PORTFOLIO
CHEW FAN YEE

LINK: MY RESUME
LINK: PORTFOLIO WEBPAGE

ABOUT ME

I'm a confident and bold problem solver with a background in cyber security, system deployment, and IT operations. I specialize in network security, vulnerability assessment, and ethical hacking, with hands-on experience from academic and internship projects.

EDUCATION

BSC (HONS) IN COMPUTER SCIENCE (CYBER SECURITY)
Asia Pacific University

- Studied cryptography, malware analysis, ethical hacking, and risk assessment.
- Final Year Project: Developed a security application integrating real-world threat mitigation techniques.

EXPERIENCE

INTERN, IT DEPARTMENT
TURCOMP BMB SDN BHD

- Supported software deployment for eWMS, ERP, and SMS platforms.
- Maintained and assisted with eCommerce and Lapasar systems.
- Gained experience in troubleshooting, integration, and system support across departments.

SKILLS

- Technical: Network Security, Cryptography, Malware Analysis, Vulnerability Assessment, Penetration Testing
- Soft Skills: Critical Thinking, Communication, Teamwork, Organization, Time Management
- Languages: English, Chinese, Malay

CONTACT

- Email: fan.yee.chew@gmail.com
- Phone: +60183123771
- Location: Kuala Lumpur, Malaysia

PORTFOLIO

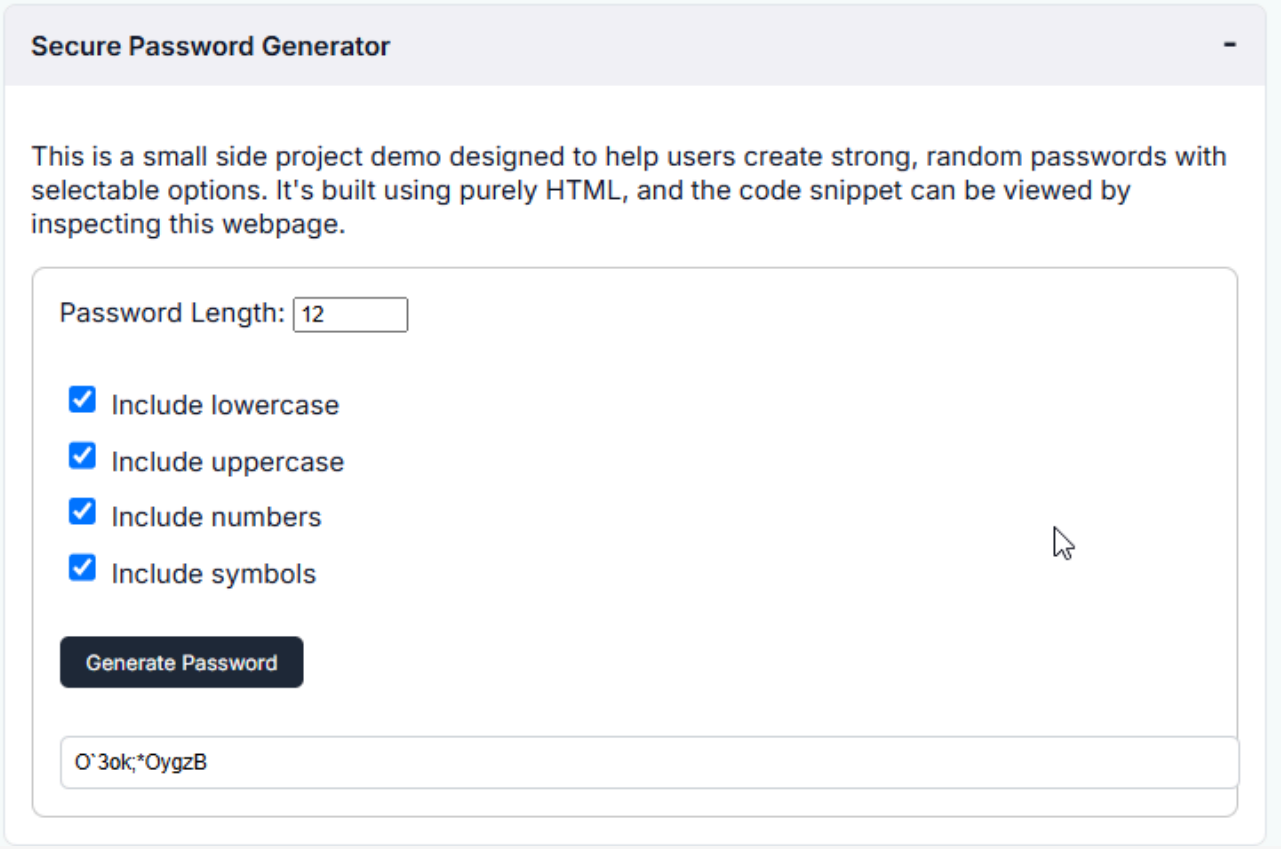
SECURE PASSWORD GENERATOR

INTRODUCTION

This is a small side project demo designed to help users create strong, random passwords with selectable options. It's built using purely HTML.

DEMONSTRATION

The password generator allows users to create strong, random passwords with customizable options. Users can specify the password length and choose to include lowercase, uppercase, numeric, and symbolic characters. The generator validates that at least one character type is selected, combines the chosen character sets into a pool, and uses a loop with random indexing to create a password of the desired length. The generated password is then displayed in a read-only text field, providing a simple and effective way to create secure passwords.



Kindly follow this link for more demonstration:

Full Showcase

PORTFOLIO

ADVANCED PASSWORD STRENGTH ASSESSMENT TOOL

INTRODUCTION

This FYP project addresses the growing need for robust password security in an increasingly digital world. It aims to empower users by providing a comprehensive solution that enhances their ability to create and maintain strong passwords, thereby mitigating cybersecurity risks.

OBJECTIVE

The primary objective of the project is to develop a user-friendly application that facilitates password strength assessment. Specific goals include creating an intuitive interface, implementing advanced algorithms for accurate evaluations, and promoting user education on secure password practices.

KEY COMPONENTS

- Real-Time Password Strength Evaluation: Users can input their passwords to receive immediate feedback on strength levels.
- Personalized Recommendations: The tool analyzes weaknesses in passwords and provides tailored suggestions for improvement.
- Educational Resources: A revolving set of links to password security best practices and informative materials is available to enhance user awareness.
- User-Friendly Interface: Designed with accessibility in mind, the interface is intuitive for users of varying technical expertise.

OUTCOME

The project successfully delivers a functional and effective password strength assessment tool that not only evaluates password security but also educates users on best practices. This outcome contributes to enhanced digital security awareness and encourages users to adopt stronger password habits.

Kindly follow this link for more information:

Full Github Documentation

FINAL YEAR PROJECT

Advanced Password Strength Assessment Tool

By

CHEW FAN YEE

TP060853

APU3FS308CS(CYB)

B.Sc. (Hons) Computer Science Specialism in Cyber Security

Supervised by Mr. David Tan

2nd Marker: Mr. Yogeswaran Nathan

2024

Contents

ACKNOWLEDGEMENT

I extend my heartfelt gratitude to all those who have played a pivotal role in the realization of my Final Year Project. Without the unwavering support and contributions from various individuals, this milestone would not have been attainable.

Foremost, I express my sincere appreciation to my supervisor, Mr. David Tan, of the School of Technology. With the guidance and encouragement from Mr. Tan, it have been instrumental in providing me with invaluable knowledge and support throughout the development of my Final Year Project. Mr. Tan's expertise in the field of Cyber Security not only steered this project in the right direction but also significantly enriched its content. The patience and constructive feedback he gave were constant motivators, pushing me to strive for a higher standard of excellence in my work.

In addition to my supervisor, I want to thank my friends, my family, and those unnamed individuals who have generously offered their help and advice. The words of encouragement, networks, and shared research insights have been indispensable in shaping the content and direction of this investigation report. I am optimistic that the groundwork laid in this initial phase will greatly contribute to the development of the system in the second half of the project, resulting in the creation of a good Final Year Project.

ABSTRACT

Motivated by the current world's pervasive threat of cyber breaches resulting from weak passwords, this research employs advanced methods to assess and strengthen password integrity. Through a systematic analysis of existing password-related vulnerabilities, the project investigates and proposes comprehensive solutions to mitigate risks. The methodology involves a meticulous examination of current password security practices, leveraging cutting-edge technologies to design an assessment tool capable of evaluating the strength and vulnerability of passwords. Preliminary results indicate promising advancements in password protection, with ongoing efforts dedicated to refining and optimizing the tool's functionality. The project's significance lies in its potential to fortify digital defences against unauthorized access, contributing to the overarching goal of creating a secure and resilient digital infrastructure. Aligned with Sustainable Development Goal 9, "Industry, Innovation and Infrastructure," the Advanced Password Strength Assessment Tool plays a crucial role in promoting technological innovation and fostering resilient information systems.

Keywords: Cybersecurity, Password Assessment, Digital Security, Innovation, Information Systems, Password Strength Evaluation, Cyber Threats.

CHAPTER 1: INTRODUCTION

1.1 Introduction

It is through our contemporary digital landscape that technology permeates every facet of our lives, the imperative for robust cybersecurity measures has reached unprecedented levels. As passwords stand as the initial line of defence against unauthorized access to sensitive information, making their strength a pivotal factor in ensuring online security. However, the disconcerting reality persists, which is the substantial portion of the global population continues to employ weak or easily decipherable passwords, exposing themselves to potential cyber threats.

