textual passwords. These passwords are typically more difficult to observe and remember than traditional textual passwords, making them less vulnerable to shoulder surfing attacks. Additionally, many authentication systems now incorporate two-factor authentication, requiring a secondary form of authentication in addition to a password, such as a fingerprint scan or one-time code.

Another effective defense against shoulder surfing attacks is the use of privacy screens or filters, which limit the visibility of a user's screen to those directly in front of it. These filters work by polarizing the light emitted from the screen, such that it can only be viewed from a specific angle. This makes it difficult for anyone attempting to observe the screen from another angle, such as an attacker in a public space, to see the information displayed.

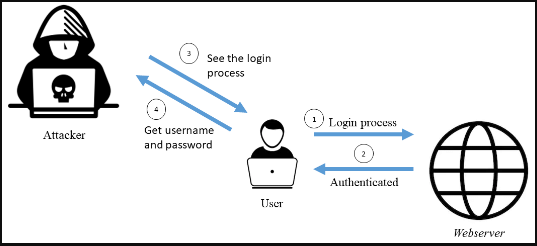


Fig 1.5: Shoulder Surfing Attack

Educating users on the risks and techniques of shoulder surfing attacks is also an important aspect of preventing these types of attacks. Users should be encouraged to shield their devices or screens when entering passwords or other sensitive information in public spaces, and to be aware of their surroundings when accessing sensitive information. Additionally, users should be made aware of the importance of using strong and unique passwords, as well as the risks of reusing passwords across multiple accounts.

## AUTHENTICATION SYSTEM

Authentication systems are mechanisms designed to verify the identity of a user or system, ensuring that only authorized parties are granted access to protected resources or information. These systems are a crucial component of computer security, playing a vital role in protecting against data breaches, fraud, and other cyber threats.

The most common method of authentication is the use of a username and password. When a user enters their login credentials, the system checks these against a stored database of usernames and passwords to determine whether access should be granted. However, this method has several limitations, including the risk of password theft, the likelihood of users selecting weak passwords, and the possibility of social engineering attacks.

To address these issues, various other authentication methods have emerged. One popular approach is two-factor authentication (2FA), which requires users to provide two forms of identification, typically a password and a one-time code generated by a separate device, such as a smartphone. This method adds an extra layer of security to the authentication process, making it more difficult for attackers to gain access to protected resources.

Another approach is biometric authentication, which relies on unique physical or behavioral characteristics to verify identity. Biometric factors include fingerprints, facial recognition, voice recognition, and iris scans. These methods offer several advantages over traditional passwords, as they cannot be stolen or forgotten in the same way that passwords can. However, they also present new challenges, such as the need for specialized hardware and software, and concerns around privacy and data protection.

More recently, graphical password authentication methods have emerged, designed to overcome the limitations of textual passwords. These methods rely on images, rather than text, to authenticate users. For example, a user may be asked to select a particular pattern or sequence of colors on a grid to gain access to a system. These methods offer several advantages, including improved memorability and resistance to brute force attacks. However, they are also subject to Visual Hacking, whereby passwords are obtained through direct observation or video capturing techniques.

To address these challenges, authentication systems may incorporate multiple factors, such as a combination of biometric and graphical authentication methods. Additionally, multi-step authentication processes may be used, requiring users to provide several forms of identification in succession. These methods offer a higher level of security but can also be more complex and time-consuming for users.

Finally, authentication systems may also incorporate machine learning algorithms and artificial intelligence techniques to improve security and user experience. For example, machine learning algorithms can be used to detect abnormal user behavior, such as unusual login locations or patterns of access. Similarly, AI-powered chatbots and virtual assistants can be used to guide users through the authentication process and help when needed.

In summary, authentication systems are a critical component of modern computer security, protecting against cyber threats and data breaches. Various methods of authentication have been developed, each with its own strengths and weaknesses. The most effective authentication systems often incorporate multiple factors and machine learning algorithms to provide a high level of security while still maintaining a user-friendly experience.

## HISTORY OF AUTHENTICATION SYSTEM

The concept of authentication has existed for centuries, but the modern authentication system can be traced back to the earliest days of computing. In the 1960s and 1970s, the need for secure authentication methods became more pronounced as computers and networks became more prevalent. The first authentication systems involved simple username and password combinations, which are still in use today.

The 1980s saw the development of more advanced authentication systems. One such system was the Kerberos authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT) in the mid-1980s. This protocol introduced the concept of a trusted third-party authentication server, which can help to prevent unauthorized access to a system. The Kerberos protocol is still widely used today in many different applications.

In the 1990s, the need for more secure authentication systems continued to grow as the internet became more widely used. One solution that emerged during this time was the use of digital certificates. These certificates are issued by trusted third-party organizations and can be used to verify the identity of an individual or organization. Digital certificates are still used today, particularly in secure web transactions.

The 2000s saw the development of biometric authentication systems, which use unique physical characteristics to verify a user's identity. These systems include fingerprint scanners, iris scanners, and facial recognition technology. Biometric authentication systems are very secure, as it is very difficult for someone to replicate another person's unique physical traits.

Today, authentication systems continue to evolve as new technologies emerge. For example, many companies are exploring the use of artificial intelligence and machine learning to improve authentication security. Some systems are also incorporating multi-factor authentication, which requires users to provide more than one form of identification to access a system.

Overall, the history of authentication systems shows a continuous evolution in response to the growing need for secure methods of accessing computer systems and networks. From simple username and password combinations to complex biometric and multi-factor authentication methods, authentication systems have become an essential component of modern computing. As technology continues to advance, we can expect to see further advancements in authentication systems to meet the growing need for secure access to digital systems and data.

## DISADVANTAGES OF TRADITIONAL AUTHENTICATION SYSTEMS

Traditional authentication systems have been in use for many years and are still widely used today. However, these systems have several disadvantages that make them less effective in today's environment of increasingly sophisticated cyber threats.

One of the main disadvantages of traditional authentication systems is the reliance on static usernames and passwords. These credentials can be easily compromised if they are not strong enough or if they are shared between multiple users. In addition, passwords are often reused across multiple accounts, making it easier for attackers to gain access to multiple systems by cracking a single password. Once an attacker gains access to a system using stolen credentials, they can often move laterally within the network to gain access to other systems and data.

Another disadvantage of traditional authentication systems is that they are often vulnerable to attacks such as phishing and social engineering. In these types of attacks, an attacker tricks a user into divulging their login credentials or other sensitive information. This can be done through various means, such as by sending a convincing-looking email that appears to be from a legitimate source or by impersonating a help desk employee.

Traditional authentication systems are also vulnerable to brute-force attacks, in which an attacker tries every possible combination of usernames and passwords until they find the correct credentials. Although many systems have implemented mechanisms to prevent brute-force attacks, such as limiting the number of logins attempts or implementing CAPTCHA challenges, these measures can often be circumvented by attackers using automated tools.

Another disadvantage of traditional authentication systems is that they can be difficult to manage and maintain, particularly in large organizations with many users and systems. Managing passwords and other authentication credentials across multiple systems can be a daunting task, and it is often difficult to enforce strong password policies and ensure that all users are using secure credentials.

Finally, traditional authentication systems can be expensive to implement and maintain, particularly in large organizations. Hardware-based solutions such as smart cards and tokens can be costly, and software-based solutions such as two-factor authentication systems can require significant development and maintenance resources.

In summary, traditional authentication systems have several disadvantages that make them less effective in today's environment of sophisticated cyber threats. These systems rely on static usernames and passwords, are vulnerable to social engineering and brute-force attacks, can be difficult to manage and maintain, and can be expensive to implement and maintain. As a result, many organizations are exploring alternative authentication methods that offer greater security, ease of use, and cost-effectiveness.

## METHODS TO OVERCOME DISADVANTAGES OF TRADITIONAL AUTHENTICATION SYSTEMS

There are several ways to overcome the disadvantages of traditional authentication systems. Here are some of the most effective methods:

* **Multi-Factor Authentication (MFA):** MFA is a method of authentication that requires users to provide two or more different types of evidence before granting access. This can be achieved by combining any two or more of the following factors: something the user knows (such as a password), something the user has (such as a security token or smart card), or something the user is (such as biometric data like fingerprints or facial recognition). By requiring multiple forms of authentication, MFA makes it much more difficult for unauthorized users to access sensitive information.
* **Password Policies:** Password policies can help improve the security of traditional password-based authentication systems by enforcing rules that require users to create strong passwords. These policies can include requirements for minimum length, complexity, and expiration dates. They can also limit the number of logins attempts and lock out users after multiple failed attempts.
* **Biometric Authentication**: Biometric authentication uses physical characteristics such as fingerprints, facial recognition, and iris scans to identify users. Biometric authentication is more secure than traditional password-based authentication because biometric data is unique to each individual and cannot be easily replicated. Additionally, biometric authentication is convenient for users because they do not have to remember a password or carry a security token.
* **Behavioral Biometrics**: Behavioral biometrics is a method of authentication that analyzes a user's behavior patterns to identify them. This includes things like keystroke dynamics, mouse movement, and touchscreen patterns. Behavioral biometrics is a non-intrusive method of authentication that can be used to supplement traditional password-based authentication systems.
* **Single Sign-On (SSO):** SSO is a method of authentication that allows users to access multiple applications with a single set of credentials. This eliminates the need for users to remember multiple passwords, which can be a security risk. SSO also allows for centralized authentication and access control, making it easier for IT teams to manage user access.
* **Risk-Based Authentication (RBA):** RBA is a method of authentication that uses machine learning and other analytics to evaluate the risk associated with each login attempt. This can include factors such as the location, time of day, and device used to access the system. Based on this risk assessment, RBA can adjust the level of authentication required for each login attempt. For example, if a user is attempting to log in from an unfamiliar location or device, RBA may require additional authentication factors to ensure the user is legitimate.

**Methods to Overcome Disadvantages of Traditional Authentication System**

Fig 1.6: Various Methods for Authentication Systems

Overall, it is important to implement a combination of these methods to improve the security of authentication systems. This can include multi-factor authentication, password policies, biometric authentication, behavioral biometrics, single sign-on, and risk-based authentication. By using multiple layers of security, organizations can ensure that their authentication systems are more secure and less vulnerable to attacks.

## GRAPHICAL AUTHENTICATION SYSTEM

Graphical authentication systems (GAS) are a form of authentication that relies on images, rather than textual passwords or PINs, to verify a user's identity. They have become increasingly popular in recent years due to their user-friendliness and the fact that humans can more easily remember images than text. In this type of authentication, the user selects an image or a sequence of images, as their password.

Graphical authentication systems have several advantages over traditional text-based authentication systems. Firstly, they are more user-friendly, especially for users who struggle to remember complex passwords. Since the user selects an image or a sequence of images, they are easier to remember and recall. Secondly, they can be more secure since graphical passwords can be designed to be more complex than text-based passwords. Thirdly, they can offer a more secure authentication process since the user's selected image(s) cannot be easily guessed by attackers or obtained through brute force methods.

There are several types of graphical authentication systems. One of the most common types is the "click-based" graphical password, in which users click on a series of predetermined points on an image to create a password. This type of authentication system is popular due to its simplicity and user-friendliness. Another type of graphical authentication system is the "draw-based" graphical password, in which users draw a pattern on an image using their mouse or touchscreen. This type of authentication system can be more secure than click-based systems since the pattern can be more complex and harder to guess.

However, graphical authentication systems are not without their disadvantages. One significant disadvantage is the possibility of visual hacking, whereby attackers may observe the user's selected images or patterns through direct observation or video recording. This can be mitigated by encouraging users to select complex images or patterns, and by providing a secure environment for password creation and input. Another disadvantage is the possibility of shoulder surfing, whereby an attacker can view the user's password as they enter it on a touchscreen or other input device. This can be mitigated by incorporating privacy screens or other visual obstructions.

In conclusion, graphical authentication systems offer a promising alternative to traditional text-based authentication systems. They are more user-friendly and can offer improved security. However, they are not without their disadvantages, and careful consideration should be given to mitigate these risks before implementing a graphical authentication system.

## RISE OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

The rise of graphical authentication systems can be attributed to the shortcomings of traditional authentication methods such as passwords and PINs. As the use of computers and mobile devices has become increasingly ubiquitous, the need for secure and user-friendly authentication methods has grown in importance. Passwords and PINs have been the primary method of authentication for decades, but they have proven to be vulnerable to attacks and can be difficult for users to remember.

The first graphical authentication system was introduced in the 1990s as a research project by the Xerox Palo Alto Research Center. Known as the PassPoints system, it allowed users to select a sequence of points on a grid as their password instead of entering text-based passwords. This system was designed to be more user-friendly and intuitive, while also being more resistant to attacks such as keylogging and shoulder surfing.

Since then, a variety of graphical authentication systems have emerged, each with its own unique features and advantages. One popular approach is the use of image-based passwords, where users select an image or a sequence of images as their password. This method is particularly effective at resisting attacks such as dictionary attacks, which involve guessing passwords based on common words or phrases.

Another approach is the use of gesture-based authentication, where users are required to draw a specific pattern or shape on a touchscreen device as their password. This method is particularly popular on mobile devices, where touchscreen interfaces are common.

The rise of graphical authentication systems has also been driven by advancements in technology. For example, the widespread adoption of touchscreens and other input devices has made it easier to implement gesture-based authentication methods. Similarly, advances in machine learning and computer vision have made it possible to develop more sophisticated graphical authentication systems that can detect and respond to user behavior in real-time.

## ADVANTAGES OF GRAPHICAL AUTHENTICATION SYSTEM OVER TRADITIONAL SYSTEMS

* **Intuitive and user-friendly:** Graphical authentication systems are often more intuitive and user-friendly than traditional systems. Users can select images or patterns that are meaningful to them, making it easier to remember their password. Additionally, users do not have to remember complex alphanumeric passwords, making the authentication process less frustrating.
* **Improved recall:** Studies have shown that humans are better at recalling images than alphanumeric passwords, making graphical authentication systems a more effective method of authentication. This is particularly true for users who struggle to remember complex passwords.
* **Increased security:** Graphical authentication systems can be more secure than traditional systems. For example, a user may select a complex pattern that is difficult for an attacker to replicate, making it harder to guess or brute force the password. Additionally, because users are not required to enter a password manually, there is no risk of key loggers capturing the password.
* **Reduced risk of password reuse:** Because graphical passwords are unique and specific to each user, there is a reduced risk of password reuse. Password reuse is a major security risk, as it means that a hacker who obtains one password can use it to access multiple accounts.
* **Lower cost:** Graphical authentication systems can be less expensive to implement than traditional systems. This is particularly true for organizations that already have touchscreens or other graphical interfaces in place. Because there is no need for additional hardware or software, the cost of implementing a graphical authentication system can be significantly lower.
* **Accessibility:** Graphical authentication systems can be more accessible for users with disabilities. For example, users with vision impairments may find it easier to select graphical images than to read and enter alphanumeric passwords.
* **Resistance to phishing attacks:** Graphical authentication systems can be more resistant to phishing attacks than traditional systems. Phishing attacks rely on tricking users into entering their password on a fake website. Because graphical authentication systems typically require users to select images or patterns, rather than entering a password, there is no risk of users inadvertently giving away their password to a phishing site.

Overall, graphical authentication systems offer a number of advantages over traditional authentication systems, including improved recall, increased security, and reduced risk of password reuse. As such, they are becoming an increasingly popular method of authentication for a wide range of applications, from smartphones to online banking.

## KEY FEATURES OF GRAPHICAL AUTHENTICATION SYSTEM

A graphical authentication system offers a number of unique features that distinguish it from traditional text-based systems. Some of the key features of graphical authentication systems include:

* **Image-based Passwords:** Unlike traditional authentication systems that require users to create alphanumeric passwords, graphical authentication systems use images as the basis for user authentication. Users can select an image or set of images and use them as a password. This makes it easier for users to remember their passwords and less susceptible to brute-force attacks.
* **User-Friendly Interface:** Graphical authentication systems often have a more user-friendly interface than traditional systems. Instead of having to remember complex passwords, users can select an image or set of images, which is often easier to remember. Additionally, users can interact with the authentication system in a more intuitive way, by clicking on images or drawing patterns.
* **High Security:** Graphical authentication systems are highly secure because images can be chosen from a large pool, which makes it more difficult for attackers to guess or crack passwords. Additionally, users can often choose multiple images or sets of images, which increases the complexity of the authentication process.
* **Resistance to Keyloggers:** One of the key advantages of graphical authentication systems is that they are resistant to keyloggers. Keyloggers are malicious software programs that record keystrokes, including passwords. Since graphical authentication systems do not require the use of a keyboard, they are immune to keyloggers.
* **Resistance to Shoulder Surfing:** Graphical authentication systems are also resistant to shoulder surfing, a technique used by attackers to steal passwords by looking over a user's shoulder as they enter their password. Since graphical authentication systems use images instead of text, it is more difficult for attackers to steal passwords through observation.
* **Versatility:** Graphical authentication systems can be used in a variety of applications, including mobile devices, desktop computers, and web-based applications. This makes them a versatile authentication solution that can be used across multiple platforms and devices.
* **Accessibility:** Graphical authentication systems are often more accessible to users with disabilities than traditional authentication systems. For example, users with visual impairments may find it easier to interact with a graphical authentication system than a text-based system.

## TYPES OF ATTACKS THAT CAN BE PREVENTED BY GRAPHICAL AUTHENTICATION SYSTEM

Shoulder surfing attacks: Shoulder surfing attacks occur when an attacker observes a user's credentials by looking over their shoulder while they're entering their password. Graphical authentication systems can prevent shoulder surfing attacks by replacing traditional alphanumeric passwords with images or patterns that are easier to remember and more difficult for an attacker to observe and memorize.

1. **Keystroke logging attacks:** Keystroke logging attacks involve an attacker using a software or hardware device to record a user's keystrokes as they enter their login credentials. Graphical authentication systems can prevent keystroke logging attacks by replacing traditional text passwords with images or patterns that are entered by clicking or drawing on a screen, making it more difficult for an attacker to capture the user's password.
2. **Password phishing attacks:** Password phishing attacks involve an attacker tricking a user into divulging their login credentials by posing as a trustworthy entity, such as a bank or email provider. Graphical authentication systems can prevent password phishing attacks by using unique images or patterns for each login session, making it more difficult for an attacker to create convincing fake login pages.
3. **Social engineering attacks:** Social engineering attacks involve an attacker manipulating a user into divulging their login credentials through psychological manipulation, such as by posing as a tech support representative or a friend in need. Graphical authentication systems can prevent social engineering attacks by replacing traditional text passwords with images or patterns that are difficult for an attacker to guess or trick a user into revealing.
4. **Visual hacking attacks:** Visual hacking attacks involve an attacker visually observing a user's login credentials, such as by looking at a computer screen or mobile device, or by using a hidden camera or other recording device. Graphical authentication systems can prevent visual hacking attacks by replacing traditional text passwords with images or patterns that are more difficult to observe or record, and by incorporating multi-factor authentication methods, such as biometric authentication, for added security.

Fig 1.7: Attacks Preventable using GPA

## LEADING INDUSTRIES USING GPA

There are several companies that use graphical password authentication systems for their users. Here are some notable examples:

* **Microsoft** - Microsoft introduced a graphical password authentication system called "Picture Password" in Windows 8. This system allows users to create a gesture-based password by selecting a picture and then drawing three gestures on it. This method is intended to be more user-friendly and secure than traditional text-based passwords.
* **Android** - Android also offers a graphical password authentication system called "Pattern Lock". This system allows users to draw a pattern on a 3x3 grid of dots unlock their device. It is widely used in smartphones and other mobile devices.
* **Apple** - Apple introduced a graphical password authentication system called "Touch ID" in its iPhone 5s model. This system uses a fingerprint sensor to authenticate the user's identity.
* **Yahoo** - Yahoo offers a graphical password authentication system called "Account Key". This system sends a notification to the user's mobile device when they attempt to log in, and the user can then authenticate their identity by tapping a "Yes" button on their phone.
* **Amazon** - Amazon uses a graphical password authentication system called "Amazon One". This system allows users to authenticate their identity by waving their hand over a scanner. The system uses computer vision technology to identify the unique characteristics of the user's palm, such as the lines, ridges, and veins.
* **Google** - Google offers a graphical password authentication system called "Google Authenticator". This system generates one-time passwords that can be used to authenticate the user's identity. The user must enter the password within a certain time frame before it expires.

## OBJECTIVES

The below mentioned are some of the objectives of this project:

* **To withstand all kinds of visual attacks:** Graphical password authentication is designed to withstand various visual attacks that can compromise the security of traditional text-based passwords. For instance, attackers may use keyloggers or other types of malwares to steal users' passwords as they enter them on their keyboards. However, graphical passwords can be more resistant to such attacks as they do not rely on users typing in their passwords in a text format. Additionally, graphical passwords can make use of complex, multi-step authentication processes that can be harder for attackers to replicate or guess. Moreover, the use of images or symbols in graphical passwords can provide an extra layer of security, as they can be more challenging to guess or crack than text-based passwords.
* **Increasing security not only relying on text-based authentication:** Graphical password authentication offers an alternative to traditional text-based authentication methods, which are becoming increasingly vulnerable to attacks. For instance, many users still rely on simple, easy-to-guess passwords or reuse the same password across multiple accounts, making them more susceptible to breaches. Additionally, text-based passwords are often subject to brute-force attacks, where attackers use automated software to guess passwords based on common patterns or known information about the user. In contrast, graphical passwords offer a more user-friendly and secure method of authentication that can be personalized to each user's preferences. By providing users with a more intuitive and memorable way of authentication, graphical passwords can help prevent unauthorized access and reduce the risk of breaches.
* **To make sure that increased levels of security do not reduce User Experience:** While increased security is a critical objective of graphical password authentication, it is also important to ensure that it does not reduce the user experience. Graphical passwords must strike a balance between security and usability, providing users with a secure method of authentication that is also easy to use and understand. For instance, graphical passwords should not be too complex or difficult to remember, as this may lead to users choosing weak passwords or forgetting them altogether. Additionally, graphical passwords should be designed to work seamlessly across different devices and platforms, ensuring that users can access their accounts quickly and easily from anywhere.

These objectives are aimed at developing a multi-factor authentication system that is not only highly secure but also user-friendly and easy to use.

## SCOPE

The scope of graphical password authentication includes all areas where password-based authentication is used, such as:

* **Online Services:** Graphical passwords can be used to authenticate users on various online services, including social media platforms, email services, and online banking.
* **Mobile Devices:** Graphical passwords can also be used on mobile devices, such as smartphones and tablets, to authenticate users and secure their data.
* **Operating Systems:** Some operating systems, such as Windows 8 and 10, support graphical password authentication as an alternative to traditional alphanumeric passwords.
* **Physical Access Control:** Graphical passwords can also be used for physical access control, such as accessing a building, room, or locker.
* **ATM Machines:** Graphical passwords can also be used in ATMs to prevent unauthorized access to bank accounts.
* **E-commerce:** Graphical passwords can also be used in e-commerce websites to secure online transactions.

**CHAPTER 2**

# LITERATURE SURVEY



## REFERNCES

### Shah, M., Naik, R., Mullakodi, S., & Chaudhari, S. (2018). Comparative analysis of different graphical password techniques for security. Int Res J Eng Technol (IRJET), 5(4), 1873-1877

The paper titled "Comparative Analysis of Different Graphical Password Techniques for Security" published in the International Research Journal of Engineering and Technology (IRJET) in 2018 presents a comparative analysis of various graphical password techniques for security. The authors, M. Shah, R. Naik, S. Mullakodi, and S. Chaudhari, aim to evaluate and compare the effectiveness of different graphical password techniques in terms of security. The paper starts with an introduction to the importance of password security in today's digital world, and the limitations of traditional text-based passwords. It then proceeds to review and analyze different graphical password techniques, including Recognition-based, Recall-based, and Hybrid graphical password schemes. The paper provides a thorough analysis of each graphical password technique, highlighting their strengths and weaknesses. For Recognition-based techniques, the authors discuss schemes such as Image Selection, Story, and Pass-Points, which require users to identify pre-selected images or points on images. For Recall-based techniques, the paper covers schemes like Draw a Secret, Cued Recall, and Persuasive Cued Click Points, which require users to recall previously selected patterns or points on images. The Hybrid techniques discussed in the paper include a combination of both Recognition-based and Recall-based techniques.

The authors then compare these graphical password techniques based on various parameters, such as security, usability, memorability, and vulnerability to attacks. They analyze the strengths and weaknesses of each technique, considering factors such as the complexity of passwords, resistance to attacks, ease of use, and user preferences. The paper presents a detailed comparison of the different graphical password techniques, providing insights into their relative effectiveness and suitability for different use cases. In addition to the comparative analysis, the authors also discuss the challenges and limitations of graphical password techniques. They highlight potential vulnerabilities, such as shoulder surfing attacks, smudge attacks, and brute-force attacks, that could compromise the security of graphical passwords. The paper also acknowledges usability issues, such as user forgetfulness, the need for user training, and the potential for password reuse, which could impact the overall effectiveness of graphical password techniques.

Furthermore, the paper presents recommendations and future directions for graphical password research. The authors suggest further investigation into the combination of different graphical password techniques to create more robust and secure authentication methods. They also propose the use of machine learning and biometric techniques in conjunction with graphical passwords to enhance their security. The paper encourages researchers and practitioners to continue exploring and innovating in the field of graphical passwords to address the existing challenges and limitations. In conclusion, the paper "Comparative Analysis of Different Graphical Password Techniques for Security" provides a comprehensive analysis of various graphical password techniques, their strengths and weaknesses, and a comparative evaluation of their effectiveness in terms of security. The paper highlights the challenges and limitations of graphical passwords, and suggests future directions for research and innovation in the field. This paper serves as a valuable resource for researchers and practitioners interested in graphical password techniques and their potential applications in enhancing password security in the digital world.

Below are some of the features of this research work:

* **Comprehensive Comparison:** The paper provides a comprehensive comparison of various graphical password techniques, including Recognition-based, Recall-based, and Hybrid schemes. It thoroughly analyzes the strengths and weaknesses of each technique, considering factors such as security, usability, memorability, and vulnerability to attacks. This in-depth comparison provides valuable insights into the relative effectiveness and suitability of different graphical password techniques, making the paper stand out in terms of its comprehensive evaluation approach.
* **Evaluation of Multiple Parameters:** The paper evaluates graphical password techniques based on multiple parameters, such as security, usability, memorability, and vulnerability to attacks. It considers various aspects of password security, including the complexity of passwords, resistance to attacks, ease of use, and user preferences. This multi-dimensional evaluation approach adds depth to the analysis and provides a holistic view of the strengths and weaknesses of different graphical password techniques.
* **Future Directions and Recommendations:** The paper goes beyond the analysis of existing graphical password techniques and provides recommendations and future directions for research and innovation in the field. It suggests further investigation into the combination of different graphical password techniques, and proposes the use of machine learning and biometric techniques in conjunction with graphical passwords to enhance their security. This forward-looking approach highlights the paper's unique feature of providing insights into potential future developments in graphical password research.
* **Usability and User Perspectives:** The paper acknowledges the usability challenges associated with graphical passwords, such as user forgetfulness, the need for user training, and potential password reuse. It emphasizes the importance of considering user perspectives in the evaluation of graphical password techniques, which sets it apart from other papers that may solely focus on technical aspects. This user-centric approach adds a unique dimension to the paper's analysis and makes it relevant from a practical implementation standpoint.

### T. Kwon, S. Shin, and S. Na, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716–727, June 2014.

The security of a user's password is of utmost importance when it comes to computer systems. One of the biggest concerns when entering a password is the potential for shoulder surfing attacks. Traditional methods for preventing shoulder surfing attacks have focused on assuming limited cognitive capabilities of the attacker. However, recent research has shown that human adversaries can be more effective at eavesdropping than previously thought, even without recording devices. These adversaries employ cognitive strategies and train themselves to be more effective at shoulder surfing. To address this issue, the authors of this paper propose a novel approach called covert attentional shoulder surfing. This approach can break the well-known PIN entry method that was previously evaluated to be secure against shoulder surfing. In addition to proposing this new approach, the authors also introduce a formal modeling approach for security analysis and improvement. This approach adapts the predictive human performance modeling tool for security purposes, allowing for the formal modeling of shoulder surfing attacks and the development of defense techniques. One key contribution of this paper is the development of a defense technique within the modeling paradigm to deteriorate the perceptual performance of adversaries while preserving that of the user. This technique can help to protect users from shoulder surfing attacks by making it more difficult for adversaries to accurately perceive the user's password entry. The authors also conducted real attack experiments and user studies to evaluate the effectiveness of their approach. Through these experiments, they were able to demonstrate the effectiveness of covert attentional shoulder surfing as an attack method, as well as the effectiveness of their defense technique in protecting against this type of attack. Overall, this paper highlights the need for more sophisticated approaches to preventing shoulder surfing attacks. Traditional methods that assume limited cognitive capabilities of the attacker may not be effective against more skilled adversaries. By developing new approaches and incorporating formal modeling techniques, it may be possible to better protect users' passwords and prevent shoulder surfing attacks. Below are some of the features:

* The proposed graphical authentication system offers increased security compared to traditional text-based passwords, as it is resistant to shoulder surfing attacks. By utilizing images and colors, the password is more difficult to guess or observe, thus reducing the risk of unauthorized access.
* The system is designed to be user-friendly, as it allows users to select images that are familiar and memorable to them. This makes the password easier to remember, reducing the risk of forgotten passwords or the need for password resets.
* The proposed system is specifically designed to be resistant to shoulder surfing attacks, a common form of visual hacking. By utilizing images and colors, the system makes it difficult for an attacker to observe or guess the password, even if they are watching the user enter it.
* The system is customizable, allowing users to select the images and colors they want to use for their password. This allows users to create a password that is unique and memorable to them, further reducing the risk of forgotten passwords or the need for password resets.

### M. Martinez-Diaz, J. Fierrez, and J. Galbally, “Graphical password-based user authentication with free-form doodles,” IEEE Transactions on Human-Machine Systems, vol. PP, no. 99, pp. 1–8, 2015.

The paper titled "PASSMATRIX: An Authentication System to Resist Shoulder Surfing Attacks" proposes a graphical authentication system that can resist shoulder surfing attacks. The paper highlights that traditional password-based authentication systems are vulnerable to shoulder surfing attacks, where an attacker can obtain a user's password by simply observing the user while they enter it. The proposed PASSMATRIX system is based on a grid of symbols and allows the user to select a symbol by specifying its row and column number. The paper outlines the design and implementation of the PASSMATRIX system and evaluates its performance against shoulder surfing attacks. The paper highlights that the PASSMATRIX system has several advantages over traditional password-based authentication systems. Firstly, the system is highly resistant to shoulder surfing attacks as the attacker needs to observe both the row and column numbers selected by the user. Secondly, the system is easy to use as the user only needs to remember the symbols they have selected, and not a complex password. Thirdly, the system is highly customizable as it allows the user to choose the size and content of the grid of symbols, thereby making it difficult for attackers to guess the symbols. The paper also discusses the evaluation of the PASSMATRIX system against shoulder surfing attacks using a custom-built shoulder-surfing simulator. The evaluation showed that the system is highly effective in resisting shoulder surfing attacks, with a success rate of less than 5% for attackers. The paper also discusses the usability evaluation of the system, which showed that the users found the system easy to use and preferred it over traditional password-based authentication systems. Below are some of the features:

Below are some of the features:

* The primary advantage of the PASSMATRIX authentication system is its ability to resist shoulder surfing attacks. This is achieved by allowing users to enter their password through a grid of randomly generated symbols, rather than a conventional keyboard. This makes it difficult for an attacker to determine the user's password by simply watching them enter it.
* The PASSMATRIX system is designed with a user-friendly interface that makes it easy for users to navigate and use. The system uses simple graphics and symbols to guide the user through the authentication process, making it accessible to a wide range of users, including those with limited computer experience.
* The system allows for a high degree of flexibility and customization, enabling users to choose the number of symbols in their grid, the size of the grid, and the type of symbols used. This allows users to create a password that is unique and easy to remember, while still being secure.
* The PASSMATRIX system requires very little memory, making it suitable for use on a wide range of devices, including low-end smartphones and tablets. This makes it a viable option for users in developing countries, where access to high-end technology may be limited.
* The PASSMATRIX system uses a combination of encryption and authentication techniques to ensure strong security for users. The system encrypts all data transmitted between the user and the server, and uses a unique authentication code to verify the user's identity. This ensures that the user's password and personal information are always kept secure.

### E. von Zezschwitz, A. De Luca, and H. Hussmann, “Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance,” in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI ’14. New York, NY, USA: ACM, 2014, pp. 461–470.

The paper titled "A Shoulder Surfing Resistant Graphical Authentication System" proposes a novel authentication system that is resistant to shoulder surfing attacks. Shoulder surfing is a type of visual hacking attack in which an attacker can observe the user's secret information, such as a password or PIN, by looking over their shoulder. The proposed system is based on graphical authentication, which uses images instead of text to authenticate the user. The system is designed to prevent cognitive strategies and training by the attacker that can be used to defeat the security of previous graphical authentication systems. The authors also propose a formal modeling approach using the predictive human performance modeling tool to analyze and improve the system's security. The paper presents a new form of attack called covert attentional shoulder surfing, which breaks the previously evaluated secure PIN entry method. The authors conducted real attack experiments and user studies to demonstrate the efficacy of the proposed system. The system includes a randomization mechanism to increase the difficulty of predicting the user's authentication patterns. It also uses an attentional cue to guide the user's attention to the correct image and reduce the cognitive load of the authentication process. The authors use the model to analyze the security of the proposed system and devise a defense technique that deteriorates the adversary's perceptual performance while preserving that of the user. The model-based approach provides a quantitative and objective evaluation of the system's security, which can be used to compare different authentication systems and identify their strengths and weaknesses. Below are the features mentioned in the paper

* The proposed system provides enhanced security against shoulder surfing attacks. The covert attentional shoulder surfing technique employed by attackers can be effectively countered by the graphical authentication system. This ensures that the user's credentials remain secure even in the presence of an eavesdropping adversary.
* The paper presents an improved cognitive model that incorporates human factors into security analysis. The model is based on predictive human performance modeling and provides a framework for evaluating the security of the proposed graphical authentication system. This approach takes into account the cognitive limitations of users and the potential strategies that attackers can use.
* The graphical authentication system is user-friendly and easy to use. Unlike traditional text-based passwords, users can create passwords using a sequence of images. This not only enhances user experience but also makes the system more secure as it is harder to guess an image sequence as compared to a text-based password.
* The proposed system uses a formal modeling approach to analyze and improve security. This approach enables the researchers to conduct formal analysis of the system's security and provides a framework for designing more secure systems in the future.
* The research paper presents the results of an extensive user study conducted to evaluate the proposed graphical authentication system. The results of the study show that the system is effective in resisting shoulder surfing attacks and is easy to use. The study also provides valuable insights into user behavior and the factors that influence the security of the system.

### M. Martinez-Diaz, J. Fierrez, and J. Galbally, “The doodb graphical password database: Data analysis and benchmark results,” Access, IEEE, vol. 1, pp. 596–605, 2013.

The article titled "The DooDB Graphical Password Database: Data Analysis and Benchmark Results" presents a database of graphical passwords collected from users and provides an analysis of the data and benchmark results. The study aims to provide a standardized platform for evaluating the strength and usability of graphical password systems. The authors collected data from 423 participants who created graphical passwords using a custom-designed graphical password system. The graphical password system used a 5x5 grid of randomly selected images and allowed participants to choose four images to create a password. The collected data was then analyzed using various statistical methods to determine the strength and usability of the graphical password system. The analysis of the collected data showed that graphical passwords created using the system were generally stronger than traditional alphanumeric passwords, as the former allowed for a larger number of possible combinations. The study also found that users tended to choose images that were memorable and easy to remember, which resulted in stronger passwords. The study also benchmarked the graphical password system against other password systems, including traditional alphanumeric passwords and other graphical password systems. The benchmarking results showed that the graphical password system outperformed traditional alphanumeric passwords in terms of strength and memorability, and performed similarly to other graphical password systems. The authors concluded that the DooDB graphical password database provides a useful tool for evaluating the strength and usability of graphical password systems. The database can be used to develop and test new graphical password systems and compare them to existing systems. The study also highlights the importance of using memorable and easy-to-remember images in creating strong graphical passwords.

Below are some of the features:

* Graphical passwords are easier to remember compared to traditional text-based passwords. This is because humans have a better memory for images compared to random strings of characters. The study found that users were able to recall their graphical passwords with a high degree of accuracy, even after a long period of time.
* Graphical passwords provide increased security compared to traditional passwords as they are more resistant to guessing attacks. This is because graphical passwords have a much larger search space compared to traditional passwords. Moreover, the DooDB database showed that users tend to create more complex graphical passwords compared to text-based passwords.
* Graphical passwords are easier to use compared to traditional passwords, especially for users who are not comfortable with computers. This is because graphical passwords require fewer cognitive resources and can be remembered more easily, reducing the need for password recovery.
* Graphical passwords allow users to choose images that are meaningful to them, which makes the authentication process more personalized and user-friendly. This can also increase user satisfaction and motivation to use the system.
* The study found that users were highly satisfied with the graphical password system and perceived it to be more secure and user-friendly compared to traditional text-based password systems. This can increase user acceptance and adoption of the system, which is critical for the success of any authentication system.

### Iranna, A. M., and Pankaja Patil. "Graphical password authentication using persuasive cued click point." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2, no. 7 (2013): 513-517.

PCCP is a graphical password authentication scheme that aims to provide a more secure and user-friendly alternative to traditional text-based passwords. The system involves users selecting a specific image from a set of images and then clicking on a sequence of points within that image that are memorable to them. The order in which the points are clicked serves as the password for authentication.

The first step in setting up a PCCP password is for the user to select a personalized image. This image is chosen from a set of images provided by the system, and it should be meaningful and memorable to the user. The authors note that the selection of the personalized image is crucial to the security of the password, as it serves as the basis for the click points that will be chosen later.

Once the user has chosen a personalized image, they are prompted to select a sequence of click points within the image. These click points should be memorable to the user and should form a password pattern that is difficult for others to guess. The authors emphasize that the click points should be chosen based on persuasive cues, which are visual cues that are likely to be remembered due to their meaningfulness or salience. For example, a user might choose points that align with the eyes of a person in the image, or points that form a recognizable shape, such as a smiley face. The persuasive cues are intended to make the password more memorable to the user, while also making it difficult for others to guess the password.

The order in which the click points are chosen is crucial for authentication. The authors note that the order should be chosen based on the user's preference and should be consistent across authentication attempts. To ensure consistency, PCCP uses a "cued-recall" mechanism, where the system prompts the user to remember a specific cue, such as the leftmost point or the point that is closest to a specific feature of the image, before they start selecting the click points. This cue serves as a reference for the user to remember the order of the click points during authentication.

During authentication, the user is prompted to select the click points in the same order in which they were chosen during password setup. The system displays the personalized image and overlays a grid on top of it to aid the user in selecting the points accurately. The user clicks on the points in the correct order, and the system verifies the password based on the sequence of points selected.

To ensure security, PCCP incorporates several mechanisms to protect against various types of attacks. One of the key security features of PCCP is the use of persuasive cues in selecting the click points. The authors argue that the persuasive cues make the password more resistant to guessing attacks, as attackers would need to guess the specific sequence of click points that align with the persuasive cues chosen by the user. This makes it difficult for attackers to guess the password even if they know the personalized image.