This project centres on the swiftly evolving realm of cybersecurity within the business and industry sector. Faced with the escalating frequency and sophistication of cyberattacks, individuals and organizations must proactively adopt measures to safeguard their digital assets. It is within this context that our project assumes significance.

The vulnerability posed by weak passwords extends beyond mere inconvenience; it encompasses substantial risks to personal and organizational security. Incidents of sensitive data breaches can result in financial losses, identity theft, and compromise the privacy and safety of individuals and communities (Groeneveld, 2022). Addressing this issue becomes not just a matter of convenience but a fundamental tenet of digital citizenship in today's interconnected world.

Aligned with the 9th Sustainable Development Goal (SDG), "Industry, Innovation, and Infrastructure," this project epitomizes the potency of innovation in the cybersecurity domain. By introducing a user-friendly, efficient, and accessible approach to assess password strength, our aim is to contribute to creating a safer digital environment. Strengthening passwords, in turn, fortifies the very infrastructure of digital systems, offering protection to individuals and organizations against potential threats.

To realize this project's objectives, a comprehensive exploration of key research areas is imperative. This includes an investigation into best practices and standards for password

security, an examination of existing assessment methods, and an exploration of algorithms for password strength. By delving into these research areas, the aim is to craft an innovative solution that not only empowers individuals to safeguard their digital identities but also aligns with the broader objective of constructing a secure, innovative, and resilient digital infrastructure in harmony with the 9th SDG.

1.2 Problem Background

In the era of digital advancement, the security of personal and organizational data pivots on the resilience of passwords. Despite an escalating awareness of cybersecurity risks, a substantial number of users grapple with the creation and maintenance of robust passwords. AustralianMutualBank (2023) underscores the crux of the issue, attributing it to users' inadequacies in knowledge, motivation, and effort – factors often insufficient in generating passwords resilient against contemporary cyber threats. Existing research has delineated key challenges within password security:

- User Knowledge Gap: One prominent challenge in password security stems from a knowledge gap among users. Misconceptions persist, equating password strength solely with complexity, leading to convoluted combinations of letters, numbers, and characters. This misunderstanding tends to let the user fosters passwords that are challenging to recall and prone to errors, exacerbated by a lack of clear guidance on crucial factors such as length, uniqueness, and unpredictability.

- User Motivation: User motivation emerges as another obstacle in password security. Convenience frequently takes precedence over security, as the onus of remembering intricate passwords for multiple accounts becomes burdensome. Some users underestimate the risks associated with weak passwords, assuming they are unlikely targets for cyberattacks.

- User Effort: The substantial effort required to create and manage robust passwords poses a significant challenge. Juggling unique, strong passwords across numerous accounts is time-consuming, fostering "password fatigue." Users may succumb to reusing passwords or employing weak ones due to the overwhelming nature of constant password management.

- Password Reuse: Widespread password reuse, driven by simplicity and convenience, constitutes a critical security concern. This practice exponentially magnifies the impact of

security breaches, granting unauthorized access to multiple accounts when one password is compromised.

- Cybersecurity Threats: The ever-evolving landscape of cybersecurity threats adds a persistent challenge. Cybercriminals employ new methods, including brute force attacks and advanced cracking software, necessitating continual adaptation of password practices. The prevalence of compromised password databases on the dark web further underscores the need for enhanced password security measures.

This project innovatively extends prior research in password security by providing a tangible tool for comprehensive password strength evaluation. Unlike previous efforts focusing on user education and complex rule recommendations, this project empowers users with real-time feedback tailored to their unique passwords. Bridging the gap between theoretical knowledge and practical implementation, it aims to tackle the root causes of weak password security.

Furthermore, aligning with recent trends in cybersecurity, the project emphasizes user-centric security solutions. Instead of solely relying on users' informed decisions, innovative algorithms will objectively assess password strength, aiding users in making more informed choices.

In conclusion, while prior work laid the foundation for password security awareness, this project represents a substantial leap forward by offering a practical solution that directly addresses user knowledge, motivation, and effort concerns. By enhancing the user experience and promoting strong password practices, it aspires to contribute to a more secure digital environment aligned with contemporary cybersecurity needs.

1.3 Project Aim

The aim of this project is to create a user-friendly and impactful tool that enables individuals to generate and sustain robust passwords, ultimately fortifying their digital security. This endeavour seeks to address the disparity in user knowledge, motivation, and effort related to password security. Aligned with the 9th Sustainable Development Goal, the primary objective is to advance innovative solutions fostering digital security, thereby aligning with broader initiatives for a secure and resilient digital infrastructure.

1.4 Objectives

In pursuit of fortifying digital security in an era rife with cyber threats, this project delineates clear objectives aimed at developing an advanced Password Strength Assessment Tool. The overarching goal is to create a comprehensive solution that addresses the critical aspects of user-friendly accessibility, robust algorithmic assessment, and user education within the realm of password security.

- To create and deploy a user-friendly application that facilitates the assessment of password strength, incorporating the development of an interface tailored to user-centric principles.

- To formulate resilient password strength assessment algorithms, capable of delivering precise and instantaneous feedback by analysing diverse factors, including password length, character variety, predictability, and resilience against common cracking techniques.

- To enlighten users on effective password security practices by integrating educational and informative resources within the tool, thereby heightening user awareness, and understanding of secure password practices.

1.5 Scope

The "Advanced Password Strength Assessment Tool" embarks on a comprehensive journey to empower individual users in fortifying their digital security through a range of targeted functionalities. The scope of this project is intricately designed to address the unique needs and objectives of individual users, fostering an environment where password security is not only assessed but actively improved. Within this framework, several key tasks are outlined to ensure the successful development and deployment of the tool.

Scope of Tasks:

- Password Strength Assessment and Feedback:
    - Users will have the ability to evaluate the strength of their passwords.
    - The tool will provide real-time feedback on the assessed strength of passwords, offering users immediate insights into the security level of their credentials.

- Personalized Recommendations:
    - The tool will analyse weaknesses in users' passwords.
    - Users will receive personalized recommendations tailored to the specific weaknesses identified, guiding them on how to strengthen their passwords effectively.

- Educational Resources:
    - The tool will incorporate a repository of educational materials and resources focused on password security practices.
    - Users can access informative content that enhances their understanding of best practices, fostering a culture of cybersecurity awareness.

- User Monitoring and Enhancement:
    - The tool will provide a user-friendly interface for regular monitoring of password security.

- Users will be able to actively enhance their password security based on the feedback and recommendations provided by the tool.

While the password strength assessment tool aims to provide a comprehensive utility for individual users, certain limitations exist. Firstly, the focus on empowering individuals to adopt improved personal password habits means enterprise-grade access management capabilities get excluded from scope. Additionally, inherent technology constraints influence the practical size and sophistication possible across the spectrum of desired features. Advanced encryption, decentralized storage protocols and biometric authentication elements will stretch the bounds of existing methods. Though leveraging cutting-edge technologies in design, balancing complex security with system performance and stability remains imperative. Ultimately the tool must deliver a reliable, user-centric experience guiding better passwords; a pragmatism which shapes decisions around balancing functional possibilities against practical achievement.

Centered on enabling individuals to securely manage personal credentials, several core capabilities define the project's development commitments. Intuitive design topping the priorities manifests through accessible interfaces navigable for tech-novice users. Robust algorithms follow, assessing password constructs across an array of vulnerability factors like length, randomness, hash strengths. Embedding educational resources takes the next spot, equipping users as informed, active cybersecurity stewards. This ethos of nurturing self-efficacy permeates the fourth focal function - continuous monitoring tools that encourage persistent, proactive safety habits versus reactive ones. Through these fused facets spotlighting usability, evaluation, guidance and habit-building, the password tool aims users can conveniently yet securely operate in modern digital ecosystems. While constrained in enterprise scope, individual empowerment persists as the central driver across all planned capabilities to make personal credential management comprehensible, actionable, and most critically, safe.

While seeking an encompassing solution for individuals, certain capabilities get consciously excluded from design scope. Tailoring usability for average consumers implies enterprise-specific adaptations lie outside project boundaries. Functionality like centralized dashboard oversight or group permission protocols cater more to organizational credential management

versus personal. Additionally, pragmatic technology restrictions set expectations around feasible features based on encrypted data limits or interface complexity tolerances. Augmenting biometric inputs or decentralizing storage may push implementation capacity. Hence users should not anticipate every conceivable bell or whistle within any initial tool launch. However, possibilities clearly exist to incrementally expand technical boundaries over later iterations once core individual user-centric functionalities get established. For now, the focus remains students and consumers enhancing personal password habits before expanding to more advanced or niche capabilities.

In conclusion, the scope of the "Advanced Password Strength Assessment Tool" is strategically crafted to empower individual users in optimizing their password security. By incorporating assessment, feedback, recommendations, educational resources, and user-friendly interfaces, the project aspires to contribute significantly to the cultivation of a secure digital environment for individual users.

1.6 Potential Benefit

1.6.1 Tangible Benefit

The primary tangible benefit of the "Advanced Password Strength Assessment Tool" is an immediate enhancement in digital security for individual users. By actively assessing the strength of passwords, providing real-time feedback, and offering personalized recommendations, users can fortify their online accounts against potential cyber threats. This tangible improvement in password security directly translates to a reduced risk of unauthorized access, data breaches, and identity theft. The tool's ability to guide users in creating and maintaining robust passwords contributes tangibly to their overall cybersecurity posture.