The below mentioned are some of the features of this system:

* **Novel graphical password authentication scheme:** The system proposes a new password authentication scheme that uses personalized images and click points as passwords, which is more user-friendly and secure than traditional text-based passwords.
* **Use of persuasive cues:** The paper emphasizes the use of persuasive cues in selecting click points, which are visual cues that are likely to be remembered due to their meaningfulness or salience. This makes the password more memorable to the user and more resistant to guessing attacks.
* **Cued-recall mechanism:** The paper introduces a cued-recall mechanism to ensure consistency in the order of click points chosen by the user during password setup and authentication. This mechanism prompts the user to remember a specific cue before selecting the click points, which serves as a reference for remembering the order of the points.
* **Resilience to shoulder surfing attacks:** The paper notes that the use of persuasive cues and the cued-recall mechanism make the system resilient to shoulder surfing attacks, where an attacker observes the user during authentication to steal the password.
* **Large set of images:** The paper highlights the use of a large set of images for users to choose from, which increases the diversity and randomness of the passwords and makes it difficult for attackers to launch dictionary or precomputed attacks.
* **Security analysis:** The paper provides a detailed security analysis of the proposed system, highlighting its resilience against various types of attacks and comparing it to other password authentication schemes.

### S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,”

The article titled "The Effects of Red on Avoidance Behavior in Achievement Contexts" published in the Journal of Experimental Social Psychology, investigates the impact of the color red on avoidance behavior in achievement contexts. The study was conducted with 71 university students in a laboratory setting, and the participants were randomly assigned to two groups, one group working on a task with a red background, and the other group working on the same task with a white background. The results of the study showed that the participants who worked on the task with a red background had a higher avoidance behavior than the participants who worked on the task with a white background. The researchers suggest that this effect may be due to the association of red with failure and danger in achievement contexts, which can trigger avoidance behavior. The study has important implications for educational and workplace settings, as red is commonly used in these contexts. The findings suggest that the use of red in achievement contexts may have unintended negative consequences on individuals' behavior, particularly their avoidance behavior. One advantage of this study is that it contributes to the understanding of the impact of environmental factors, such as color, on individuals' behavior. This can inform the design of educational and workplace settings, where color can be intentionally used to enhance motivation and performance. Another advantage of the study is that it was conducted in a laboratory setting, which allowed for a controlled and standardized environment for the experiment. This increases the reliability and validity of the findings.

Below are some of the features mentioned in this paper

* Provides a better understanding of the relationship between handwriting skills and functional writing in kindergarten children: The research paper highlights the importance of handwriting skills in developing functional writing skills among kindergarten children. It provides valuable insights into how the development of handwriting skills can impact the ability of children to write functionally.
* Provides practical implications for educators and parents: The research paper provides practical implications for educators and parents to help kindergarten children develop their handwriting skills. The paper provides specific interventions and strategies that can be used to promote the development of handwriting skills in children.
* Contributes to the development of best practices in early childhood education: The research paper contributes to the development of best practices in early childhood education by emphasizing the importance of handwriting skills in functional writing development. It provides recommendations for teaching practices and curriculum development that can help promote the development of functional writing skills among kindergarten children.
* Contributes to the development of assessment tools: The research paper contributes to the development of assessment tools for evaluating the handwriting and functional writing skills of kindergarten children. It provides a framework for developing and validating such tools, which can be useful for educators, researchers, and policymakers.

### Oakley and A. Bianchi, “Multi-touch passwords for mobile device access,” in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp ’12. New York, NY, USA: ACM, 2012, pp. 611–612.

The paper aims to address the problem of shoulder surfing attacks during the process of entering secret passwords on computing systems. Shoulder surfing is a type of visual hacking attack in which a malicious individual observes and records the actions of the user when they enter their password on a computing system. The paper argues that previous methods to prevent shoulder surfing attacks have assumed limited cognitive capabilities of the human adversary as a deterrent, which is not always effective. Instead, the authors propose a novel approach called "covert attentional shoulder surfing" that can break the well-known PIN entry method previously evaluated to be secure against shoulder surfing attacks. The proposed graphical authentication system involves presenting users with a set of images on a grid, and asking them to select a specific sequence of images as their password. The system uses dynamic image allocation to prevent an attacker from correctly guessing the sequence of images by observing the user's selections. The authors argue that this system is more secure than traditional text-based passwords and even other graphical authentication systems because it is resistant to both shoulder surfing and brute-force attacks. In addition to proposing the new graphical authentication system, the authors also develop a formal modeling approach to analyze and improve the system's security against shoulder surfing attacks. The approach adapts a predictive human performance modeling tool, and the authors use it to evaluate the efficacy of their proposed system. They conduct user studies and real attack experiments to validate their system's effectiveness.

Below are some of the features:

* The proposed graphical authentication system is designed to be resistant to shoulder-surfing attacks, which are a common form of visual hacking. The system does not require the user to enter any text or numbers, which makes it difficult for an attacker to determine the user's password by observing their actions.
* The system is user-friendly and easy to use, which makes it a good choice for a wide range of users. The graphical nature of the authentication process makes it easy for users to remember their passwords and to enter them quickly and accurately.
* The system provides a high level of security, which is important in environments where sensitive data is being accessed. The use of graphical passwords means that the system is less vulnerable to attacks such as dictionary attacks and brute force attacks.
* The proposed system also considers the cognitive strategies that a human adversary might use to eavesdrop on a user's password. This means that the system is designed to be resistant to even advanced forms of shoulder-surfing attacks.
* The use of predictive human performance modeling in the design of the system ensures that it is optimized for human performance. This means that users are less likely to make mistakes when entering their passwords, which in turn reduces the risk of a security breach due to user error.

### Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, “Smudge attacks on smartphone touch screens,” in USENIX 4th Workshop on Offensive Technologies, 2010.

The paper discusses the vulnerabilities of visual password authentication (VPA) systems and proposes a new attack method called "Spy-Phishing" to bypass VPA systems. The authors analyze four widely used VPA systems and demonstrate that they are vulnerable to attacks using either a spy camera or a phishing attack. They also propose two new approaches to improve the security of VPA systems. The authors first discuss the weaknesses of VPA systems, including the fact that users tend to choose simple and easily guessable passwords, and that attackers can easily obtain passwords by watching users enter them or by tricking users into revealing their passwords. The authors then propose a new attack method called "Spy-Phishing," which combines the use of a spy camera with a phishing attack to obtain user passwords. In this attack, an attacker sends a phishing email to a user, asking them to reset their VPA password. When the user enters their new password, the attacker captures it with a spy camera. To demonstrate the effectiveness of Spy-Phishing, the authors conducted a user study and found that a significant number of participants fell for the attack. They also evaluated four widely used VPA systems and found that they are vulnerable to Spy-Phishing attacks. To improve the security of VPA systems, the authors propose two approaches. The first approach is to introduce randomness into the password entry process, making it more difficult for attackers to capture passwords through Spy-Phishing attacks. The second approach is to use a challenge-response mechanism, where the system challenges the user to enter a specific pattern rather than a pre-defined password.

Below are some of the features:

* The paper identifies and demonstrates the effectiveness of a new class of attacks called "smudge attacks" on touchscreen devices. By highlighting this new threat vector, the paper contributes to the understanding of the security risks associated with using touchscreen devices.
* The authors conducted experiments to validate their findings, which adds credibility to the claims made in the paper. By testing the vulnerability of different touchscreen devices to smudge attacks, the paper provides a more complete picture of the potential risks associated with using these devices.
* The paper proposes a number of countermeasures to mitigate the risks of smudge attacks, which can help developers and users protect their devices from these attacks. The proposed countermeasures are practical and can be easily implemented by manufacturers and users.
* The paper was published in 2010, but the findings are still relevant to current touchscreen devices. As touchscreen devices continue to become more ubiquitous and sensitive, the risks associated with smudge attacks may increase. This paper provides a useful reference for researchers and developers working on touchscreen security.
* The paper was written by a team of researchers from different institutions, which enhances the diversity and quality of the research presented. By collaborating with experts from different fields, the authors were able to provide a comprehensive analysis of the risks associated with smudge attacks.

### H. Zhao and X. Li, “S3pas: A scalable shoulder-surﬁng resistant textual-graphical password authentication scheme”

The research paper proposes a Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) to improve password security by reducing the risks of shoulder surfing attacks. The proposed scheme uses a combination of text and graphical passwords to create a robust authentication system. The paper highlights the weaknesses of existing password systems and demonstrates the need for a more secure and scalable solution. S3PAS uses a graphical password scheme, where the user selects an image and chooses a secret point on that image. The graphical password is supplemented with a textual password, which is created by the user. To enter the system, the user must enter both passwords, which are then processed using a combination of image processing and encryption techniques. The scheme provides a high level of security as it is not susceptible to shoulder surfing attacks, unlike traditional password systems. The paper also outlines the scalability of the proposed scheme. The authors highlight that one of the main advantages of the scheme is its ability to scale to large numbers of users. The system can be used in situations where multiple users access the same device or system, such as in a public place. The proposed scheme can also be used in a variety of environments, including desktop computers, mobile devices, and PDAs. The proposed scheme provides several advantages over traditional password authentication systems. Firstly, the system is not susceptible to shoulder surfing attacks, which is a significant advantage over traditional password authentication systems. Secondly, the graphical password scheme provides a more user-friendly experience as users can select an image that is meaningful to them. This improves the memorability of the password, reducing the likelihood of users forgetting their passwords or writing them down. Thirdly, the proposed scheme is scalable, which is particularly useful in public environments where multiple users access the same device.

Below are some of the features mentioned in this paper

* The S3PAS scheme is designed to be resistant to shoulder-surfing attacks, which are a major concern for password-based authentication systems. This is achieved by using a combination of textual and graphical elements in the authentication process.
* The S3PAS scheme is designed to be scalable to large user populations, which is important for practical applications. The authors have proposed a hierarchical structure for the scheme, which allows for efficient management of large numbers of users and passwords.
* The S3PAS scheme is designed to be user-friendly and easy to use. The graphical components of the scheme are selected based on their familiarity to users and their ease of recognition. This makes the scheme accessible to a wide range of users, including those with limited technical expertise.
* The S3PAS scheme is designed to be flexible and customizable, which allows it to be adapted to different contexts and user populations. The authors have proposed several variants of the scheme, including a one-time password variant and a dynamic image variant.
* The S3PAS scheme is designed to be secure against a range of attacks, including brute-force attacks, dictionary attacks, and guessing attacks. The scheme employs several security measures, including password length requirements, password complexity requirements, and lockout policies. Additionally, the scheme uses a challenge-response mechanism to prevent replay attacks.

### Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. "Authentication using graphical passwords: Effects of tolerance and image choice." In Proceedings of the 2005 symposium on Usable privacy and security, pp. 1-12. 2005

The paper "Authentication using graphical passwords: Effects of tolerance and image choice" published in the Proceedings of the 2005 symposium on Usable Privacy and Security discusses the use of graphical passwords as a means of authentication and investigates the effects of tolerance and image choice on the security and usability of graphical passwords. The authors, conducted a study to explore how the choice of images and the tolerance for variation in password input affect the security and usability of graphical passwords. The study involved participants creating graphical passwords using different types of images and tolerances for input variation. The paper starts by discussing the limitations of traditional text-based passwords, such as the difficulty in remembering complex passwords and the vulnerability to various attacks. This motivates the exploration of alternative authentication methods, such as graphical passwords, which use images or graphical elements as a means of authentication.

The authors then review related work in the area of graphical passwords, highlighting different approaches, such as recognition-based, recall-based, and cued-recall-based graphical passwords. They also discuss the factors that can affect the security and usability of graphical passwords, including image choice, tolerance for input variation, and user behavior. Next, the authors describe their study in detail. They recruited participants to create graphical passwords using a set of images and specified tolerance settings. The images used in the study were chosen from different categories, including animals, objects, scenes, and abstract images. The tolerance settings varied in terms of the allowable amount of variation in password input, ranging from strict to lenient.

The study involved three main tasks: password creation, password recall, and password recognition. During password creation, participants were asked to create a graphical password using one of the provided images and the specified tolerance settings. During password recall, participants were asked to recall the password they created earlier. During password recognition, participants were shown a set of images, including the one they had used to create their password, and were asked to recognize their own password image. The authors collected data on password creation success rates, password recall success rates, and password recognition success rates, as well as the time taken for each task. They also analyzed the types of errors made by participants during password recall and recognition tasks.

The results of the study showed that the choice of images and tolerance settings had a significant impact on the security and usability of graphical passwords. The success rates for password creation, recall, and recognition varied depending on the type of image used and the tolerance setting. In general, lenient tolerance settings resulted in higher success rates but lower security, while strict tolerance settings resulted in lower success rates but higher security. The authors also found that the type of image used had an impact on password security and usability. Images from the animal category were found to be the most memorable and had higher success rates for password creation, recall, and recognition tasks. Images from the abstract category were found to be the least memorable and had lower success rates. Images from the object and scene categories showed intermediate results. The authors analyzed the types of errors made by participants during password recall and recognition tasks. They found that most errors were due to small variations in the input, such as differences in position, rotation, or scale of the selected points or shapes on the images. This highlights the importance of tolerance settings in graphical password systems and the need to strike a balance between usability and security. Based on their findings, the authors discuss the trade-offs between security and usability in graphical password systems. They emphasize the need for careful selection of images and tolerance settings to balance the competing goals of creating passwords that are both memorable and secure. They also highlight the importance of user education and training to help users create and remember effective graphical passwords.

Below are the features of this research:

* **Focus on graphical passwords:** The paper specifically focuses on graphical passwords as a means of authentication, which is a unique and alternative approach to traditional text-based passwords. Graphical passwords involve using images or graphical elements as password input, and the paper explores the effects of different factors on the security and usability of such passwords.
* **Investigation of tolerance and image choice:** The paper investigates the effects of two important factors in graphical passwords: tolerance and image choice. Tolerance refers to the allowable amount of variation in password input, while image choice refers to the type of images used for creating passwords. The paper systematically studies how different tolerance settings and image categories impact the security and usability of graphical passwords, providing valuable insights into these aspects.
* **Empirical study:** The paper presents the results of an empirical study conducted by the authors, where participants were recruited to create, recall, and recognize graphical passwords. The study involved a variety of images and tolerance settings, and the data collected from the study provides empirical evidence on the effectiveness of graphical passwords in different scenarios.
* **Analysis of errors:** The paper analyzes the types of errors made by participants during password recall and recognition tasks, which adds to the understanding of the usability challenges of graphical passwords. The authors identify common errors, such as small variations in input, and discuss the implications of these errors for the design of graphical password systems.
* **Trade-offs between security and usability:** The paper discusses the trade-offs between security and usability in graphical password systems, which is a unique aspect of this research. The authors highlight the challenges of balancing the need for strong security with the desire for passwords that are easy to remember and use. This provides valuable insights for designing graphical password systems that strike the right balance between security and usability.
* **Image categorization:** The paper categorizes images used in the study into different categories, including animals, objects, scenes, and abstract images. This categorization allows for a comparison of the effectiveness of different types of images in graphical password systems, providing unique insights into the impact of image choice on password security and usability.
* **Contribution to usable privacy and security:** The paper is published in the Proceedings of the 2005 symposium on Usable Privacy and Security, highlighting its contribution to the field of usable privacy and security. The paper provides insights into the usability and security aspects of graphical passwords, which can inform the design of more effective authentication methods that are user-friendly and secure.

### Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." In 21st Annual Computer Security Applications Conference (ACSAC'05), pp. 10-pp. IEEE, 2005.

The paper "Graphical Passwords: A Survey" provides a comprehensive overview of graphical password techniques and their applications in computer security. The authors, Suo, Zhu, and Owen, conduct a thorough survey of the existing literature on graphical passwords and summarize the key findings and developments in the field. The paper begins by introducing the concept of graphical passwords and their advantages over traditional text-based passwords, such as improved usability and resistance to dictionary attacks. It then categorizes graphical password techniques into four main types: Recognition-based, Recall-based, Cued-recall, and Hybrid schemes, and provides detailed explanations of each type along with examples of commonly used techniques.

The authors further analyze the security aspects of graphical passwords, including the strength of passwords, resistance to attacks, and potential vulnerabilities. They discuss various types of attacks, such as shoulder surfing, brute force attacks, and smudge attacks, and their potential impact on the security of graphical passwords. The paper also highlights the challenges and limitations associated with graphical passwords, such as the potential for users to forget their chosen images or patterns, the need for user training, and the potential for password reuse. In addition to security considerations, the authors also evaluate graphical password techniques based on usability factors, such as memorability, user preference, and ease of use. They discuss the results of various user studies conducted to assess the usability of graphical passwords and identify factors that may affect user behavior, such as image complexity, password length, and the use of cues. The paper also provides insights into the potential use of graphical passwords in different application domains, such as mobile devices, ATM machines, and web-based systems, and discusses the advantages and limitations of graphical passwords in these contexts.

Furthermore, the authors highlight the potential for combining graphical passwords with other authentication mechanisms, such as biometrics and multi-factor authentication, to enhance their security. They discuss the concept of "cognitive passwords," which involve using personal knowledge or memories as a basis for authentication, and explore the potential of integrating cognitive passwords with graphical passwords for increased security. The paper concludes with a discussion of the future directions of graphical password research, including the need for further investigations into the usability, security, and practical implementation of graphical password techniques. The authors emphasize the importance of considering user perspectives and preferences in the design and evaluation of graphical password systems, and highlight the potential for innovation and advancement in the field through the use of emerging technologies, such as machine learning and image recognition.

Below are some of the features of this research work:

* **Comprehensive overview:** The paper provides a comprehensive overview of graphical password techniques, covering various types of graphical passwords, their security and usability aspects, potential applications, and future research directions. It offers a holistic view of the field of graphical passwords, consolidating the existing literature and presenting a thorough analysis.
* **Categorization of graphical password techniques:** The authors categorize graphical password techniques into four main types: Recognition-based, Recall-based, Cued-recall, and Hybrid schemes. This categorization provides a systematic framework for understanding different types of graphical passwords, their characteristics, and their potential applications in different contexts.
* **Security and usability considerations:** The paper discusses both the security and usability aspects of graphical passwords. It highlights the potential vulnerabilities and attacks that graphical passwords may be susceptible to, while also considering usability factors such as memorability, user preference, and ease of use. This balanced approach allows for a comprehensive assessment of the strengths and limitations of graphical passwords.
* **Discussion of potential applications:** The authors discuss the potential applications of graphical passwords in different contexts, such as mobile devices, ATM machines, and web-based systems. This provides insights into the practical use of graphical passwords in real-world scenarios and their potential advantages and limitations in different application domains.
* **Exploration of cognitive passwords:** The paper explores the concept of "cognitive passwords," which involve using personal knowledge or memories as a basis for authentication. This innovative approach highlights the potential for combining graphical passwords with other authentication mechanisms to enhance their security, and presents a novel direction for future research in the field.
* **Future research directions:** The paper concludes with a discussion of the future research directions in the field of graphical passwords, including the need for further investigations into usability, security, and practical implementation of graphical password techniques. It also highlights the potential for innovation and advancement in the field using emerging technologies, such as machine learning and image recognition, indicating the authors' forward-thinking approach.

**User-centric perspective:** The paper emphasizes the importance of considering user perspectives and preferences in the design and evaluation of graphical password systems. It highlights the usability aspects of graphical passwords and the need to understand user behavior and preferences to ensure the effectiveness of graphical password systems in practice.

|  |  |  |  |
| --- | --- | --- | --- |
| **S No** | **Title** | **Year** | **Focus** |
| 1 | Comparative analysis of different graphical password techniques for security | 2018 | Comparative analysis of various graphical password systems |
| 2 | Graphical password-based user authentication with free-form doodles | 2015 | Design and evaluation of graphical password systems |
| 3 | Covert attentional shoulder surfing: Human adversaries are more powerful than expected | 2014 | Security and privacy in password authentication systems |
| 4 | Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance | 2014 | Influence of mobile devices on password authentication systems |
| 5 | The doodb graphical password database: Data analysis and benchmark results | 2013 | Data analysis and benchmarking of graphical password systems |
| 6 | Graphical password authentication using persuasive cued click point | 2013 | Design and evaluation of graphical password systems using persuasive cued click point |
| 7 | PassPoints: Design and Longitudinal Evaluation of a Graphical Password System | 2013 | Design and evaluation of graphical password system |
| 8 | Multi-touch passwords for mobile device access | 2012 | Design and implementation of multi-touch password systems |
| 9 | Smudge attacks on smartphone touch screens | 2010 | Security vulnerabilities of smartphone touch screens |
| 10 | S3pas: A scalable shoulder-surﬁng resistant textual-graphical password authentication scheme | 2007 | Design and evaluation of shoulder-surfing resistant password systems |
| 11 | Authentication using graphical passwords: Effects of tolerance and image choice | 2005 | Design and evaluation of graphical password systems |
| 12 | Graphical passwords: A survey | 2005 | A survey of graphical password systems |

Table 2.1: Literature Survey - Analysis

## EXISTING SYSTEMS

There are several existing graphical password authentication systems that are in use. Here are some of the most used ones:

### HYBRID COLOR SHUFFLING

The authentication of user identity is an essential requirement for many applications and services. Traditionally, alphanumeric passwords have been the primary means of authentication. However, these passwords are susceptible to attacks such as brute-force and dictionary attacks. To address these vulnerabilities, many graphical authentication systems have been proposed. One such system is a concentric circle graphical authentication system that utilizes three concentric circles, each separated into eight segments. The outermost circle contains numbers, the middle circle contains colors, and the innermost circle contains random strings of length eight. The system consists of two steps to verify the user's identity. The first step involves assigning a unique number to a color of the user's choice during the registration process. The user selects a color and assigns a number to it. This number will later be used to verify the user's identity. This step provides an additional layer of security since the number assigned to a color is unique to each user and cannot be easily guessed or hacked. The second step is the actual authentication process. To authenticate, the user must rotate the circles to create a combination where the assigned number matches the corresponding color on the middle circle, and then select a random string that contains most of the characters of the password entered during registration. The user has to match the assigned number to the correct color on the middle circle. Once the user has matched the color and number, they need to select the random string that contains most of the characters of the password entered during registration. If both combinations are correct, the user is successfully authenticated. This authentication process provides an additional layer of security over traditional text-based passwords. The concentric circle graphical authentication system is more difficult to hack, and the combination of matching the color and number with the random string of characters makes it almost impossible for an unauthorized user to gain access.

Furthermore, this graphical authentication system is also user-friendly. The concentric circles provide an intuitive interface that is easy to use and understand. The use of colors and numbers also makes it easy for users to remember their assigned combination. In conclusion, the concentric circle graphical authentication system provides an additional layer of security over traditional text-based passwords. The two-step authentication process, which involves matching a unique number with a color on the middle circle and selecting a random string of characters, makes it difficult for unauthorized users to gain access. Additionally, the system is user-friendly and easy to use, making it a suitable alternative to traditional alphanumeric passwords. Overall, this graphical authentication system has the potential to enhance the security of various applications and services that require user authentication.

### HUEBOX SCHEME

The Hybrid Color Shuffling technique, which adds an improvement to the basic Color Shuffling technique by incorporating a user's rank and text in their password. The Hybrid Color Shuffling technique requires users to enter a username and password during registration. The password is composed of text, rank, and color, making it more secure than previous techniques. The use of color and rank adds an additional layer of security, and the combination of text, rank, and color makes it more challenging to crack the password.

In addition to their login credentials, users are also required to provide a valid email address during registration in case they forget their password. This feature ensures that users can reset their password securely and regain access to their account. During the login process, the system displays a tabular representation consisting of numbers, colors, and randomly placed characters. The numbers are static, while the other two rows are shiftable using buttons. This graphical representation provides an intuitive interface that is easy to use and understand. To authenticate, users must first align the color of their choice under their specified rank using the color left and right shift buttons and then confirm it. The user selects the rank and then shifts the color row to match the assigned color to their selected rank. This step adds an additional layer of security since the assigned color is unique to each user. Next, users must align each character of their password under their specified text using the text left and right shift buttons and confirm each character individually. This step ensures that the password is entered correctly, and it is difficult for unauthorized users to gain access to the account.

Finally, users click the login button, which generates a password for the session. This password is valid for that session only, and the system generates a new password for each session. This feature adds an additional layer of security since the password cannot be reused, making it challenging for an unauthorized user to access the account. If a user forgets their password, it will be sent to their registered email address. This feature ensures that users can reset their password securely and regain access to their account. The use of a valid email address for password recovery is a standard practice in most authentication systems and provides an additional layer of security.

The Hybrid Color Shuffling technique is a graphical authentication system that adds an additional layer of security over traditional alphanumeric passwords. The use of a combination of text, rank, and color makes it more challenging for unauthorized users to gain access to the account. The system's use of a tabular representation and shift buttons provides an intuitive interface that is easy to use and understand. The system also generates a new password for each session, making it challenging for unauthorized users to gain access to the account. Additionally, the system uses a valid email address for password recovery, ensuring that users can reset their password securely and regain access to their account. Overall, the Hybrid Color Shuffling technique has the potential to enhance the security of various applications and services that require user authentication.

**Advantages:**

* Enhanced Security: The Hybrid Color Shuffling technique is more secure than traditional alphanumeric passwords, as it uses a combination of text, rank, and color to create a password, making it challenging for unauthorized users to gain access to the account.
* Intuitive Interface: The system's use of a tabular representation and shift buttons provides an intuitive interface that is easy to use and understand, even for non-technical users.
* Session-based Passwords: The system generates a new password for each session, making it challenging for unauthorized users to gain access to the account, even if they manage to intercept the user's password.
* Password Recovery: The system uses a valid email address for password recovery, ensuring that users can reset their password securely and regain access to their account.
* Customizable: The system allows users to assign a unique color to their selected rank, adding an additional layer of security, as the assigned color is unique to each user.

**Disadvantages:**

* Limited Password Strength: The use of only text, rank, and color to create a password may limit the password strength compared to alphanumeric passwords. However, the addition of a color and rank makes the password more secure than traditional text-based passwords.
* Password Recovery: While the system's use of a valid email address for password recovery is an advantage, it also introduces a potential vulnerability if the user's email account is compromised.
* Limited Character Set: The system's use of a limited character set may make it easier for attackers to crack the password using brute-force or dictionary attacks.
* Not Suitable for all Users: Some users may find it challenging to remember their selected rank and assigned color, making it difficult for them to use the system effectively.
* Vulnerable to Shoulder Surfing: As the system relies on aligning the color, rank, and text using the shift buttons, it may be vulnerable to shoulder surfing attacks where an attacker can observe the user's actions and gain access to their account.

### COLOR-CODE COMBINATION SYSTEM

The hybrid user authentication technique is a novel approach that combines text and colors to enhance security, usability, and stability in authentication systems. The use of text and colors in combination makes it challenging for attackers to crack the user's password and gain unauthorized access to the system. This system presents a detailed analysis of the proposed technique, including its implementation, advantages, and limitations. The hybrid user authentication technique consists of two primary steps: registration and authentication. During the registration process, the user selects three different colors and rates them individually from 0 to 9, with 0 being the least preferred and 9 being the most preferred. The color-coded combination is kept in the database as the user's password. This step ensures that the password is unique and difficult to guess, as it is based on the user's personal preference of colors.

During the authentication process, the system displays the three colors randomly and asks the user to rate them correctly. The user rates the colors based on their preference, and the system calculates the distance between the user's rating and the registered rating of the color. If the distance is less than a predefined threshold value, the user is successfully authenticated. Otherwise, the authentication process fails, and the user is prompted to try again. The hybrid user authentication technique has several advantages over traditional authentication methods. Firstly, it is more secure than traditional alphanumeric passwords, as it is based on a combination of text and colors. The use of colors makes it difficult for attackers to guess the password, as the password is unique to each user and based on their personal preference of colors. Secondly, it is more usable than traditional passwords, as users find it easier to remember colors than alphanumeric passwords. This makes the authentication process more user-friendly and reduces the chances of users forgetting their passwords. Thirdly, the hybrid user authentication technique is more stable than traditional authentication methods, as it is less vulnerable to attacks such as dictionary attacks. Dictionary attacks involve guessing passwords using a list of common words and phrases, which is not effective against the hybrid user authentication technique, as the password is based on a unique combination of colors and ratings.

The hybrid user authentication technique also has some limitations that need to be addressed. Firstly, the system requires users to remember their preferred colors and ratings, which may be difficult for some users. Secondly, the system may be vulnerable to attacks such as brute-force attacks, where an attacker tries to guess the password by trying all possible combinations of colors and ratings. To mitigate this, the system can use a CAPTCHA system to prevent automated brute-force attacks.

Another limitation of the hybrid user authentication technique is that it may be vulnerable to shoulder surfing attacks, where an attacker can observe the user's actions and determine the preferred colors and ratings. To mitigate this, the system can use a one-time password or a two-factor authentication system to enhance security. In conclusion, the proposed hybrid user authentication technique is a novel approach that combines text and colors to improve security, usability, and stability in authentication systems. The use of colors makes it challenging for attackers to crack the user's password, and the system is more user-friendly and less vulnerable to attacks such as dictionary attacks. However, the system has some limitations, such as the need for users to remember their preferred colors and ratings, and vulnerability to shoulder surfing attacks. These limitations can be mitigated by implementing additional security measures such as CAPTCHA systems and two-factor authentication. Overall, the hybrid user authentication technique shows promise as a secure, usable, and stable authentication method that can be used in a variety of applications.

**Advantages:**

* Improved security: The hybrid user authentication technique that combines text and colors makes it difficult for attackers to guess or crack the user's password.
* Improved usability: The user only needs to remember three colors and their ratings, making it easier to use and remember compared to traditional text-based passwords.
* Increased stability: Since the color-coded combination is kept in the database as the user's password, there is less likelihood of the password being lost or forgotten, and there is no need for frequent password resets.
* Random color combinations: The system displays different color combinations each time the user logs in, making it harder for attackers to guess or crack the user's password.
* Scalability: The hybrid user authentication technique can be easily scaled up to accommodate more users and different applications.

**Disadvantages:**

* Limited number of colors: The user is only allowed to select three different colors, which limits the number of possible combinations and may make it easier for attackers to guess or crack the password.
* Security vulnerabilities: The system may still be vulnerable to attacks such as phishing, social engineering, and malware that can compromise the user's password and compromise security.
* Usability challenges for colorblind users: Users who are colorblind may have difficulty using this authentication technique, which may impact usability.
* Technical issues: There may be technical issues related to the implementation and maintenance of the system, such as system crashes, database failures, and software bugs.
* Dependence on user ratings: The user's ratings of the three selected colors may be subjective and could impact the security of the system if the user's ratings are not accurate.

### OTHER EXISTING SYSTEMS

Apart from the above existing systems, the below mentioned are some of the systems that are currently under development.

1. **PassFaces:** PassFaces is a graphical password authentication system that uses a set of facial images to create a password. Users select a set of faces from a larger set, and the system uses the order in which the faces were selected as the password. PassFaces is designed to be resistant to both shoulder surfing and brute force attacks.
2. **DAS:** DAS (Draw-a-Secret) is a graphical password authentication system that requires users to draw a specific shape or pattern as their password. DAS is designed to be resistant to shoulder surfing attacks, as it is difficult for an attacker to reproduce the exact shape or pattern that was drawn.
3. **Story-Based Authentication:** Story-based authentication is a graphical password authentication system that requires users to create a story or scenario using a set of images. Users select a set of images from a larger set and then create a story that incorporates those images. The system uses the story as the password. Story-based authentication is designed to be resistant to shoulder surfing attacks, as it is difficult for an attacker to reproduce the exact story that was created.
4. **PassPoints:** PassPoints is a graphical password authentication system that requires users to select a set of points on a grid as their password. Users select a set of points from a larger grid, and the system uses the order in which the points were selected as the password. PassPoints is designed to be resistant to both shoulder surfing and brute force attacks.
5. **Cued Click-Points:** Cued Click-Points is a graphical password authentication system that requires users to select a set of points on a set of images as their password. Users select a set of images from a larger set, and then select a set of points on each image. The system uses the order in which the images were selected and the points that were selected as the password. Cued Click-Points is designed to be resistant to both shoulder surfing and brute force attacks.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S No** | **Existing System** | **Important Features** | **Advantages** | **Disadvantages** |
| 1 | Hybrid Color Shuffling | Uses a combination of image and color-based authentication | Provides an extra layer of security against visual hacking | Difficult to remember the correct sequence of images and colors |
| 2 | Huebox Scheme | Uses a combination of color and pattern recognition | Provides high security and resistance to shoulder surfing attacks | Can be difficult to remember the correct sequence of colors and patterns |
| 3 | Color-Code Combination System | Uses a combination of colors and numbers | Easy to remember and use | Vulnerable to shoulder surfing attacks |
| 4 | PassFaces | Uses facial recognition technology | Provides high security and is easy to use | Requires specialized hardware and software, and may not work well in low light conditions |
| 5 | DAS | Uses mouse movements to create a unique signature | Provides an extra layer of security and is easy to use | Vulnerable to replay attacks |
| 6 | Story Based Authentication | Uses a user-generated story to authenticate | Provides high security and is easy to remember | Difficult to create a story that is both memorable and secure |
| 7 | PassPoints | Uses a combination of clicks on an image grid | Delivers a strong level of protection and is easy to operate. | Vulnerable to shoulder surfing attacks |
| 8 | Cued Click-Points | Uses a combination of clicks on an image grid with cues | Delivers robust security while maintaining user-friendliness | Vulnerable to shoulder surfing attacks and can be difficult to remember the correct sequence of clicks and cues |

Table 2.2: Existing Systems - Analysis

**CHAPTER 3**

# REQUIREMENT ANALYSIS



## STAKEHOLDERS

This project is intended for the users:

* **Corporate Employees:** One of the primary targeted users of this project is corporate employees who need to frequently log into their work systems and applications. The proposed authentication system aims to make their login process more secure and convenient.
* **Online Shoppers:** Another targeted user group for this project is online shoppers. With the increasing popularity of e-commerce, online shoppers are at risk of cyber-attacks and frauds. This authentication system can provide an additional layer of security to their online shopping experience.
* **Social Media Users:** Social media platforms are also popular targets for cyber-attacks, and their users are at risk of data breaches and identity theft. This authentication system can help social media users to secure their accounts and personal information.
* **Banking And Financial Service Customers:** Banking and financial services are critical industries where security is of utmost importance. This authentication system can be used by their customers to make their transactions more secure.
* **Government Employees:** Government organizations are also vulnerable to cyber-attacks, and their employees need to access secure systems and applications. This authentication system can help to strengthen their security measures and protect sensitive information.
* **Healthcare Professionals:** The healthcare industry is also a high-risk sector, where sensitive patient data needs to be protected. This authentication system can help to ensure the confidentiality of medical records and personal health information.

## REQUIREMENT GATHERING

Requirement gathering is a crucial step in the software development life cycle (SDLC) that involves collecting, analyzing, and documenting the needs and expectations of stakeholders for a particular project. The effectiveness of the software development process depends on the quality of the requirements gathered at the initial stage. There are several requirement gathering methods available, each with its advantages and disadvantages.

* **Questionnaires:** Questionnaires are a structured and standardized set of questions that can be used to gather requirements from a large group of stakeholders. The primary advantage of this method is that it is cost-effective and can be administered remotely, allowing the interviewer to reach a broad audience. The disadvantage of this method is that the responses obtained may lack context, and stakeholders may not take the time to provide detailed answers.
* **Workshops:** Workshops involve bringing together stakeholders from different areas of the organization to discuss and brainstorm ideas for the project. The primary advantage of this method is that it promotes collaboration and generates a broad range of ideas from different perspectives. The disadvantage of this method is that it can be time-consuming, and some stakeholders may dominate the conversation, leading to a bias towards their interests.
* **Observation:** Observation involves the gathering of requirements by directly observing the activities of stakeholders in their natural environment. The primary advantage of this method is that it provides a deep understanding of the stakeholders' needs and expectations. The disadvantage of this method is that it can be time-consuming and may not be possible for all stakeholders, especially those who work remotely.
* **Focus Groups:** Focus groups involve bringing together a small group of stakeholders to discuss their needs and expectations for the project. The primary advantage of this method is that it promotes collaboration and generates a broad range of ideas from different perspectives. The disadvantage of this method is that some stakeholders may dominate the conversation, leading to a bias towards their interests, and the results may not be representative of the larger stakeholder group.
* **Prototyping:** Prototyping involves creating a basic version of the product or service to gather feedback from stakeholders. The primary advantage of this method is that it provides stakeholders with a tangible representation of the product, enabling them to provide more detailed feedback. The disadvantage of this method is that it can be time-consuming and costly to develop prototypes for each iteration.
* **Interviews:** Interviews are the most common and straightforward method for requirement gathering, involving face-to-face or telephonic conversations with stakeholders. The primary advantage of this method is that it enables the interviewer to ask specific questions and clarify ambiguities in real-time. The disadvantage of this method is that it can be time-consuming, and the responses obtained may not always be accurate or comprehensive.

## REQUIREMENT ANALYSIS

In the above methods, we used Questionnaires as our method to collect requirements from our stakeholders. From the variety of the responses that we received we chose the ones that were most needed by the user and held the most merit. The same are listed below:

* The graphical password authentication system should offer a high level of security to prevent any unauthorized access
* The system should be user-friendly and easy to use for individuals with varying levels of technical expertise
* The system should allow for secure access to electronic health records through a graphical password authentication
* The system should include measures to prevent shoulder surfing attacks and unauthorized access to sensitive information
* Quick and easy password reset options
* Robust encryption and secure storage of login credentials
* Multiple authentication methods for enhanced security
* Easy to remember passwords
* Quick and seamless authentication process
* Able to easily integrate with multiple vendor applications

### HARDWARE REQUIREMENTS

|  |  |  |
| --- | --- | --- |
| **S. No** | **Hardware** | **Specification** |
| 1 | Processor | Intel i3 10th Gen |
| 2 | Speed | 2.4 Ghz |
| 3 | RAM | 2 GB (min) |
| 4 | Hard Disk | 1 GB |

Table 4.1: Hardware Requirements

### SOFTWARE REQUIREMENTS

|  |  |  |
| --- | --- | --- |
| **S. No** | **Software** | **Specification** |
| 1 | Operating System | Windows 10/11 |
| 2 | Application Server | Tomcat 8.5 |
| 3 | Front - End | Java 1.8 |
| 4 | Back – End | MySQL 10.4 |

Table 4.2: Software Requirements

## PROBLEM STATEMENT

From the above requirements collected from the user, the problem statement is defined as,

“To develop a Graphical Password Authentication System which enhances security and user experience while reducing the burden of remembering complex text-based passwords. The system must provide a reliable and user-friendly authentication mechanism for various applications and devices.”