1.6.2 Intangible Benefit

An intangible benefit of the tool is the cultivation of a heightened sense of cybersecurity awareness among users. Through the integration of educational materials and resources within the tool, users gain a deeper understanding of password security best practices. This increased awareness extends beyond the immediate use of the tool, empowering users to make informed decisions about their digital security in various online contexts. The intangible benefit lies in the long-term impact of creating a user base that is more vigilant, knowledgeable, and proactive in safeguarding their digital identities.

1.6.3 Target User

The primary target user for the "Advanced Password Strength Assessment Tool" is individuals across diverse demographics who seek to bolster their password security. This includes but is not limited to:

- General Users: Individuals with varying levels of technical expertise who want to enhance the security of their online accounts.
- Students: Particularly those navigating the digital landscape for educational purposes.
- Professionals: Individuals using digital platforms for work-related activities.
- Elderly Users: Tailoring the tool to be accessible and user-friendly for individuals less familiar with advanced technologies.

The tool's design and functionalities cater to a broad spectrum of users, making it inclusive and applicable to anyone aiming to strengthen their password security. The target user base reflects the tool's versatility and accessibility, ensuring that individuals from different walks of life can benefit from its features.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In the realm of academic research and scholarly pursuits, a literature review stands as a crucial cornerstone, providing the essential framework upon which new knowledge is constructed. This comprehensive survey and synthesis of existing literature on a particular subject serve multifaceted purposes, each contributing to the depth and validity of any research endeavour. The University of EDINBURGH stated as a foundational step in the research process, the literature review serves to contextualize, analyse, and critically evaluate the body of knowledge that precedes the study, offering a roadmap for further exploration. This introduction outlines the indispensable reasons why undertaking a literature review is not merely a procedural step but an integral and invaluable component of academic inquiry.

2.2 Domain Research

Passwords are ubiquitous in the digital world, used to protect access to devices, accounts, services, and sensitive data. However, many users still employ weak passwords that are easy for cybercriminals to guess. Recent research analyses the continued prevalence of weak passwords and evaluates updated techniques to bolster password strength and security. Despite frequent security breaches and awareness campaigns, weak passwords like “123456” and “password” remain stubbornly common. Simple numerical and keyboard patterns, names, and dictionary words continue to dominate. The most popular passwords have not changed significantly in the last decade. The authors conclude that guidance encouraging password complexity has failed to motivate the majority to move beyond basic insecure choices.

To analyse aggregated password data sets, security researchers have developed quantitative password strength estimators. Ur et al. (2020) recently introduced an open-source tool called Password Evidence and Strength (PEAS) to provide feedback on portfolio strength for a collection of passwords. Built on neural networks, it considers the full distribution of passwords rather than assessing passwords individually. In tests, PEAS generated strength estimates better aligned with password cracking rates compared to entropy metrics. Creating more accurate

models for password strength at scale enables appropriately targeted interventions to improve security.

Many proposed solutions aim to nudge users towards stronger passwords without overly disrupting their experience. Research find that requiring three-character types produces a good level of security while maintaining usability. Custom strength meters providing instant feedback during password creation may also positively influence security. Egelman et al.'s (2020) meter assessing semantics improved resistance to guessing attacks. Explicitly enforcing expiration dates continues to be controversial, as very frequent resets annoy users who then make minimal changes to their old passwords.

Recent research provides updated perspectives on the severity of weak password usage and pathways for improving security. While passwords likely will not disappear any time soon, supplemental authentication schemes provide users options for enhanced convenience without compromising security. More accurate estimating of portfolio password strength can enable policies and targeted interventions to be efficiently tailored towards those most at risk. Individual accounts now may be protected through multiple factors, but improving baseline password strength across platforms remains critical for overall security and data protection.

In 2020 and beyond, weak passwords continue to predominate despite the known risks. Through leveraging emerging strength estimators to target those most vulnerable, researching usability of composition policies and feedback systems, and integrating convenient alternative authentication schemes, cybersecurity experts are making headway in addressing this persistent problem. But much work remains to change ingrained user behaviour and prevent threats enabled through easily guessed passwords permeating so many facets of digital life.

2.3 Similar Systems

2.3.1 Microsoft Password Checker

Microsoft built a password strength evaluating tool into its Windows 10 and Windows 11 operating systems to assess new account passwords created by users. When creating an account,

such as when setting up a new user profile on a Windows computer, it will analyse the password entered and provide real-time feedback. The Microsoft password checker tool looks at multiple components including length, complexity, use of common passwords, and key patterns to determine strength. It provides a coloured coded indicator highlighting passwords as very weak, weak, medium, or strong. The tool offers helpful tips during password creation, guiding the user to lengthen the password, add special symbols and numbers, and avoid reused or common passwords to strengthen it. Since it is baked into the Windows sign-up flow, it provides a frictionless way for users to create stronger passwords from the start, though the criteria and assessments are fixed based on Microsoft's guidelines, so users have limited configuration (Alexander, 2018).

2.3.2 Dropbox zxcvbn

Dropbox developed an open-source password analysing tool called zxcvbn that serves as a JavaScript library that developers can integrate into both web and mobile applications. It uses a very advanced set of patterns matching rules and entropy calculations to estimate the strength of passwords. Zxcvbn runs through thousands of common passwords, manipulations of keyboard patterns, repeats of characters, sequences, dates, and names to detect weak passwords. Unlike basic length and complexity checks, it can catch a wide array of password choices that follow predictable patterns generally considered unsafe (Wheeler, 1970). The tool generates an entropy score from 0 to 4 to rate password strength from highly guessable to extremely secure based on computations of all possible password permutations fitting the identified patterns. One of the most useful features of zxcvbn is that goes beyond just assigning a score, and it provides meaningful feedback about the specific weakness that was identified so developers can guide users properly.

2.3.3 Google Password Checkup

As one of the most widely adopted password management solutions, Google developed a simple browser extension called Password Checkup. It can be added into Chrome, Edge and other Chromium based browsers and provides a way to check on passwords already stored in users' Google accounts. Once installed, Password Checkup syncs with a user's Google products like Gmail, Drive and Android device passwords and alerts them if any credentials are reused, known

to be compromised or otherwise unsafe. It flags the specific weak passwords and prompts users to immediately change them rather than just assigning an arbitrary score. Part of what makes Password Checkup user-friendly is it never asks users to manually enter any current passwords for analysing. It simply taps into passwords Google already manages across products and devices to recommend fixes for compromised ones. However, the tool does not estimate overall password strength or prevent bad passwords when initially created, it merely checks existing passwords and relies on user's own judgement for changing them.

2.4 Comparison

Tool	Analysis Method	Interface	Use Cases	Weaknesses
Microsoft Checker	Length, complexity, common passwords	During password creation in Windows	Creating new Windows user accounts	Limited scope, fixed criteria
Dropbox zxcvbn	Pattern matching, entropy	API/library for integration	Password validation for web/mobile apps	Computation heavy, requires coding
Google Checkup	Known compromised passwords	Browser extension	Checking already saved Google passwords	Only for Google products, no strength estimate

CHAPTER 3: METHODOLOGY

3.1 System Development Methodology

The Waterfall methodology will provide a structured, linear approach to the development of the password strength assessment tool. This methodology involves progressing sequentially through a series of distinct phases, with some overlap and iteration between phases. The Waterfall methodology allows for clear documentation of requirements early on, followed by orderly design, development, testing, and deployment stages. It is an appropriate choice for this project due to the clear product definition and understanding of requirements at the start, as well as the straightforward functionality to be built without need for ongoing revisions.

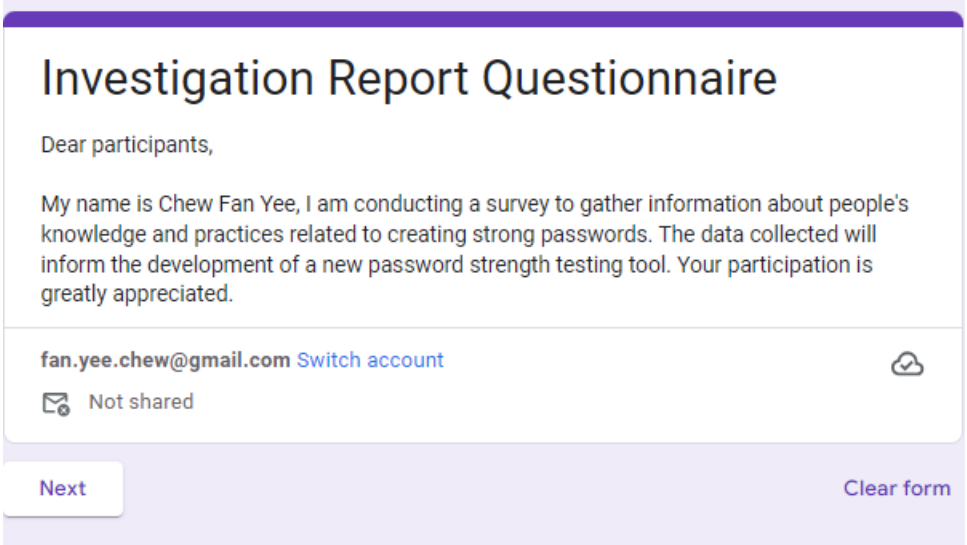
Atlassian stated that a major advantage of applying the Waterfall model to this project is that the product requirements are already well-defined. The goal is to develop a tool focused specifically on evaluating and scoring password strength. There is no need to spend time on exploratory requirements activities given this narrowly focused tool. The requirements can be fully specified at the very beginning, in terms of detailed security rules, password criteria scoring, interface choices, and performance requirements. These requirements then drive the downstream processes in a structured way.