**CHAPTER 4**

# DESIGN



## PROPOSED SYSTEM

The Graphical Password Authentication System is an innovative solution designed to tackle the pervasive threat of shoulder surfing attacks, which involve malicious actors observing users as they enter their login credentials. The system employs a unique combination of graphical features to create a robust authentication experience. One key feature is the Password Verification component, which uses hashing algorithms to encrypt user passwords, providing an added layer of security against data breaches and unauthorized access to sensitive data. Another aspect of the system is the Color Matcher, which requires users to select six distinct colors from a varied color palette and match them in the correct sequence during login. By ensuring that each user has a unique set of colors, the system makes it much harder for attackers to guess or steal user passwords. The Pattern Matcher component requires users to draw a custom pattern on a 3x3 grid of dots during registration, which must be replicated correctly during login. This feature provides an additional layer of security, as each user's pattern is complex and hard to guess or replicate. Furthermore, the system is equipped with pre-emptive measures to thwart brute-force attacks by locking out users after a specified number of unsuccessful attempts. This ensures that attackers cannot keep guessing login credentials until they get it right, as the system will lock them out after a certain number of tries. Overall, the Graphical Password Authentication System is a powerful tool for individuals seeking maximum online security and protection of their sensitive data from malicious entities. It combines multiple graphical features to create a robust and secure authentication experience, providing peace of mind to users that their confidential information is safe from prying eyes.

## SYSTEM ARCHITECTURE

The proposed system has the following components.

* Input Receiver and Validator
* Request Processor
* Sender
* Database
* **­­­** Client Side

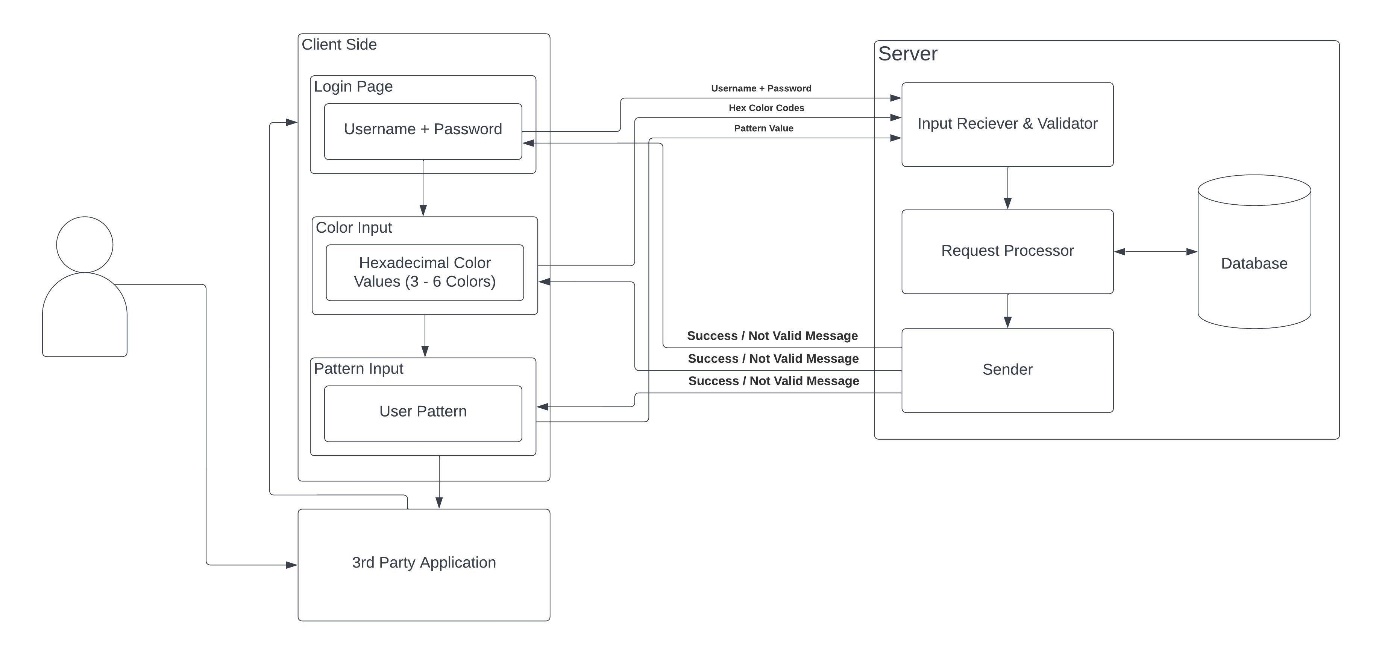


Fig 4.1: System Architecture

* **Input Receiver and Validator:**

It is a software component that receives user input and verifies its validity. It checks the input against predefined criteria or rules, such as length, format, and data type. The input receiver and validator can be part of a larger system, such as a web application or a database management system, and plays a critical role in ensuring data quality and integrity. It helps prevent errors, vulnerabilities, and malicious attacks that may result from incorrect or invalid input.

* **Request Processor:**

It is a component or software module responsible for receiving and handling incoming requests from various sources. It processes and validates the requests, extracts relevant data, and prepares the response for the requester. The request processor can also perform additional tasks such as authentication, authorization, and data encryption. It is an essential part of any system that handles incoming requests, such as web servers, APIs, and application servers. The efficiency and accuracy of the request processor can significantly impact the overall performance and user experience of the system.

* **Sender:**

It is responsible for transmitting the user's login credentials to the authentication server for verification. This component typically works in conjunction with the Input Receiver and Validator, which collect the user's credentials and perform preliminary checks to ensure that the information entered is in the correct format. Once the credentials are validated, the Request Sender sends the information to the authentication server for further verification, after which the user is either granted access or denied entry. The Request Sender plays a crucial role in ensuring that the login process is smooth and seamless, with minimal delays or errors. It must be designed to handle high traffic volumes and function reliably under different network conditions. Additionally, the Request Sender must incorporate appropriate security measures to prevent interception, tampering, or unauthorized access to user data during transmission.

* **Database:**

Database serves as a crucial component that stores user credentials and other sensitive information securely. It is responsible for storing user IDs, passwords, hashed passwords, color and pattern data, and other relevant information. The database is designed to ensure data integrity and prevent unauthorized access, and it must be protected against external threats such as hacking, malware, and other forms of cyberattacks. Additionally, the database must have robust backup and recovery mechanisms to minimize the risk of data loss in the event of system failures or disasters. Proper database management and security are essential to ensure the smooth functioning of the graphical password authentication system and protect user data from potential security breaches.

* **Client Side**

The client-side component captures the user's graphical password input, such as a drawn pattern or selected image, and displays the graphical interface for the user to interact with. To ensure the validity of user input, the component also performs data validation. Additionally, it may store some data locally to enhance the user experience and reduce server load. The client-side component communicates with the server-side to authenticate the user, retrieve user data, or perform other necessary functions. Overall, the client-side component plays a critical role in the graphical password authentication system by facilitating the user's interaction with the system and ensuring the security of the authentication process.

## MODULES

Our proposed system comprises of 3 modules namely:

* Password Verification Modules
* Color Matcher Module
* Pattern Verification Module

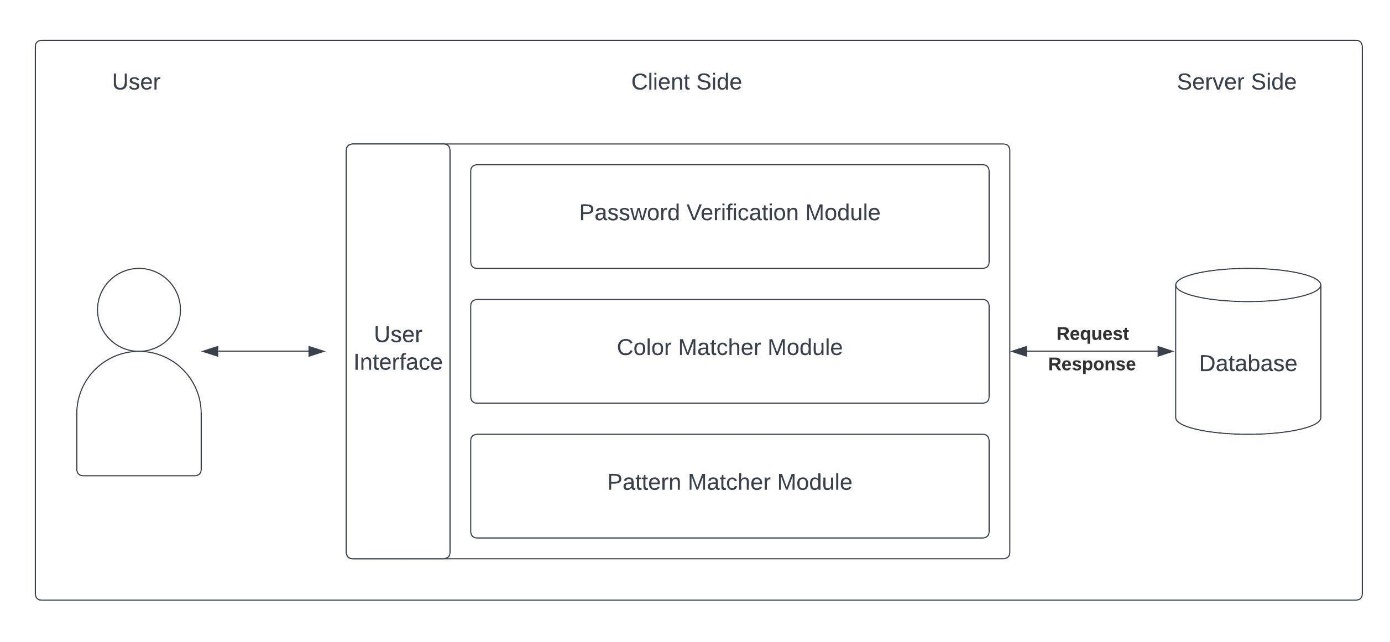


Fig 4.2: Overall Module Diagram

### PASSWORD VERIFICATION MODULE

Password verification is the process of confirming whether a user's password matches the one stored in a database or system. Passwords are used to secure personal information, financial data, and other sensitive data from unauthorized access. The primary purpose of password verification is to ensure that the user attempting to access a system or application is, in fact, who they claim to be. Passwords are a commonly used form of authentication, and password verification is a critical component of security. Password verification typically involves comparing the password entered by the user to a stored hash value of the password. A hash is a mathematical function that converts the password into a unique string of characters, called a hash value. The hash value is then stored in a database or system, instead of the actual password.

When a user enters their password, the system applies the same hash function to the password and compares the resulting hash value to the stored hash value. If the two values match, the system knows that the user has entered the correct password, and access is granted. If the values do not match, access is denied. There are several best practices for password verification that can improve security. One such practice is to use strong passwords. A strong password is one that is difficult to guess or crack using brute force methods. Strong passwords typically include a combination of upper and lowercase letters, numbers, and symbols.

Another best practice is to enforce password complexity requirements. Password complexity requirements can include minimum length requirements, requirements for including a combination of upper and lowercase letters, numbers, and symbols, and requirements for avoiding easily guessable words or phrases. It is also important to limit the number of failed login attempts. This can help prevent brute force attacks, where an attacker tries to guess a user's password by systematically trying many possible passwords. Finally, it is important to store passwords securely. Passwords should be stored using a strong hashing algorithm, and the hash values should be salted. Salting involves adding a random string of characters to the password before it is hashed, which makes it more difficult for attackers to crack the password using precomputed hash tables.

The password verification module is a critical component of any authentication system. Its main function is to ensure that only authorized users are granted access to the system by verifying the user's password. The module typically consists of two main components:

* Password hashing
* Password comparison

In this module, we have used the BCrypt Hashing function to hash the user’s password in the database. This helps to protect the user's password from being compromised in the event of a security breach. Password comparison, on the other hand, involves comparing the hashed password stored in the system's database with the hashed version of the password entered by the user. If the two hashes match, the user moves to the next layer which is the Color Matcher Module. Otherwise, access is denied.

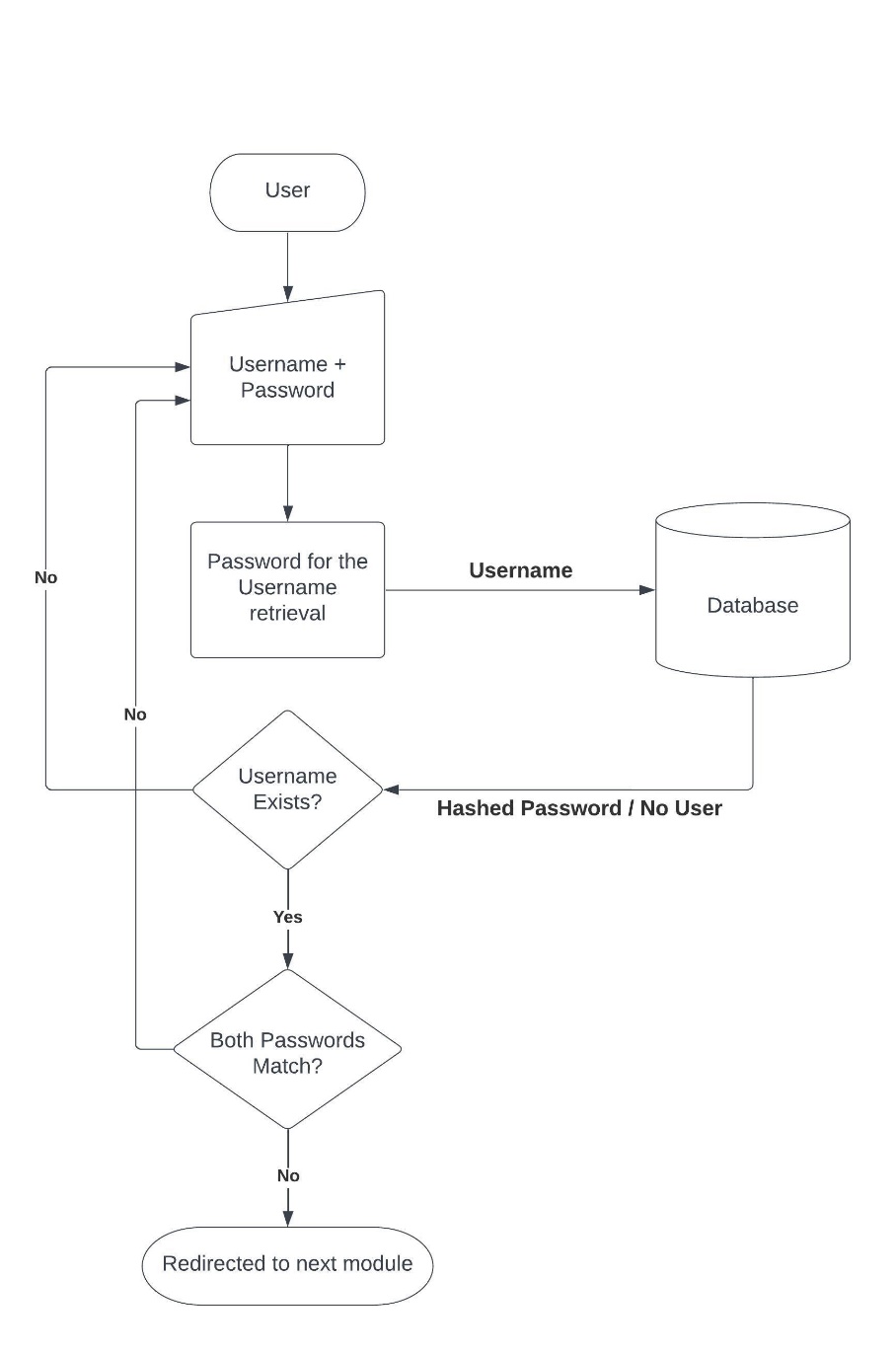


Fig 4.3: Password Verification Module

### COLOR MATCHER MODULE

The color matcher module is a unique and innovative component of the authentication system used in this project. Unlike traditional authentication methods, such as passwords or PINs, which are often forgotten, easily guessed or cracked, the color matcher module offers a highly secure and memorable way for users to authenticate their identity. During registration, users are prompted to select six different colors from a color palette provided by the system. These colors are then stored in the system's database as the user's authentication credentials. The color palette is carefully selected to ensure that the colors are distinguishable from each other and provide a wide range of color options to suit different preferences.

To authenticate, the user is prompted to select the same six colors in the correct order as the ones they selected during registration. The order of the colors is an important component of the authentication process, as it adds an extra layer of security by making it difficult for attackers to replicate the exact sequence of colors required to gain access to the system. Each user has a unique set of colors, which makes it highly unlikely that an unauthorized user will be able to guess or replicate the correct sequence. Additionally, since the colors are selected by the user themselves, it becomes easier for the users to remember their authentication credentials, making the authentication process more efficient. This is particularly beneficial for users who struggle with remembering complex passwords or PINs. As a result, the color matcher module offers a user-friendly and accessible approach to authentication, which can be especially important for individuals who may have disabilities or other challenges that make traditional authentication methods difficult.

The color matcher module also offers a high degree of flexibility in terms of user customization. During registration, users can choose from a range of color palettes, including ones that are specifically designed to be accessible for individuals with visual impairments. This ensures that users have the ability to choose colors that they are comfortable with and that meet their individual needs.

In addition to providing a user-friendly and secure authentication method, the color matcher module also offers several other benefits. For example, it can be easily integrated with other security features, such as two-factor authentication or biometric authentication, to provide an additional layer of security. The module can also be customized to meet the specific needs of different organizations or industries, such as banking or healthcare, where security is of utmost importance.

However, like any authentication method, the color matcher module is not fool-proof and may be vulnerable to certain types of attacks. For example, attackers could potentially use social engineering techniques to trick users into revealing their color sequence or could use sophisticated hacking techniques to gain access to the system's database. As a result, it is important for organizations to implement appropriate security measures, such as regular system updates, strong encryption protocols, and user education programs, to minimize the risk of a security breach.

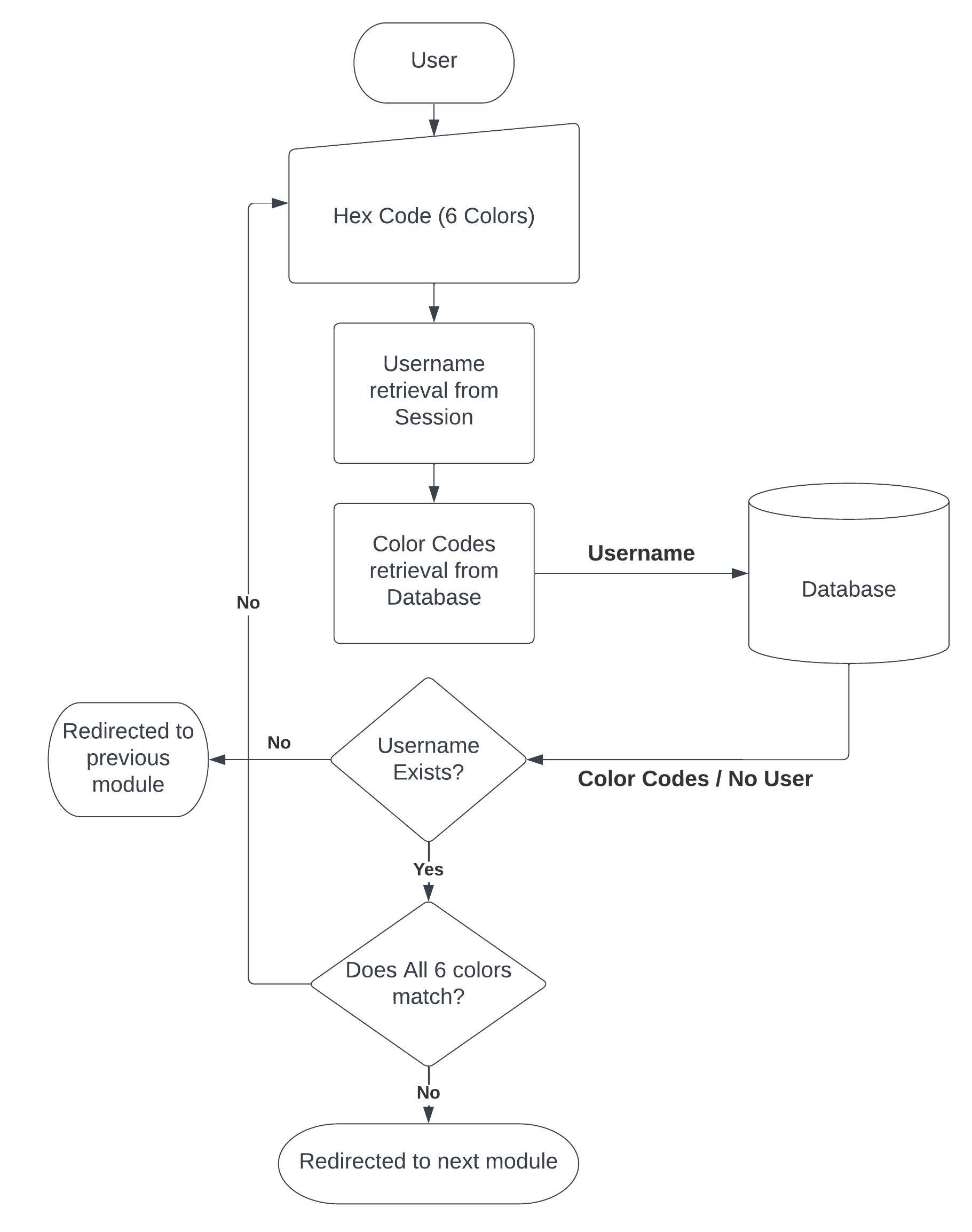
****

Fig 4.4: Color Matcher Module

### PATTERN MATCHER MODULE

The pattern matcher module is the last component of this project. The pattern authentication module is a novel approach to authentication that utilizes a sequence of dots arranged in a 3 x 3 grid as the user's authentication credentials. This authentication method is becoming increasingly popular as it provides a high degree of security and is more user-friendly than traditional authentication methods such as passwords. During the registration process, the user is prompted to draw a pattern by connecting dots in the 3 x 3 grid. The user is free to choose any combination of dots in the grid to create their unique pattern. This pattern is then stored in the system's database as the user's authentication credentials. To authenticate, the user is prompted to draw the same pattern in the correct order as the one they drew during registration. The order of the dots in the pattern is an important component of the authentication process, as it adds an extra layer of security by making it difficult for attackers to replicate the exact sequence of dots required to gain access to the system. One of the major advantages of the pattern authentication method is its simplicity. Users do not have to remember complex passwords, making the authentication process more efficient and less prone to errors. Furthermore, users are more likely to remember their unique pattern, which reduces the likelihood of them forgetting their authentication credentials and having to reset their password. Another advantage of the pattern authentication method is its high degree of security. Each user has a unique pattern, and it becomes highly unlikely that an unauthorized user will be able to replicate the exact sequence of dots required to gain access to the system. Attackers attempting to brute-force their way into the system will have to try numerous combinations of dots, making the process highly time-consuming and inefficient.

The pattern authentication module also includes measures to prevent brute-force attacks. For instance, the module can be configured to set limits on the number of failed attempts before locking the user out of the system. This reduces the likelihood of attackers gaining access to the system through brute-force attacks. Furthermore, the module can be configured to require users to draw their pattern within a specific time frame. This prevents attackers from using automated tools to repeatedly try various combinations of dots until they find the correct pattern. By requiring users to draw their pattern within a specific time frame, the module ensures that the user is an actual human being and not an automated tool attempting to gain access to the system. Despite its many advantages, the pattern authentication method also has some limitations. One of the main limitations is the lack of randomness in the pattern creation process. Users tend to create patterns that are easily recognizable and memorable, making them more susceptible to attacks such as shoulder surfing. Shoulder surfing is a type of attack where an attacker observes the user's pattern while they are authenticating. This attack is particularly effective if the user is authenticating in a public place, such as a café or airport. Attackers can observe the user's pattern from a distance, making it easier for them to replicate the exact sequence of dots required to gain access to the system.

To mitigate the risk of shoulder surfing attacks, the pattern authentication module can be configured to require users to draw their pattern in a specific order. This makes it difficult for attackers to replicate the user's pattern even if they observe the pattern creation process.

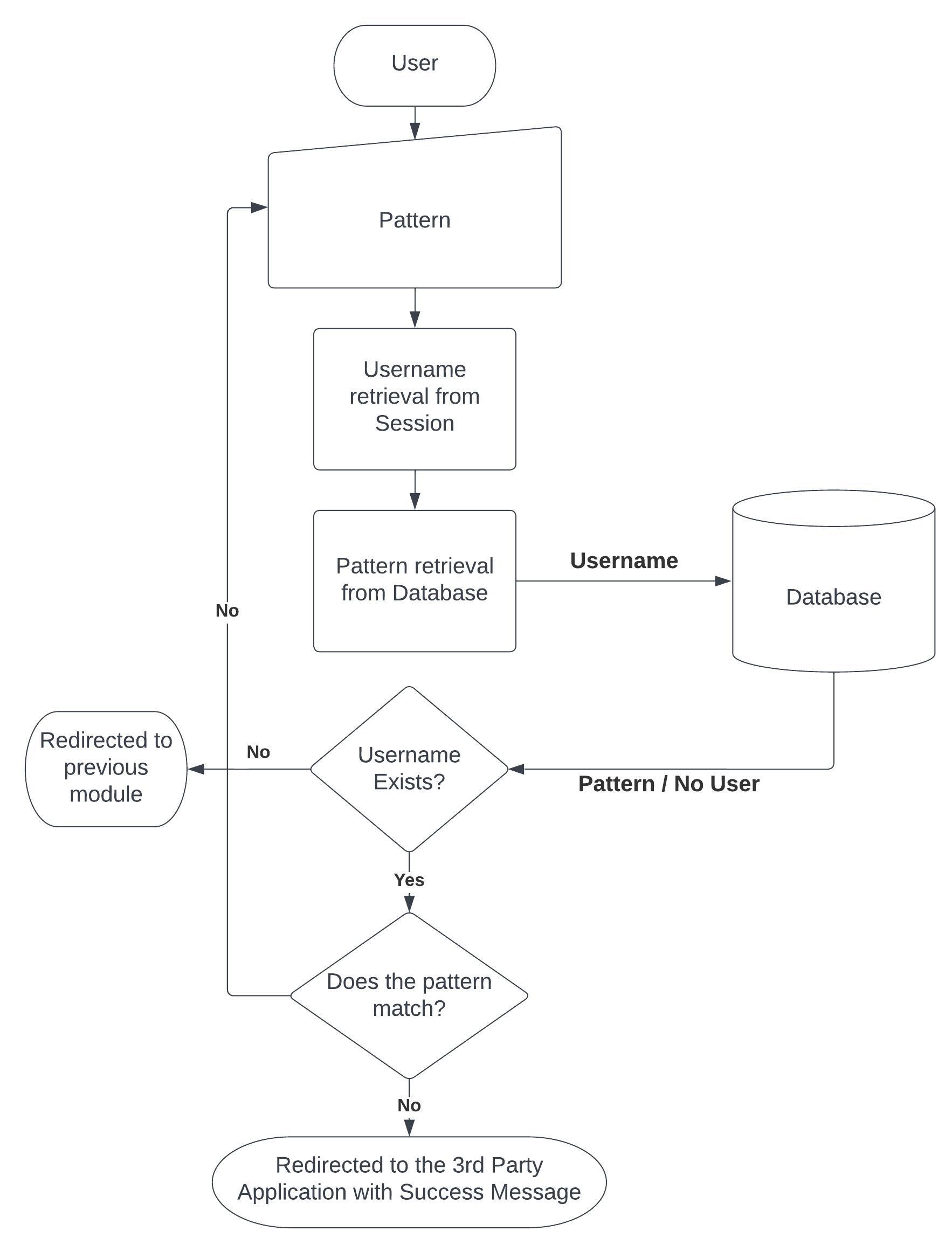


Fig 4.5: Pattern Verification Module

## SOFTWARE ENVIRONMENT

### JAVA

Java is a high-level programming language originally developed by Sun Microsystems and released in 1995. Java runs on a variety of platforms, such as Windows, Mac OS, and the various versions of UNIX.

One design goal of Java is portability, which means that programs written for the Java platform must run similarly on any combination of hardware and operating system with adequate runtime support. This is achieved by compiling the Java language code to an intermediate representation called Java bytecode, instead of directly to architecture-specific machine code.

Java is −

* **Object Oriented** − In Java, everything is an Object. Java can be easily extended since it is based on the Object model.
* **Platform Independent** − Unlike many other programming languages including C and C++, when Java is compiled, it is not compiled into platform specific machine, rather into platform independent byte code. This byte code is distributed over the web and interpreted by the Virtual Machine (JVM) on whichever platform it is being run on.
* **Simple** − Java is designed to be easy to learn. If you understand the basic concept of OOP Java, it would be easy to master.
* **Secure −** With Java's secure feature it enables to develop virus-free, tamper-free systems. Authentication techniques are based on public-key encryption.
* **Architecture-neutral −** Java compiler generates an architecture-neutral object file format, which makes the compiled code executable on many processors, with the presence of Java runtime system.
* **Portable −** Being architecture-neutral and having no implementation dependent aspects of the specification makes Java portable. Compiler in Java is written in ANSI C with a clean portability boundary, which is a POSIX subset.
* **Robust −** Java tries to eliminate error prone situations by emphasizing mainly on compile time error checking and runtime checking.
* **Multithreaded −** With Java's multithreaded feature it is possible to write programs that can perform many tasks simultaneously. This design feature allows the developers to construct interactive applications that can run smoothly.
* **Interpreted −** Java byte code is translated on the fly to native machine instructions and is not stored anywhere. The development process is more rapid and analytical since the linking is an incremental and light-weight process.
* **High Performance −** With the use of Just-In-Time compilers, Java enables high performance.
* **Distributed −** Java is designed for the distributed environment of the internet.
* **Dynamic −** Java is more dynamic than C or C++ since it is designed to adapt to an evolving environment. Java programs can carry extensive amount of run-time information that can be used to verify and resolve accesses to objects on run-time.

### INTEGRATED DEVELOPMENT ENVIRONMENT (IDE)

NetBeans is a Java-based integrated development environment (IDE). The term also refers to the IDE’s underlying application platform framework. The IDE is designed to limit coding errors and facilitate error correction with tools such as the NetBeans Find Bugs to locate and fix common Java coding problems and Debugger to manage complex code with field watches, breakpoints, and execution monitoring. Although the NetBeans IDE is designed specifically for Java developers, it also supports C/C++, PHP, Groovy, and HTML5 in addition to Java, JavaScript, and JavaFX.

Tools and capabilities of the NetBeans IDE include a feature-rich text editor with refactoring tools and code templates, high level and granular views of applications, a drag and drop GUI design, and versioning using out-of-the-box integration with tools such as Git. The NetBeans IDE can run on any operating system that supports a compatible JVM including Linux, Windows and OS X. The underlying NetBeans platform supports creation of new applications and further development of existing applications using modular software components.

As an application running on the NetBeans Platform, the NetBeans IDE itself is extensible and can be extended to support new languages. The IDE and Platform were converted to open source by Sun Microsystems in 2000. Oracle continues to sponsor the NetBeans project since acquiring Sun in 2010

Features of NetBeans can be mentioned as follows

* Fast & Smart Code Editing
* Easy & Efficient Project Management
* Rapid User Interface Development
* Write Bug Free Code
* Support for Multiple Languages
* Cross Platform Support
* Rich Set of Community Provided Plugins

### APACHE TOMCAT

Apache Tomcat, often referred to as Tomcat, is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF). Tomcat implements several Java EE specifications including Java Servlet, Java Server Pages (JSP), Java EL, and WebSocket, and provides a "pure Java" HTTP web server environment in which Java code can run.

Tomcat is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation, released under the Apache License 2.0 license, and is open-source software.

* **COMPONENTS**

Tomcat 4.x was released with Catalina (a servlet container), Coyote (an HTTP connector) and Jasper (a JSP engine).

* ***Catalina:*** Catalina is Tomcat's servlet container. Catalina implements Sun Microsystems's specifications for servlet and Java Server Pages (JSP). In Tomcat, a Realm element represents a "database" of usernames, passwords, and roles assigned to those users. Different implementations of Realm allow Catalina to be integrated into environments where such authentication information is already being created and maintained, and then use that information to implement Container Managed Security as described in the Servlet Specification.
* ***Coyote:*** Coyote is a Connector component for Tomcat that supports the HTTP 1.1 protocol as a web server. This allows Catalina, nominally a Java Servlet or JSP container, to also act as a plain web server that serves local files as HTTP documents.
* ***Jasper:*** Jasper is Tomcat's JSP Engine. Jasper parses JSP files to compile them into Java code as servlets. At runtime, Jasper detects changes to JSP files and recompiles them. Three new components were added with the release of Tomcat 7:
* ***Cluster:*** This component has been added to manage large applications. It is used for load balancing that can be achieved through many techniques. Clustering support currently requires the JDK version 1.5 or later.
* ***High availability:*** A high-availability feature has been added to facilitate the scheduling of system upgrades without affecting the live environment. This is done by dispatching live traffic requests to a temporary server on a different port while the main server is upgraded on the main port. It is very useful in handling user requests on high-traffic web applications.
* ***Web application:*** It has also added user- as well as system-based web applications enhancement to add support for deployment across the variety of environments. It also tries to manage sessions as well as applications across the network.
* **FEATURES**

Tomcat 7.x implements the Servlet 3.0 and JSP 2.2 specifications. It requires Java version 1.6, although previous versions have run on Java 1.1 through 1.5. Versions 5 through 6 saw improvements in garbage collection, JSP parsing, performance and scalability. Native wrappers, known as "Tomcat Native", are available for Microsoft Windows and Unix for platform integration.

Tomcat 8.x implements the Servlet 3.1 and JSP 2.4 Specifications. Apache Tomcat 8.5.x is intended to replace 8.0.x and includes new features pulled forward from Tomcat 9.0.x. The minimum Java version and implemented specification versions remain unchanged.

### MYSQL

MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed, and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons:

* MySQL is released under an open-source license. So, you have nothing to pay to use it.
* MySQL is a very powerful program in its own right. It handles a large subset of the functionality of the most expensive and powerful database packages.
* MySQL uses a standard form of the well-known SQL data language.
* MySQL works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA, etc.
* MySQL works very quickly and works well even with large data sets.
* MySQL is very friendly to PHP, the most appreciated language for web development.
* MySQL supports large databases, up to 50 million rows or more in a table. The default file size limit for a table is 4GB, but you can increase this (if your operating system can handle it) to a theoretical limit of 8 million terabytes (TB).
* MySQL is customizable. The open-source GPL license allows programmers to modify the MySQL software to fit their own specific environments.

**CHAPTER 5**

# IMPLEMENTATION

The implementation of a graphical password authentication system involves designing and building a system that allows users to log in to a computer or using a graphical password. We have this project into 3 unique modules and we built them in a sequential manner. Each module has its own specific functionality and together, they form a complete system for graphical password authentication. In the following sub sections, we will discuss specific details of each module including the algorithms used and its source code.

As the project is an authentication system, the user needs to register and then only can use this system to authenticate themselves. So, the modules are split in a manner that each module has 2 sub modules, namely

* Registration Sub Module
* Login Sub Module

The first module is responsible for registering a new user while the second one is responsible for authenticating existing users.



## PASSWORD VERIFICATION MODULE:



### REGISTRATION SUB MODULE:

1. The user enters their desired username and other details for registration.
2. The details are validated in the front end and the details are sent to server via POST method.
3. The password is hashed using BCrypt hash function.
4. The user's details are saved in the database along with the hashed password.
5. The user is redirected to the next level of registration

**SOURCE CODE:**

<%@page import = "com.oreilly.servlet.\*, java.sql.\*, java.lang.\*, java.text.SimpleDateFormat, java.util.\*, java.io.\*, javax.servlet.\*, javax.servlet.http.\*" %>

<%@ page import="java.sql.\*"%>

<%@ page import="org.mindrot.jbcrypt.\*" %>

<%@ include file="connect.jsp" %>

<%@ page import="java.util.Date" %>

<%

// Receiving the validated user details from the front end

String name = request.getParameter("userid");

String pwd = request.getParameter("pswd");

String mail = request.getParameter("email");

String phn = request.getParameter("mobile");

String address = request.getParameter("address");

String loc = request.getParameter("loc");

String pin = request.getParameter("pin");

String dob = request.getParameter("dob");

String gender = request.getParameter("gender");

try {

// Checking if the Username already exists (User Defined Method)

if(chkUserName(name, connection)) {

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserReg.jsp?fail=uname");

return;

}

// Checking if the Email already exists (User Defined Method)

if(chkEmail(mail, connection)) {

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserReg.jsp?fail=mail");

return;

}

// Checking if the Mobile Number already exists (User Defined Method)

if(chkPhn(phn, connection)) {

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserReg.jsp?fail=phn");

return;

}

// Hashing the password with JBCrypt and storing it in the same variable

String salt = BCrypt.gensalt();

pwd = BCrypt.hashpw(pwd, salt);

// Now registering the user with his credentials

PreparedStatement stmt = connection.prepareStatement("INSERT INTO reg (name, pass, email, mobile, addr, dob, gender, pin, location) VALUES (?, ?, ?, ?, ?, ?, ?, ?, ?)");

stmt.setString(1, name);

stmt.setString(2, pwd);

stmt.setString(3, mail);

stmt.setString(4, phn);

stmt.setString(5, address);

stmt.setString(6, dob);

stmt.setString(7, gender);

stmt.setString(8, pin);

stmt.setString(9, loc);

int rows = stmt.executeUpdate();

// If the number of rows affected by the INSERT statement is greater than zero, then the insert was successful

if (rows > 0) {

application.setAttribute("name", name);

session.setAttribute("name", name);

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/RegColor.jsp");

} else {

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserReg.jsp?fail=u");

}

} catch(Exception e) {

out.print(e);

}

%>

### LOGIN SUB MODULE:

1. The user enters their registered username or mail ID and password for login.
2. The password is retrieved from the database for the entered username.
3. If no user exists with the username, the user is denied access and prompted to enter the correct credentials.
4. If there exists a user, the entered password is hashed using the BCrypt hash function.
5. The hashed password is compared with the hashed password retrieved from the database.
6. If the passwords match, the username is set in the session and the user is redirected to the next level.
7. If the passwords do not match, the user is denied access and prompted to enter the correct credentials.