Another driver for choosing Waterfall is the ability to clearly estimate schedules and costs due to the linear execution. Because each phase, such as design, coding, and testing, is executed one after another, timelines and resource needs can be accurately predicted. This ensures the product roadmap is realistic and helps with planning. Relatedly, the assumed stability of requirements also fits the direct way this password checker will be built. Once documented, the requirements will remain largely static, requiring no complex, iterative development cycles.

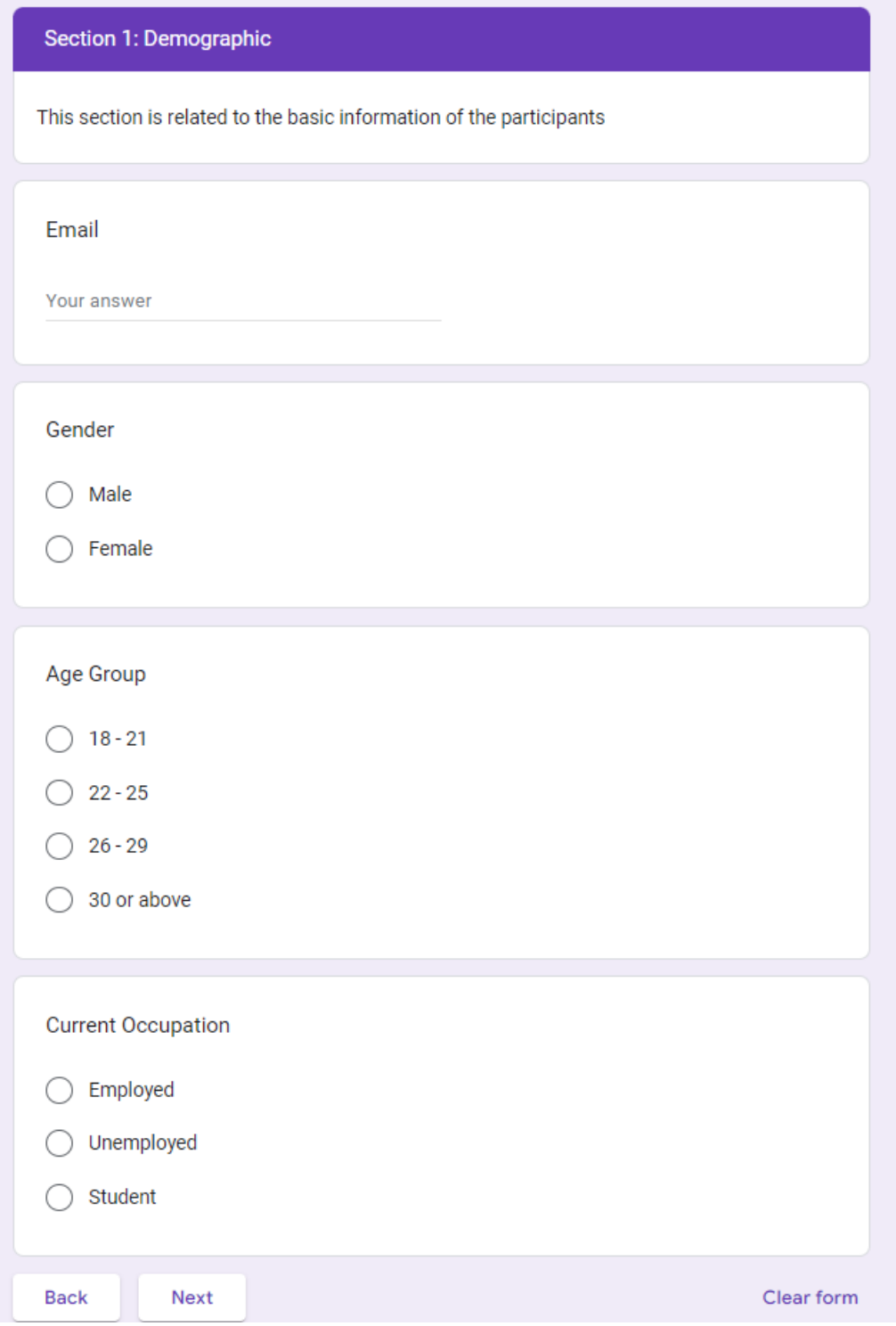
The phases begin with gathering all requirements related to capabilities, system interactions, security needs, and platform/language choices. These requirements are documented, reviewed, and approved before design commences. The next phase focuses on technical software and hardware designs that specify component breakdowns, interfaces, data flows, algorithms, architecture, and infrastructure. Code implementation adheres strictly to these completed

technical designs. Robust testing verifies all documented requirements and design elements, first through isolated unit testing, then integration testing, and finally system verification. This Waterfall methodology provides an appropriate, structured process for this password assessment project, aligning with understood requirements, and linear development approach suitable for the well-defined product goals.

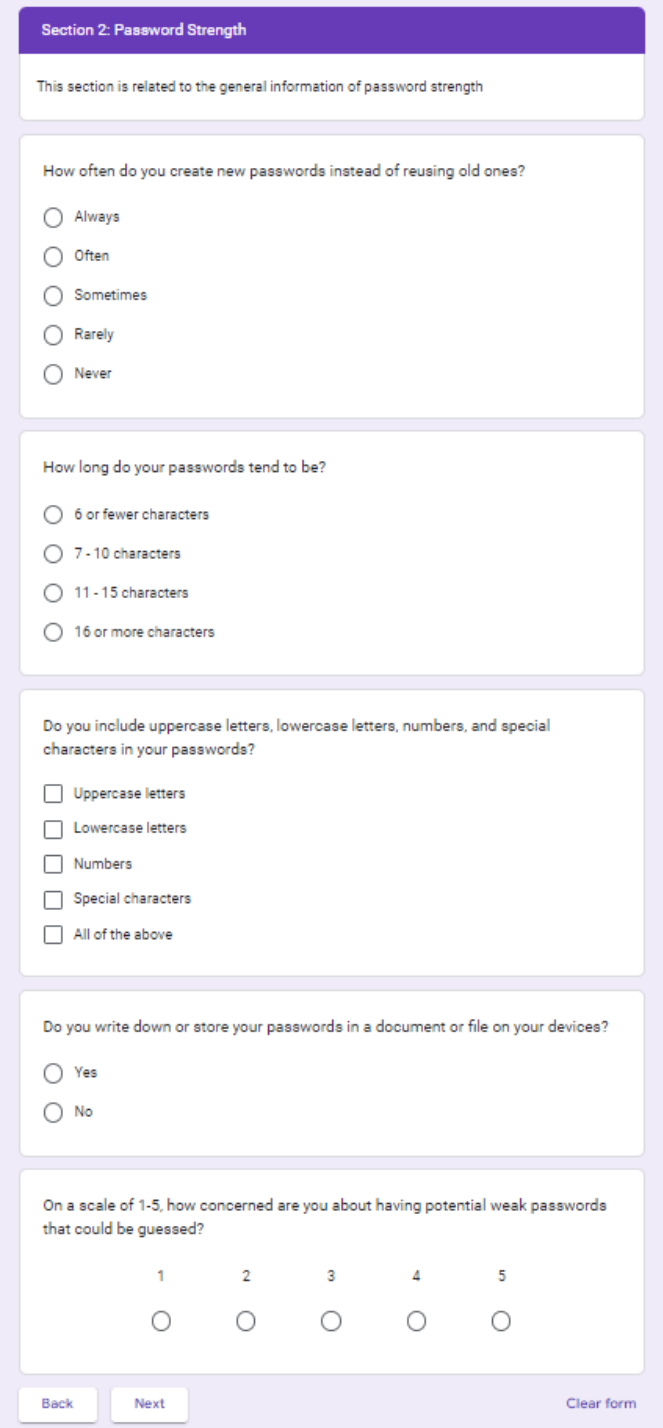
3.2 Data Gathering Design



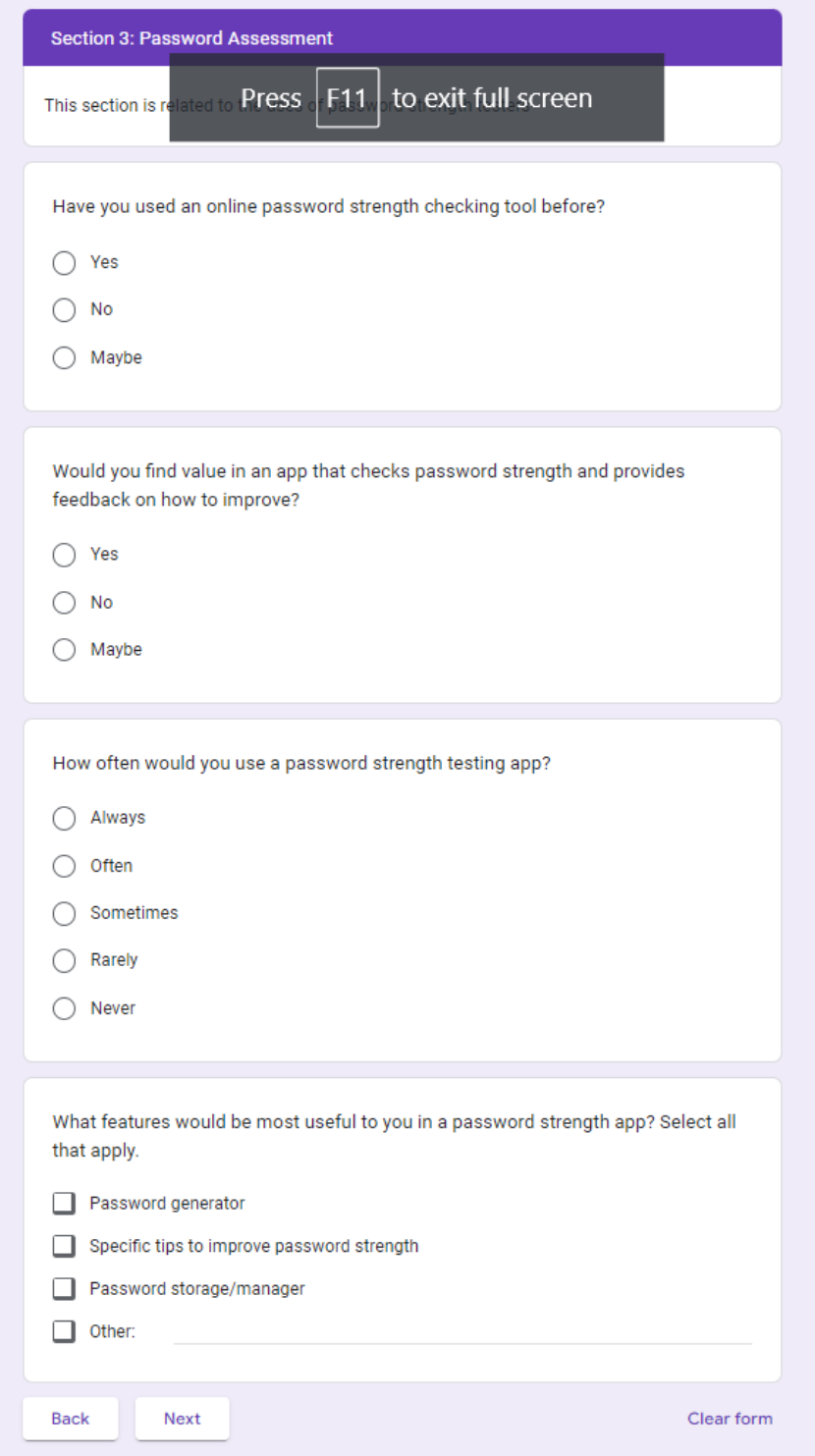
The introduction paragraph explained the purpose of conducting this questionnaire - to gather insights about people's password knowledge, attitudes, and habits to inform the development of a new password strength testing tool. It established the academic nature and voluntary participation aspect of the research.



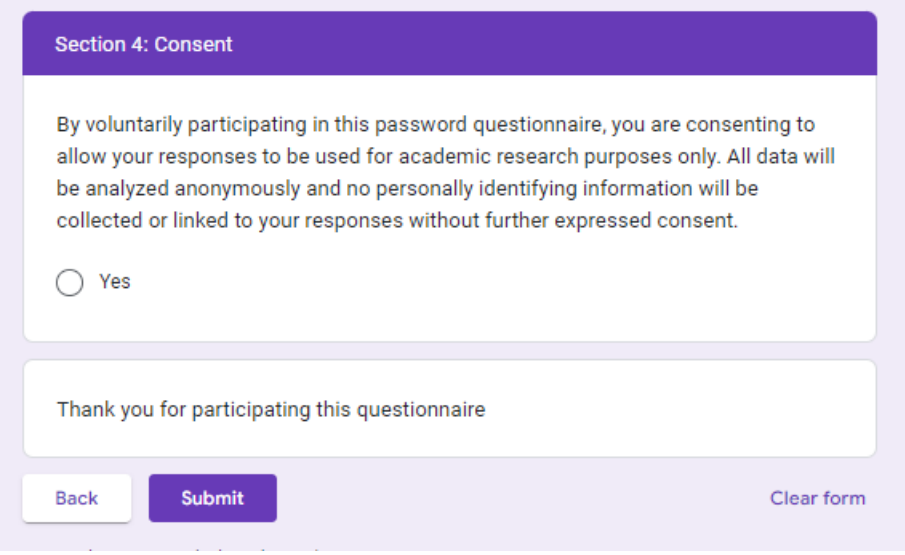
The demographics section with questions about age and occupation was included to facilitate analysis of any differences in password practices across groups. Understanding variances by factors like age could allow customization of the tool to match different user needs.



Five questions comprised the general password knowledge section. This covered self-reported behaviors like password reuse tendencies, typical password length and complexity used, saving passwords in files/documents, and overall concern about weak passwords. The goal was to benchmark general security awareness and gaps that could be addressed with an enhanced strength testing tool.

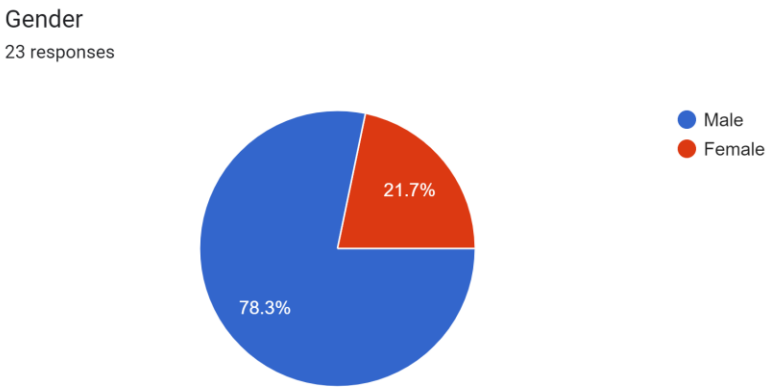


As the most directly relevant section, four questions focused specifically on receptiveness and desired features for a strength testing tool. This provided insights on tool necessity, frequency of potential usage, specific functionality preferences like password generation, and storage/manager.

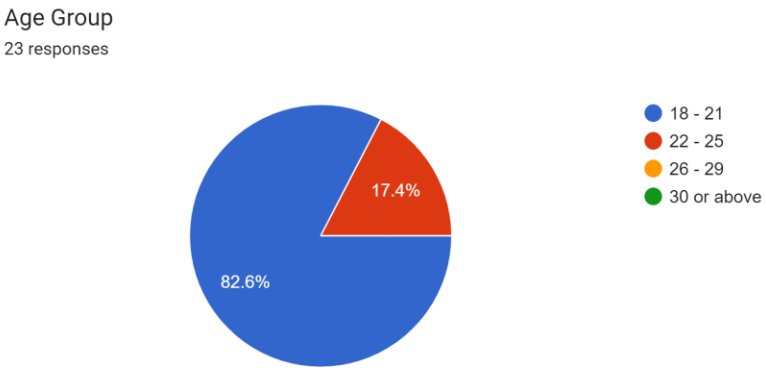


The consent section established voluntary participation, anonymity, minimal risks involved, option to withdraw, estimated time commitment and oversight contact details. Obtaining informed consent protects participant rights.

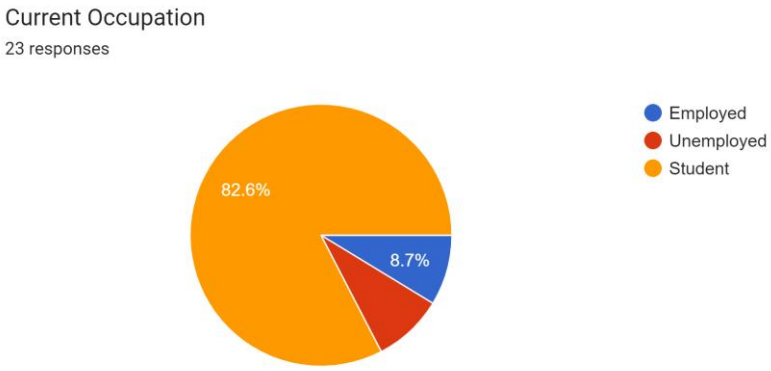
3.3 Analysis



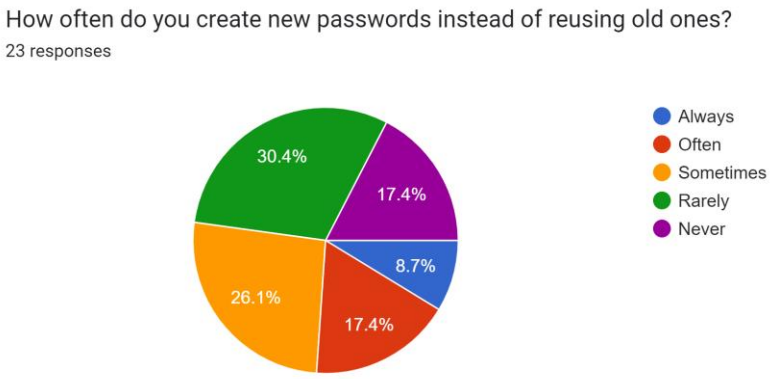
The questionnaire responses revealed that 78.3% of respondents were male. The significant overrepresentation of males provides an interesting insight. It could suggest that men more actively seek out tools to evaluate password strength, indicative of comparatively higher digital security awareness. However, the high percentage of male participants also introduces potential gender bias.



The age breakdown reveals the vast majority of responses came from either 18–21-year-olds (82.6%) or 22–25-year-olds (17.4%).