**SOURCE CODE:**

<%@page import="java.util.\*"%>

<%@ include file="connect.jsp"%>

<%@ page import="org.mindrot.jbcrypt.\*" %>

<%

//Receiving Data from Front End

String name = request.getParameter("username");

String pass = request.getParameter("pswd");

try {

// SQL Query for selecting user's password from the database with his username / Mail ID

String sql = "SELECT \* FROM reg where name='" + name+ "' or email = '"+ name + "'";

Statement stmt = connection.createStatement();

// Executing the query and the result is stored

ResultSet rs = stmt.executeQuery(sql);

// Checking whether there exists any user with the given username or Email ID

if (rs.next()) {

String DBPass = rs.getString(3);

// If there exists a user, the entered password is checked with the hashed password retrieved from the database

if(BCrypt.checkpw(pass, DBPass)) {

// If the passwords match, the username is set in the session variable and is redirected to the next level

String id = rs.getString(1);

name = rs.getString(2);

application.setAttribute("name", name);

application.setAttribute("id", id);

session.setAttribute("name", name);

session.setAttribute("id", id);

response.sendRedirect("LoginColor.jsp");

} else {

// Redirecting the user to the same login page with the appropriate prompt

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserLogin.jsp?log=fail");

}

} else {

// Redirecting the user to the same login page with the appropriate prompt

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserLogin.jsp?log=fail");

}

} catch (Exception e) {

out.print(e);

e.printStackTrace();

}

%>

## COLOR MATCHER MODULE

### REGISTRATION SUB MODULE:

1. The user is presented with a set of colors and prompted to choose 6 colors in the order of their choice.
2. Once the user submits, the HEX values of the colors are sent to server and stored in the database.
3. The user is redirected to the next level of registration

**SOURCE CODE:**

<%@page import="java.sql.ResultSet"%>

<%@page import="java.util.Random"%>

<%@page import="java.sql.Statement"%>

<%@page import="java.sql.DriverManager"%>

<%@page import="java.net.InetAddress"%>

<%@include file="connect.jsp"%>

<%@page import="java.sql.\*" import="databaseconnection.\*"%>

<%@page contentType="text/html" pageEncoding="UTF-8"%>

<%

Statement st = null;

ResultSet rs1 = null;

String color=null, color1=null, color2=null, color3=null, color4=null, color5=null;

// Retrieving the username from the session variable

String name=(String) session.getAttribute("name");

// Receiving the HEX Color codes from the frontend

color = request.getParameter("color1");

color1 = request.getParameter("color2");

color2 = request.getParameter("color3");

color3 = request.getParameter("color4");

color4 = request.getParameter("color5");

color5 = request.getParameter("color6");

try {

// Ensuringwhether the user has completed the first level of Registration

String query1 = "SELECT \* FROM reg WHERE name='"+ name + "' ";

Statement st1 = connection.createStatement();

ResultSet rs2 = st1.executeQuery(query1);

if (rs2.next()) {

// Updating the user's color codes

Statement st2=connection.createStatement();

st2.executeUpdate("UPDATE reg SET color1='"+color+"', color2='"+color1+"',color3='"+color2+"',color4='"+color3+"',color5='"+color4+"',color6='"+color5+"' WHERE name='"+name+"'");

response.sendRedirect("RegPattern.jsp");

} else {

// Redirecting user if something goes wrong during registration

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/RegColor.jsp?fail=serErr");

}

} catch(Exception ex) {

// Redirecting user to 1st level of registration if not have registered

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserReg.jsp?fail=oneFst");

}

%>

### LOGIN SUB MODULE:

1. The user is presented with a set of colors and prompted to choose 6 colors.
2. Once the user submits, the HEX values of the colors are sent to server
3. The color matcher module compares the RGB values of the colors selected by the user to the stored RGB values of the user's chosen colors.
4. From the session the username is retrieved and the corresponding 6 colors are retrieved from the database.
5. If the selected colors match the stored colors in the correct order, the user is granted access to the system.
6. Otherwise, the authentication attempt is rejected and the user is prompted to try again.

**SOURCE CODE:**

<%@ page language="java" contentType="text/html; charset=ISO-8859-1" pageEncoding="ISO-8859-1"%>

<%@page import="java.util.\*"%>

<%@ include file="connect.jsp"%>

<%

// Retrieving the username from the session variable

String name=(String)session.getAttribute("name");

// Receiving HEX Color codes from the frontend

String color1 = request.getParameter("color1");

String color2 = request.getParameter("color2");

String color3 = request.getParameter("color3");

String color4 = request.getParameter("color4");

String color5 = request.getParameter("color5");

String color6 = request.getParameter("color6");

String user = null;

try {

// SQL Query to check whether the color codes entered by the user matches the ones in the database

String sql = "SELECT \* FROM reg where color1='"+color1+"' and color2='"+color2+"' and color3='"+color3+"' and color4='"+color4+"' and color5='"+color5+"' and color6='"+color6+"' and name='" + name+ "'";

Statement stmt = connection.createStatement();

ResultSet rs = stmt.executeQuery(sql);

// Checking if there is any result from the executed query

if (rs.next()) {

// If there exists a result, the user is redirected to the next level of authentication

response.sendRedirect("LoginPattern.jsp");

} else {

// If there is no result, the entered color codes are wrong the user is prompted the information

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/LoginColor.jsp?log=fail");

}

} catch (Exception e) {

out.print(e);

e.printStackTrace();

}

%>

## PATTERN MATCHER MODULE

### REGISTRATION SUB MODULE:

1. The user is presented a grid of 3x3 dots and each dot is associated with a number form 1-9.
2. Then the user is prompted to draw a unique pattern by connecting at least 6 dots without any overlap.
3. The number series corresponding to the drawn pattern is sent to the server.
4. The number series is stored in the database for the current user.
5. Now the user is redirected to a success page.

**SOURCE CODE:**

<%@page import="java.sql.ResultSet"%>

<%@page import="java.util.Random"%>

<%@page import="java.sql.Statement"%>

<%@page import="java.sql.DriverManager"%>

<%@page import="java.net.InetAddress"%>

<%@ include file="connect.jsp" %>

<%@page import="java.sql.\*" import="databaseconnection.\*"%>

<%@page contentType="text/html" pageEncoding="UTF-8"%>

<%

// Retrieving the username from the session variable

String name = (String)session.getAttribute("name");

// Receiving the number series from the front end

String pattern = request.getParameter("password");

try{

// Ensuring whether the user has completed the previous registration process

String query1 = "SELECT \* FROM reg WHERE name='"+ name + "' ";

Statement st1 = connection.createStatement();

ResultSet rs2 = st1.executeQuery(query1);

if (rs2.next()) {

// If there exists a user, then the number series is updated in the database.

Statement st2 = connection.createStatement();

st2.executeUpdate("UPDATE reg SET pattern='" + pattern + "' WHERE name='" + name + "'");

// The user is redirected to the success page where they can login

response.sendRedirect("RegSuccess.jsp?Message=success");

} else {

// If the user has not registered, they are redirected to the previous registration module

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/UserReg.jsp?fail=oneFst");

}

} catch(Exception ex) {

out.println(ex);

}

%>

### LOGIN SUB MODULE:

1. The user is presented a grid of 3x3 dots.
2. Then the user is prompted to draw the pattern drawn during the registration phase.
3. From the session the username is retrieved and the corresponding number series is retrieved from the database.
4. If the selected numbers match the retrieved numbers in the correct order, the user details are sent to the vendor application with a message of login successful.
5. If the number does not match, access is denied and the user is prompted to redraw the pattern.

**SOURCE CODE:**

<%@page import="java.util.\*"%>

<%@ include file="connect.jsp"%>

<%

// The username is retrieved from the database

String name = (String)session.getAttribute("name");

// Receiving the pattern from the front end

String pattern = request.getParameter("password");

try {

// SQL Query that is used to select the record if there is a user with the given name and the pattern

String sql="SELECT \* FROM reg where name='"+name+"' and pattern='"+pattern+"'";

Statement stmt = connection.createStatement();

ResultSet rs = stmt.executeQuery(sql);

if (rs.next()) {

//If there exists a record, then the user session is set and the user is redirected to the 3rd party application

application.setAttribute("name", name);

session.setAttribute("name",name);

response.sendRedirect("UserHome.jsp");

} else {

// If there is no record retrieved, then the user is prompted to re-enter his pattern

response.sendRedirect("http://localhost:8080/Shoulder\_Surfing/LoginPattern.jsp?log=fail");

}

} catch(Exception e) {

out.print(e);

e.printStackTrace();

}

%>

**CHAPTER 6**

# TESTING

Testing is a critical phase in software development, as it helps to identify and remove errors, bugs, and defects from the software. In this project, we performed 2 types of software testing to ensure the quality of the authentication system. The following section describes the testing methods and results.



## UNIT TESTING

The unit testing phase involved testing each module of the authentication system individually to ensure that they function correctly. For splitting the whole project into smaller units, all the 3 modules are split into two parts as mentioned in the Implementation section. After splitting, there are totally 6 units in that was tested. For testing each unit, manual testing was performed. The 6 units are:

* Level 1 – Registration Unit
* Level 2 – Registration Unit
* Level 3 – Registration Unit
* Level 1 – Login Unit
* Level 2 – Login Unit
* Level 3 – Login Unit

Each unit had one common test and some unit specific tests. Input validation was the common test for all the 6 units. The purpose of this test is to safeguard the system against some of the common security attacks such as SQL Injection, XSS Attacks, etc. Some of the unit specific tests that was done to ensure the smooth working of the system is explained below.

### REGISTRATION UNITS

In this project, all the registration units perform similar tasks but not same. So, for testing all the 3 registration units, same tests were performed but with minor or no variation in inputs or outputs. The tests performed and their purpose are given below:

|  |  |  |
| --- | --- | --- |
| **Test Case Number** | **Test Case Name** | **Purpose** |
| UT\_REG\_01 | Input Validation Test | This test is to make sure that all the inputs received were of correct format and to prevent the possibility of any SQL Injection or XSS Attacks. |
| UT\_REG\_02 | Unique User Test | This test is to make sure that only 1 user should be associated with the same email ID, Phone Number and Username. No new user should be able to register with already existing user’s email or username or phone number. |
| UT\_REG\_03 | Database Registration Test | This test is to make sure that the new user’s data is successfully inserted into the database without any errors. |
| UT\_REG\_04 | Error Prompts Test | This test is to make sure that user can see the error prompts of relevant to what went wrong during the process. For each unit, the prompts change depending upon the type of error and the unit |

Table 6.1: Test Case details for Registration Units

### LOGIN UNITS

In this project, just like the registration units, all the login units perform similar tasks but not same. So, for testing all the 3 login units, same tests were performed but with small or no variation in inputs or outputs.

|  |  |  |
| --- | --- | --- |
| **Test Case Number** | **Test Case Name** | **Purpose** |
| UT\_LOG\_01 | Input Validation Test | This test is to make sure that all the inputs received were of correct format and to prevent the possibility of any SQL Injection or XSS Attacks. |
| UT\_LOG\_02 | User Data Retrieval Test | In the Level 1 – Login Unit, for logging into the system, the user can use either username or mail ID. Regardless of both inputs, the correct details associated with the username or mail ID should be retrieved without missing out. Also in the remaining units, color or the pattern should be retrieved successfully for that user. |
| UT\_LOG\_03 | Error Prompts Test | This test is to make sure that user can see the error prompts of relevant to what went wrong during the process. For each unit, the prompts change depending upon the type of error and the unit. |
| UT\_LOG\_04 | 3rd Party Transition Test | This test is to make sure that after successfully authenticating the user, he or she is logged in to the 3rd party application from which they were redirected. |

Table 6.2: Test Case details for Login Units

## INTEGRATION TESTING

After successfully testing each unit separately and ensuring that every unit is working in the way 0that was expected, next stage of testing is the Integration Testing. This testing is to make sure that all works in the way that is expected and not causing any errors or exceptions when integrated with other modules. As in Unit Testing, manual testing was performed. The detailed explanation of test cases and their purpose are given below.

|  |  |  |
| --- | --- | --- |
| **Test Case Number** | **Modules to be Integrated** | **Purpose** |
| Test Case 1 | Level 1 - Level 2 Registration Unit | Verify that the registration details entered by the user are received and processed by Level 1 - Registration Unit and the user is passed on to Level 2 - Registration Unit. |
| Test Case 2 | Level 2 - Level 3 Registration Unit | Verify that the user registration details are validated and verified by Level 2 - Registration Unit and the user is passed on to Level 3 - Registration Unit. |
| Test Case 3 | Level 3 Registration Unit | Verify that the user registration is completed successfully by Level 3 - Registration Unit and the user account is created. |
| Test Case 4 | Level 1 - Level 2  Login Unit | Verify that the login credentials entered by the user are received and processed by Level 1 - Login Unit and only the users who cleared level 1 are passed on to Level 2 - Login Unit and the rest are prompted to re-enter their level 1 login credentials |
| Test Case 5 | Level 2 - Level 3  Login Unit | Verify that the user login credentials are validated and verified by Level 2 - Login Unit and only the users who cleared level 2 are passed on to Level 3 - Login Unit and the rest are prompted to re-enter their login credentials. |
| Test Case 6 | Level 3 Login Unit - 3rd Party Application | Verify that the user login credentials are validated and verified by Level 3 - Login Unit and only the users who cleared level 3 are passed on to the 3rd party application. |

Table 6.3: Test Case details for Integration Testing

**CHAPTER 7**

# CONCLUSION AND FUTURE SCOPE

The graphical password authentication system offers a unique and innovative way to authenticate users. The system offers a high degree of security and is less prone to attacks like brute-force attacks and password guessing. The use of patterns and colors makes it easier for users to remember their authentication credentials and reduces the burden of memorizing complex passwords. Additionally, the system offers a user-friendly experience that is engaging and fun, increasing user satisfaction. The use of multiple authentication factors, such as patterns, colors, and passwords, makes it difficult for attackers to gain unauthorized access to the system. Overall, the graphical password authentication system offers a promising method additional to traditional password-based authentication systems.

There are several opportunities for further development and improvement of the graphical password authentication system. One area of improvement could be to replace and implement authentication factors such as biometric authentication, such as fingerprint or facial recognition, to further enhance the security of the system. The use of biometric authentication would make the system even more secure and would reduce the chances of unauthorized access to the system. Furthermore, the system could benefit from incorporating machine learning algorithms to analyze user behavior and recognize patterns in their authentication methods. This would enable the system to learn and adapt to each user's unique authentication patterns, further enhancing the system's security. Moreover, it would be beneficial to explore the integration of the graphical password authentication system with other security measures, such as two-factor authentication, to create a more comprehensive security solution. The integration of multiple security measures would offer a more robust security framework and would make it even more challenging for attackers to gain unauthorized access to the system. Furthermore, the system can include measures to prevent brute-force attacks, such as setting limits on the number of failed attempts before locking the user out of the system. In conclusion, the graphical password authentication system offers a promising alternative to traditional password-based authentication systems. The system is user-friendly, engaging, and provides a high degree of security, making it suitable for use in a wide range of applications. There are several opportunities for further development and improvement of the system, including the implementation of additional authentication factors, improving the user interface and user experience, incorporating machine learning algorithms, and integrating the system with other security measures. The graphical password authentication system is a promising technology with vast potential, and it is expected to become an increasingly popular authentication method in the future.