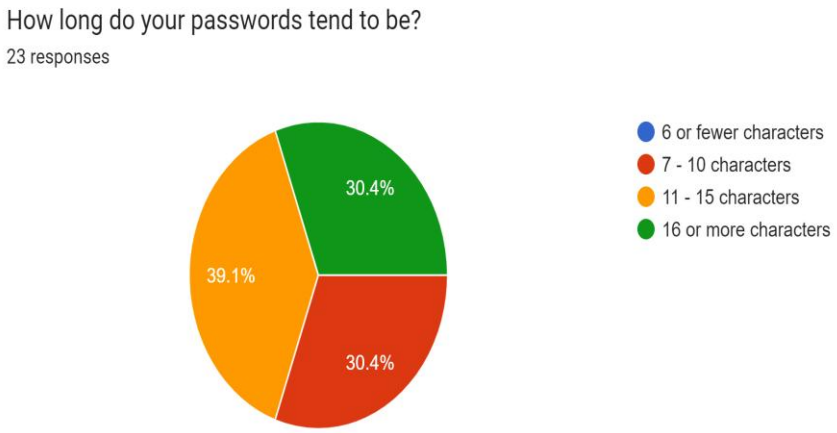


Aligned with the young age, students made up 82.6% of respondents, employed people comprised 8.7%, and the remaining subset was currently unemployed.



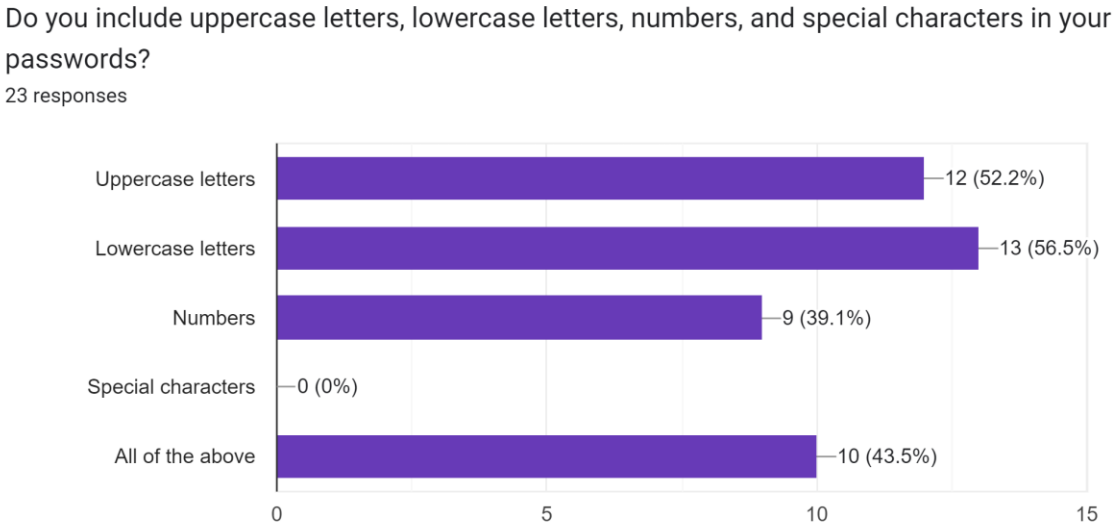
The responses reveal considerable concerning rates of password reuse rather than regular password refreshing, especially among such a tech-dependent demographic. The largest subset at 30.4% reported rarely creating new, unique passwords. A further 17.4% disturbingly never create new passwords at all, relying fully on recycling old logins for all accounts. Combined, close to half of participants demonstrated highly insecure tendencies by infrequently or never updating passwords.

On the more positive end, 26.1% sometimes changed passwords and 8.7% claimed to always use new, non-duplicated passwords across the accounts they set up. Interestingly, while less than 10% internally committed to best practices, 17.4% self-assessed as often creating fresh passwords. Overall, the widespread password reuse rates likely stem from perceived inconvenience around managing multiple unique logins. These quantitative results confirm poor practice baselines that urgently need addressing for younger users through remedial guidance.



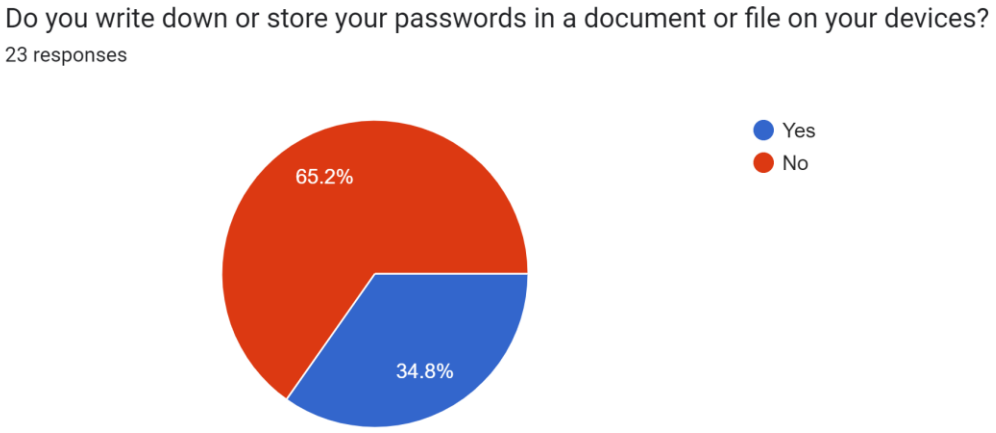
Fortunately, most respondents claimed to use reasonably strong password lengths of 11-15 characters (39.1%) or 16+ characters (30.4%). This aligns positively with the widespread embrace of longer passwords enabling greater complexity among younger demographics. However, 30.4% also acknowledged still sticking with weaker 7–10-character passwords vulnerable to quicker guessing.

Most concerningly, no one admitted to using dangerously short 6 or fewer character passwords. This potentially indicates some positive bias in self-reported behaviour though, especially considering the high password reuse rates simultaneously reported. Some participants may not wish to openly acknowledge clearly poor security habits on the survey even when granted anonymity.

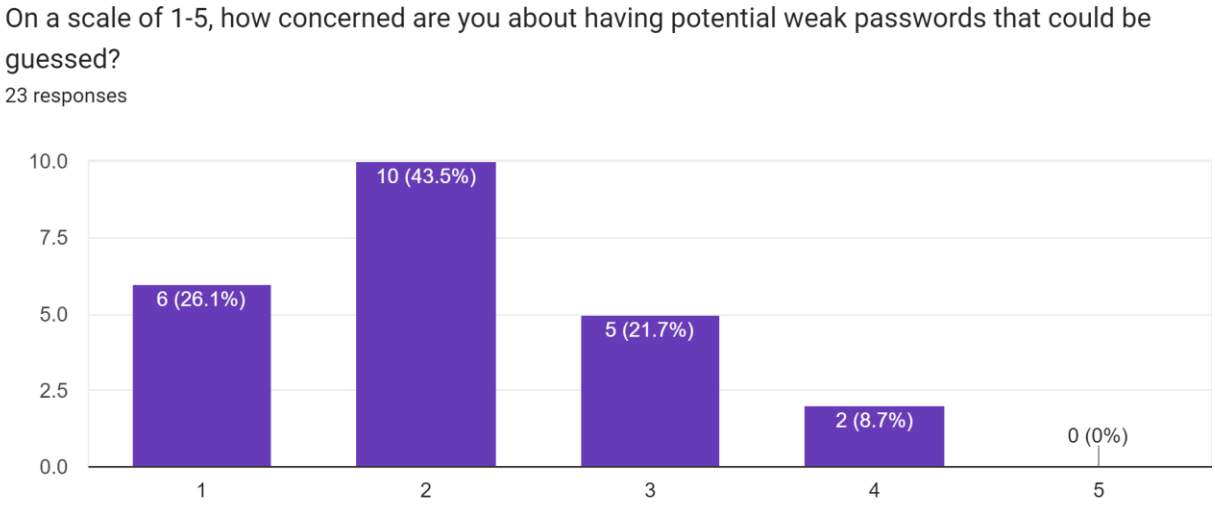


The data on inclusion of expanded password complexity elements proves concerning, as optimal practice involves combining uppercase, lowercase, numbers, and special characters for heightened security. However, no one claimed implementing the ideal combination. Just 43.5% came close, reporting attempting to incorporate all uppercase, lowercase, numbers, and special characters.

More respondents indicated including lowercase (56.5%) over uppercase letters (52.2%), alluding to the widespread abandonment of initial capitalization in informal messaging. Disconcertingly few leverage numbers (39.1%) often considered the easiest way to lengthen and strengthen passwords. And special characters see 0%, suggesting major perceived usability barriers. Overall, current complexity practices fall substantially short. The intention is there for many participants but not the understanding of vital special characters or tools to easily employ them.

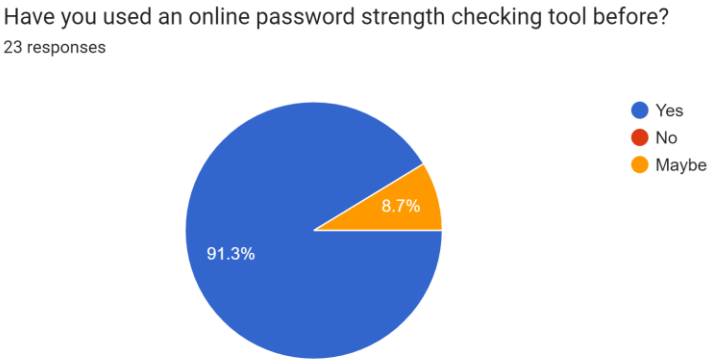


With 65.2% answering affirmatively about saving passwords in documents/files, most participants demonstrate dangerous practices jeopardizing account security despite increased reliance on digital access. This ties directly to the previously reported insights around rarely creating unique passwords and low diversity of special characters or case formats used.



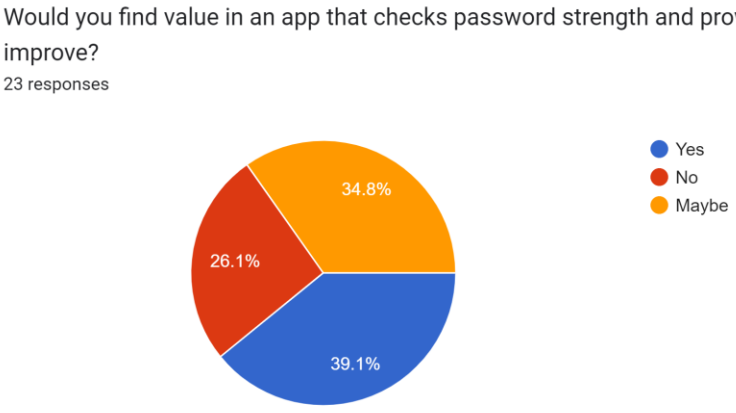
Worryingly, close to 70% of respondents registered only minimal concern about having hackable passwords, rating just 1-2 on a 5-point scale. 26.1% showed complete apathy, not worried whatsoever. This aligns to the previously outlined risky security behaviours including reusing passwords and saving them in plain text documents.

In contrast, only 8.7% expressed heightened concern, ranking a 4. And no participant showed extreme concern, or 5, on the scale. The apparent divide between actual password hygiene practices documented and degree of concern hints at a disconnect for younger digital natives.

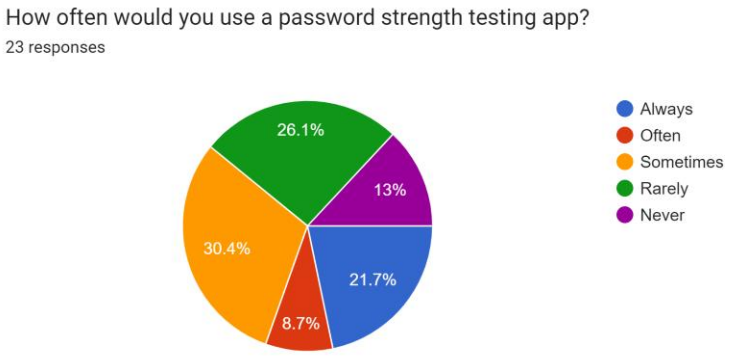


Promisingly, the vast majority at 91.3% indicate awareness and access of online tools available for checking password strength, saying yes to prior use. Just 8.7% expressed uncertainty, answering maybe. However, no one outright said they have not utilized a strength testing tool before.

Combining these statistics with the numerous unsafe password practices reported an apparent paradox emerges though. Participants claim utilizing checking tools yet simultaneously engage in easily avoidable behaviours like never changing passwords and saving them in plain text files. This implies the current solutions fail at motivating meaningful improvements once users exit the tool interfaces.

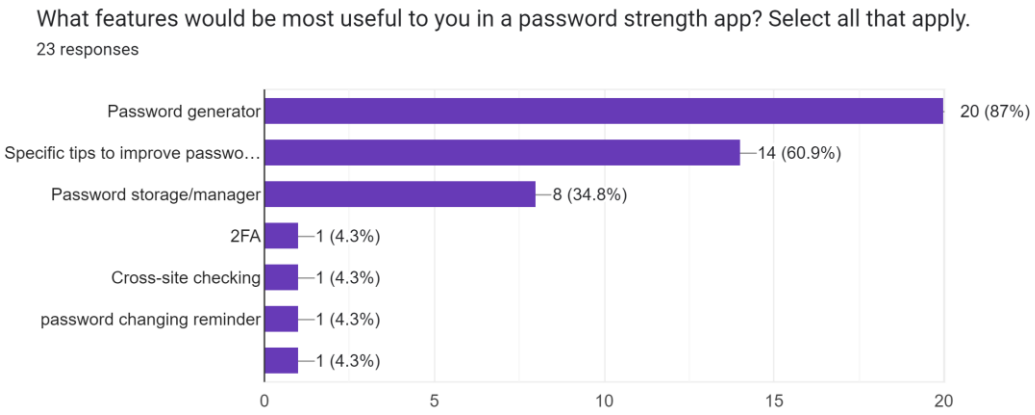


Intriguingly the responses split regarding openness towards a dedicated password strength testing and improvement application. Only 39.1% definitively saw value potential, answering yes, while 26.1% flat out said no. But 34.8% sat on the fence, expressing maybe interest in such an app dependent on specifics.



The largest segment at 30.4% see themselves interacting with a dedicated password testing application just sometimes, followed by 26.1% expecting rare use. However, 21.7% estimate they would use such an app quite consistently, selecting always. Just 8.7% aligned to significant but occasional use by choosing often for likely frequency.

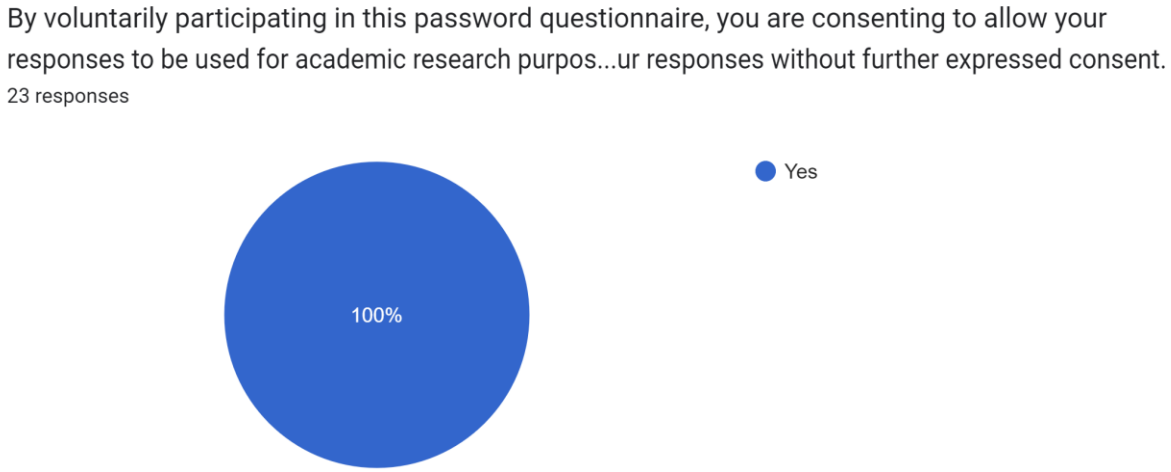
13% appear resistant, asserting they would never actually use a testing app regardless of core purpose or helpful features. These mixed results regarding prospective engagement suggest that both spreading awareness around utility for the resistant minority and ensuring seamless embedding in natural use flows for the intermittently interested majority stand as pivotal adoption factors.



The clear front runner feature with 87% interest is an integrated password generator to enable hassle-free creation of complex passwords, confirming earlier assumptions around desired convenience. Password storage management ranked substantially lower at 34.8%, likely due to existing reliance on insecure documents.

60.9% felt specific improvement tips would provide decent utility, suggesting receptiveness to coaching. Though based on engagement issues with current tools, proactive education may prove more effective than reactive suggestions only upon assessments. Surprisingly few opted for multifactor authentication or proactive changing reminder capabilities given security gaps identified.

The 4.3% who took initiative to manually specify other useful features championed innovations like cross-site duplicate checking and password change prompts. This shows a subset prioritizes more advanced protections but may still assume to get the baseline offerings in the suggested features without considering their absence.



Fortunately, 100% of respondents digitally signed the consent form to voluntarily participate under common academic research ethical guidelines. This helps validate capturing and reporting insights around potentially sensitive password practices and attitudes. Granting permission to record responses anonymously enables further statistical testing for observational trends.

CHAPER 4: DESIGN AND IMPLEMENTATION

4.1 Introduction

As we know it, the design and implementation of a system are two critical phases in the software development life cycle, and they play quite a crucial role in the successful delivery of a software system. To start off with design, it is the phase in the software development process where the overall architecture and structure of the software system are defined (Kovalenko, 2023). The design phase involves creating some sort of blueprint or a detailed written plan that outlines how to build the system and how the functionality will be presented. The design phase is also generally divided into two main stages, which are the high-level design and the low-level design.

Architectural design, or also known as a high-level design, focuses on defining the overall structure of the system, the components inside, and the interactions between them. This stage usually involves creating diagrams and models that represent the system's architecture, such as class diagrams, use-case diagrams, and system design diagrams (Sharma, 2024). The high-level design also acted as a suggestion towards addressing non-functional requirements, such as performance, security, and scalability of the system.

As for the low-level design, it involves specifying the internal structure and implementation details of each component or module within the system. This stage includes creating algorithms, data structures, and user interface designs (Pandey, 2024). Low-level design also involves defining the interfaces between components and determining how data will flow through the system.

The design phase is crucial because it ensures that the software system is well-planned and organized, making it easier to implement, maintain, and extend in the future. It is said that a well-designed system should be modular, flexible, and scalable, allowing for easier integration of new features or modifications as requirements change over time.

As for the implementation, it is the phase in the software development process where the design on paper is transformed into a proper working software system. It involves programmers writing

the actual code that will be implemented in the specified functionality in the design phase. The implementation phase typically follows a structured approach, with developers working on individual components or modules of the system.

During the implementation phase, developers will write the system's code in a chosen programming language, following coding standards and best practices. They also tend to integrate external libraries, frameworks, and online tools as needed to support the required functionality and enhance the development process. Testing is also an integral part of the implementation phase (Itexus, 2024). Developers often conduct unit tests to verify the correctness of the system's components or modules, ensuring that they work as expected before integrating them into the larger system. There is also performance testing of integration testing to ensure that the components work together seamlessly.