**APPENDIX – 1 (INDUSTRY APPROVAL & COMPLETION)**

**APPENDIX – 2 (SCREENSHOTS)**

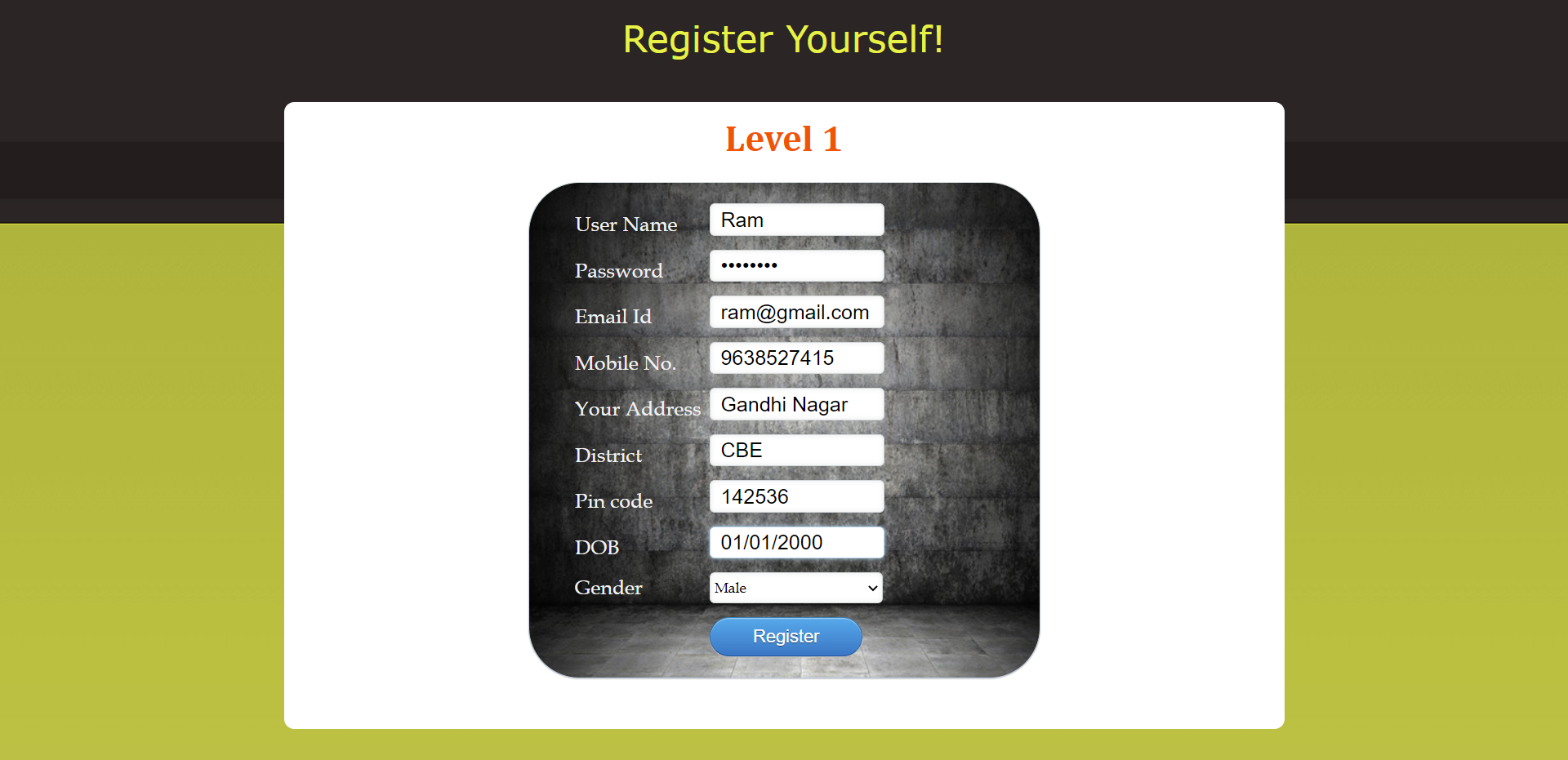
****

Fig 1: User Registration Page

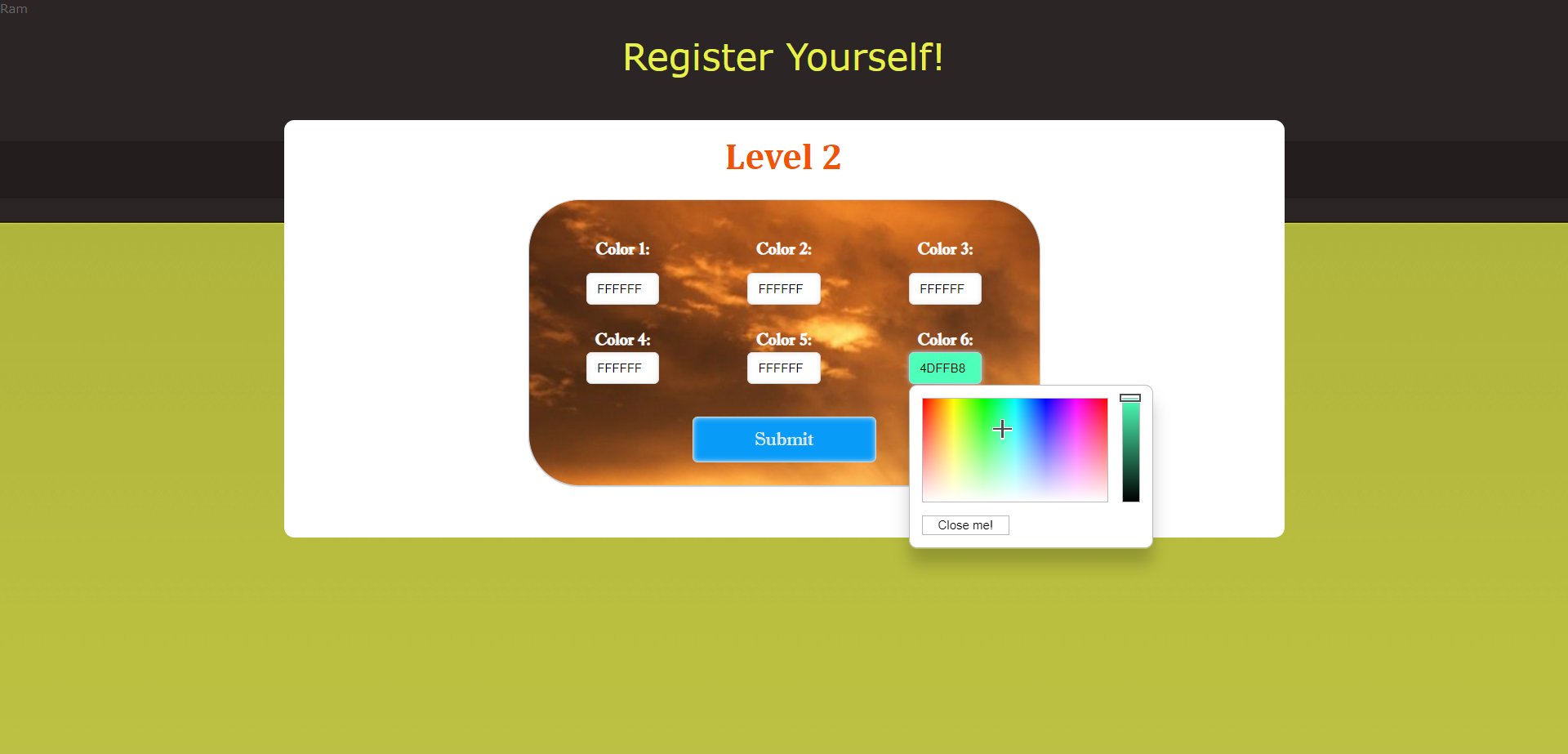
****

Fig 2: Color Registration Module

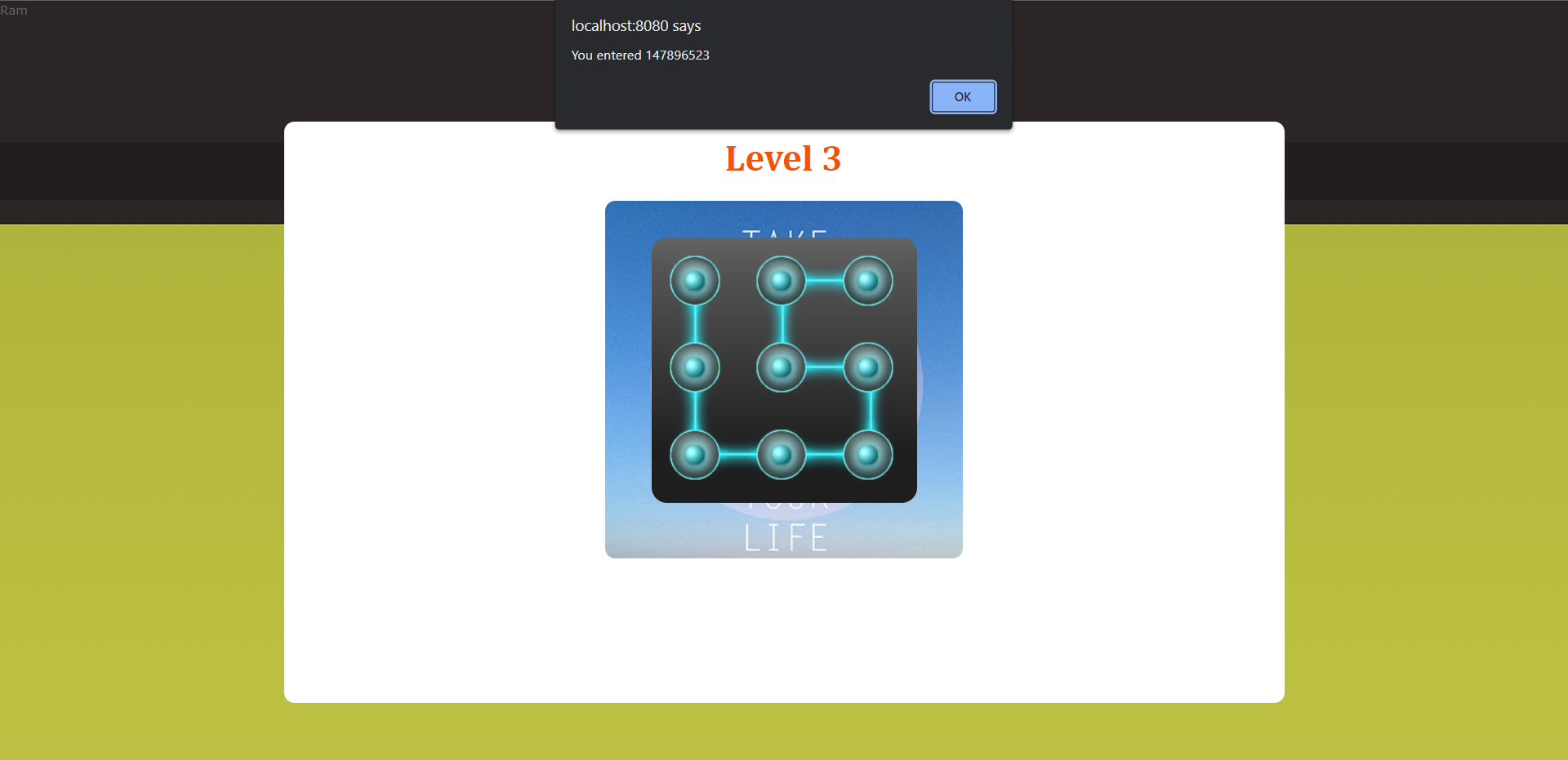
****

Fig 3: Pattern Registration Module



Fig 4: Password Login

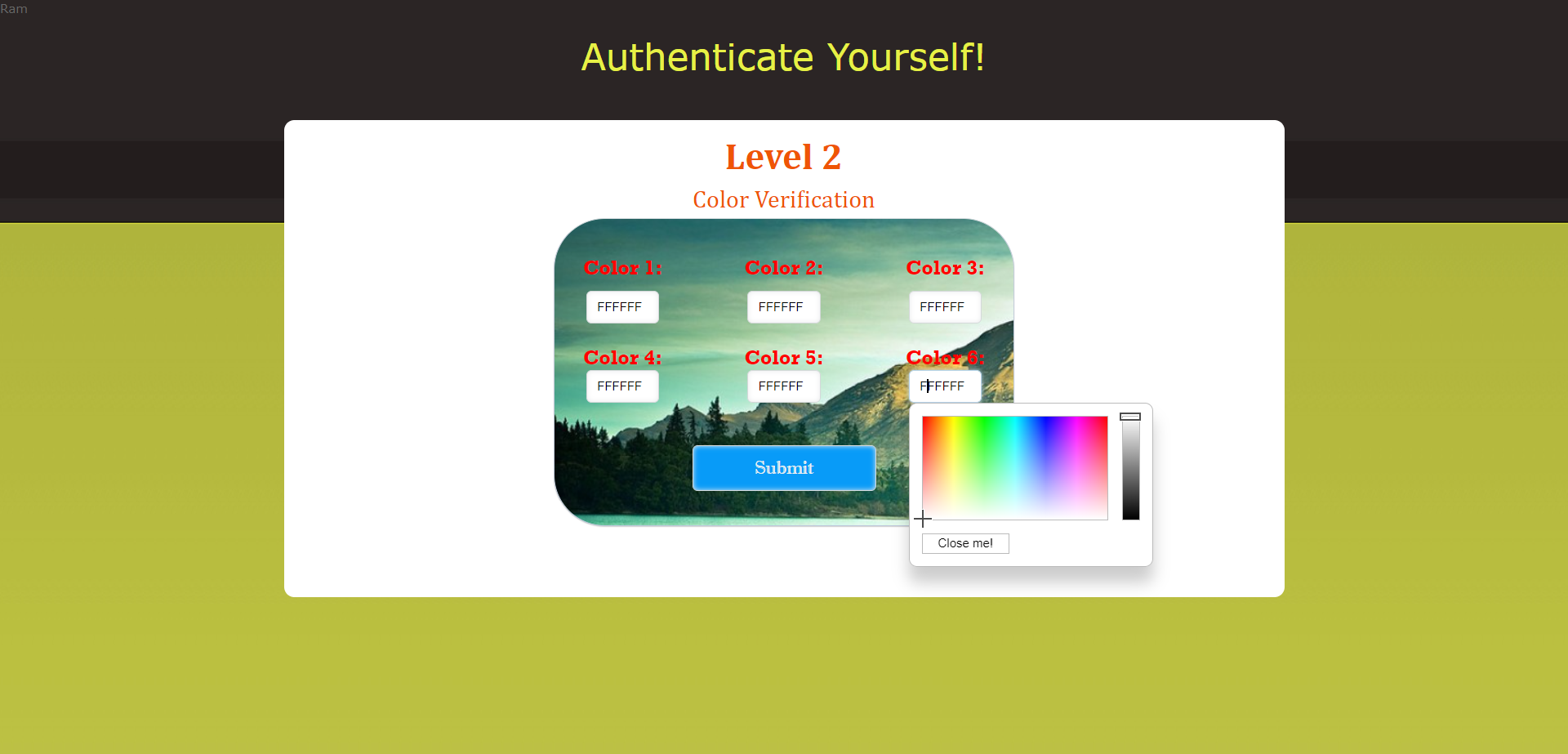


Fig 5: Color Verification

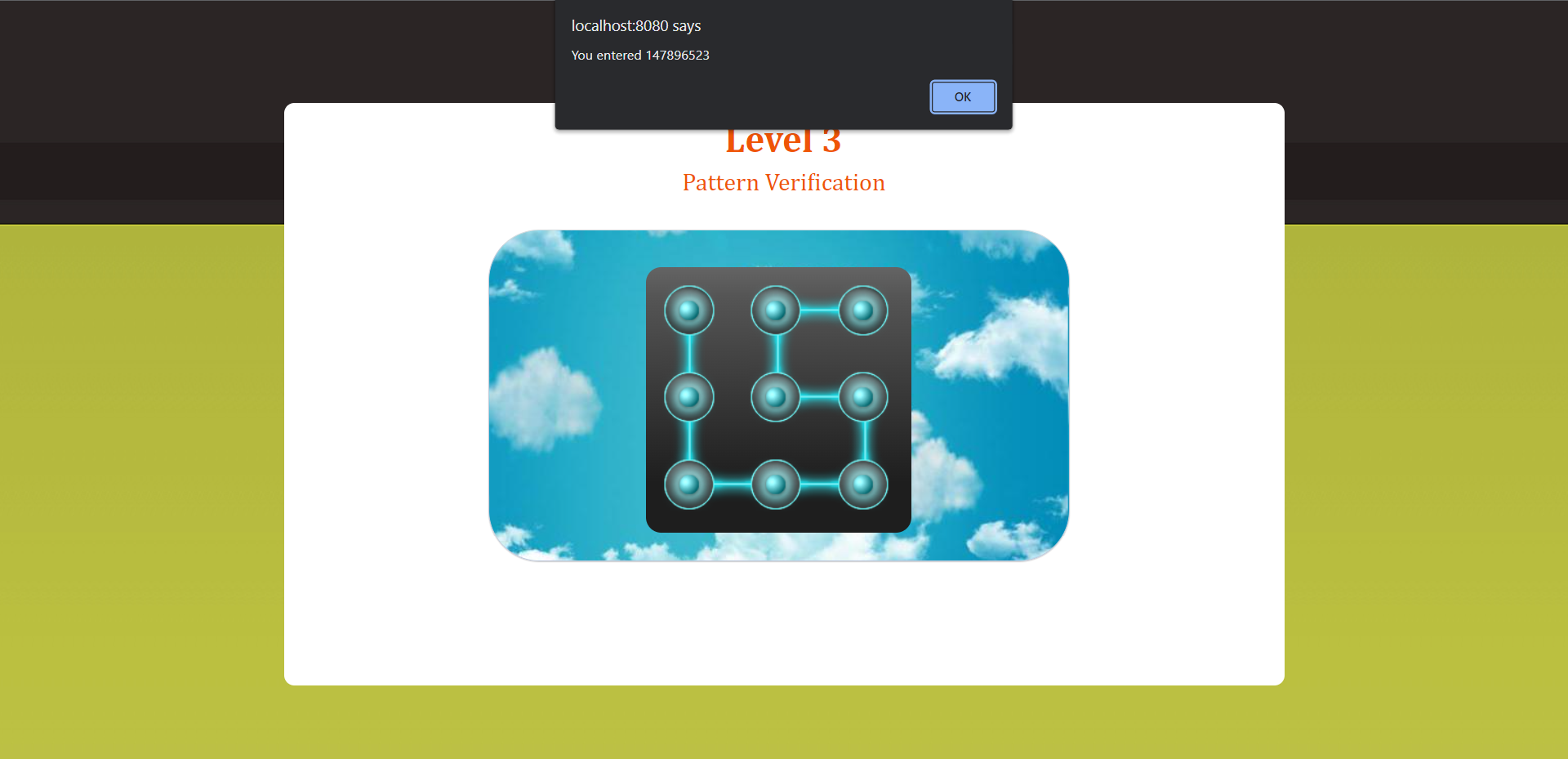


Fig 6: Pattern Verification

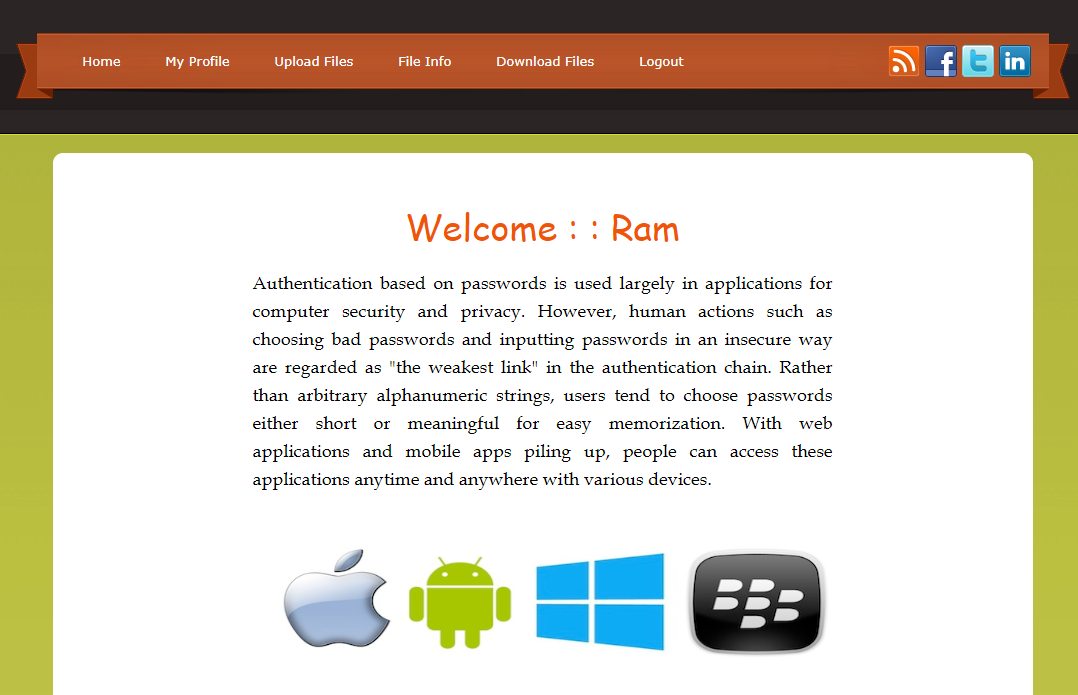


Fig 7: Login Successful!

**APPENDIX – 3 (PUBLICATION)**

**PUBLICATION DETAILS:**

**Authors:**

Jebakumar Immanuel D, Ramalingam V, Akash Iyer, Tharun Kumar, Narayanan M S.

**SCOPUS Publication:**

|  |  |
| --- | --- |
| **Conference Name:** | International Conference on Pervasive Computing and Social Networking |
| **Status :** | Received Acceptance & Paid and Submitted final draft of the paper |

**UGC CARE Journal Publication:**

|  |  |
| --- | --- |
| **Jounal Name :** | ICTACT Journal on Communication Technology |
| **Status :** | Submitted paper & Waiting for Acceptance |

**SCOPUS INDEXED JOURNAL**

**UGC CARE JOURNAL**

**REFERENCES**

1. A. Paivio, T. Rogers, and P. Smythe, “Why are pictures easier to recall than words?
2. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, “Smudge attacks on smartphone touch screens,” in USENIX 4th Workshop on Offensive Technologies, 2010.
3. Bousfield, Weston Ashmore, J. Esterson, and Gerald A. Whitmarsh. "The effects of concomitant colored and uncolored pictorial representations on the learning of stimulus words." Journal of applied psychology 41, no. 3 (1957): 165.
4. E. von Zezschwitz, A. De Luca, and H. Hussmann, “Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance,” in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI ’14. New York, NY, USA: ACM, 2014, pp. 461–470.
5. Iranna, A. M., and Pankaja Patil. "Graphical password authentication using persuasive cued click point." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2, no. 7 (2013): 513-517
6. Jermyn, Ian H., Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. "The design and analysis of graphical passwords." USENIX Association, 1999
7. M. Martinez-Diaz, J. Fierrez, and J. Galbally, “Graphical passwordbased user authentication with free-form doodles,” IEEE Transactions on Human-Machine Systems, vol. PP, no. 99, pp. 1–8, 2015
8. M. Martinez-Diaz, J. Fierrez, and J. Galbally, “The doodb graphical password database: Data analysis and benchmark results,” Access, IEEE, vol. 1, pp. 596–605, 2013.
9. Mazurek, Michelle L., et al. "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1309-1318. ACM, 2013.
10. Monrose, Fabian, and Aviel Rubin. "Authentication via keystroke dynamics." In Proceedings of the 4th ACM Conference on Computer and Communications Security, pp. 48-56. 1997.
11. Nali, Deholo, and Julie Thorpe. "Analyzing user choice in graphical passwords." School of Computer Science, Carleton University, Tech. Rep. TR-04-01 (2004).
12. Oakley and A. Bianchi, “Multi-touch passwords for mobile device access,” in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp ’12. New York, NY, USA: ACM, 2012, pp. 611–612.
13. Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words. Psychonomic Science, 11(4), 137-138.
14. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,”
15. Shah, M., Naik, R., Mullakodi, S., & Chaudhari, S. (2018). Comparative analysis of different graphical password techniques for security. Int Res J Eng Technol (IRJET), 5(4), 1873-1877
16. Sobrado, Leonardo, and Jean-Camille Birget. "Graphical passwords." The Rutger Scholar 4 (2002).
17. Stobert, Elizabeth, Alain Forget, Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. "Exploring usability effects of increasing security in click-based graphical passwords." In Proceedings of the 26th Annual Computer Security Applications Conference, pp. 79-88. 2010.
18. Stobert, Elizabeth, and Robert Biddle. "Memory retrieval and graphical passwords." In Proceedings of the ninth symposium on usable privacy and security, pp. 1-14. 2013.
19. Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2016). A shoulder surfing resistant graphical authentication system. IEEE Transactions on Dependable and Secure Computing, 15(2), 180-193.
20. Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." In 21st Annual Computer Security Applications Conference (ACSAC'05), pp. 10-pp. IEEE, 2005.
21. Tari, Furkan, A. Ant Ozok, and Stephen H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords." In Proceedings of the second symposium on Usable privacy and security, pp. 56-66. 2006.
22. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies, 63(1-2), 102-127.
23. Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. "Authentication using graphical passwords: Effects of tolerance and image choice." In Proceedings of the 2005 symposium on Usable privacy and security, pp. 1-12. 2005
24. Zhao, H., & Li, X. (2007, May). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In 21st international conference on advanced information networking and applications workshops (AINAW'07) (Vol. 2, pp. 467-472). IEEE.