In the end, effective design and implementation are critical for the success of a software project. A well-designed system that follows best practices and adheres to industry standards is easier to implement and maintain. Proper implementation ensures that the software system meets the specified requirements, functional, and performs as expected. It is together that these two phases lay the foundation for a high-quality, reliable, and maintainable software product.

4.2 System Design Diagram

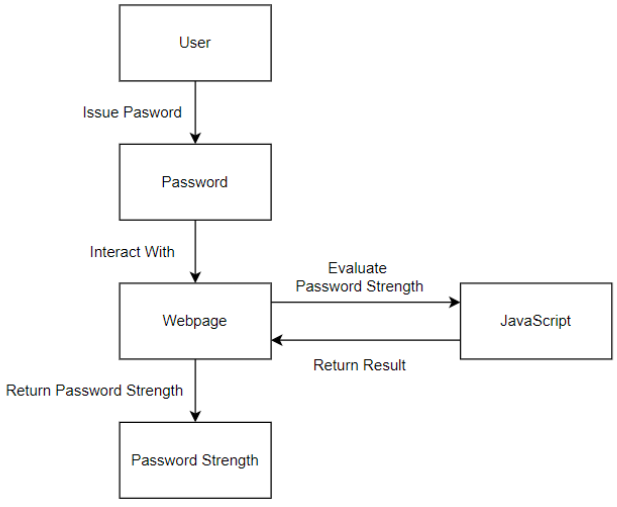


Figure 4.1: System Design Diagram

4.3 Use-Case Diagram

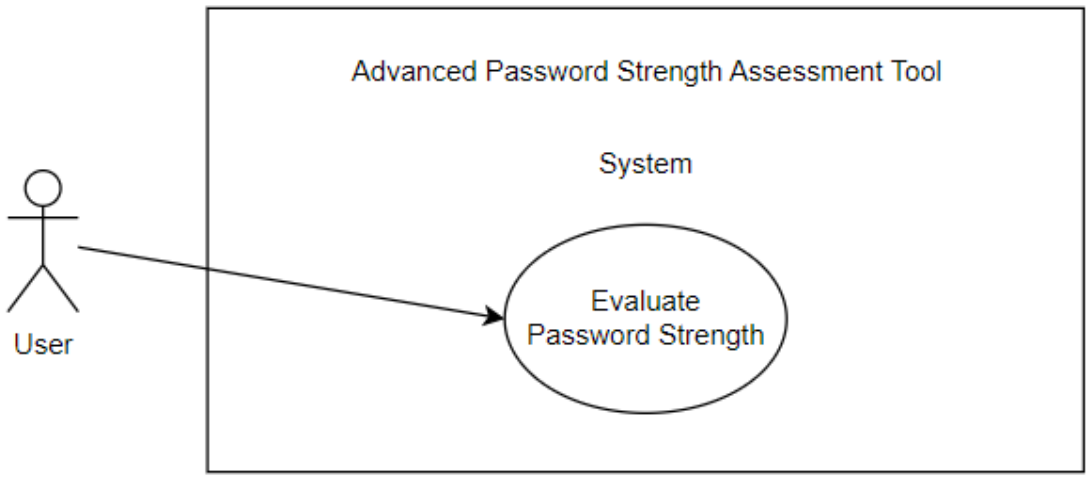


Figure 4.2: Use-Case Diagram

4.4 Use-Case Specifications

Use-Case Name	Evaluate Password Strength
Description	The process where user enter password into provided input field, and the system evaluate the strength of the password based on various criteria. Then display corresponding message indicating level of password strength
Actor	System
Priority	High
Status	Approved
Pre-conditions	The system is initiated and ready for user input
Post-conditions	The user is informed about the strength of the password through the displayed strength text message
Basic Flow	1. Users enter the password into input field 2. The system calculates the strength score of entered password 3. The system maps the calculated score to the strength's level based on predefined thresholds 4. The system displays the strength level message to the use
Alternative Flow	The system will display a strength text message indicating that the password is too short
Exception	None

Table 4.3: Use-Case Specifications

4.5 Class Diagram

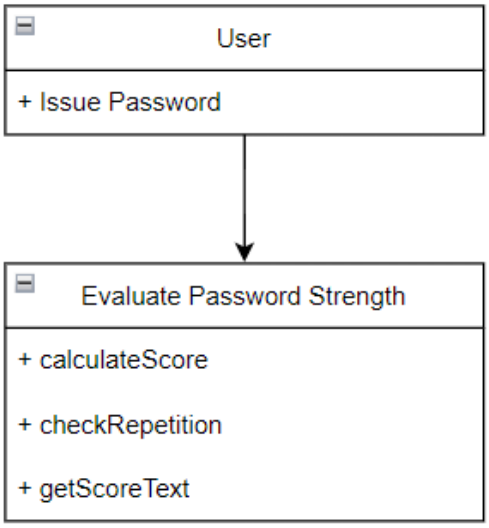


Figure 4.4: Class Diagram

4.6 Activity Diagram

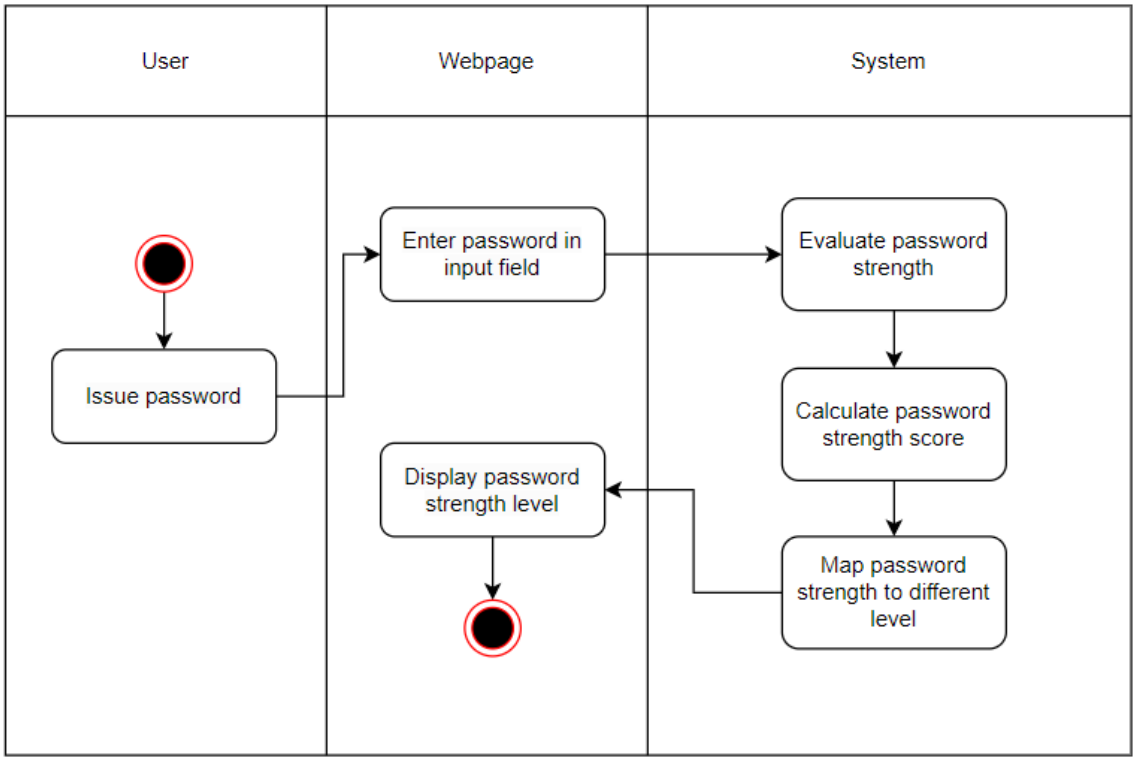


Figure 4.5: Activity Diagram

4.7 Sequence Diagram

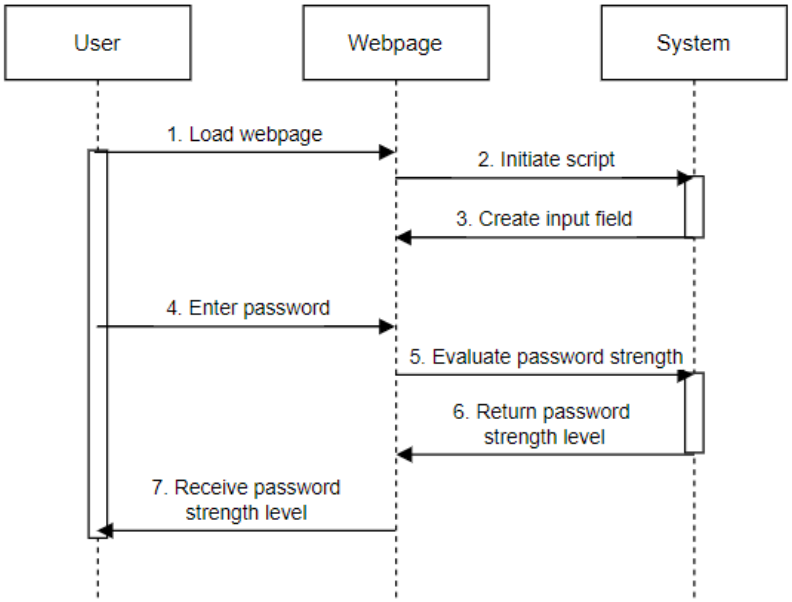


Figure 4.6: Sequence Diagram

4.8 Interface Design

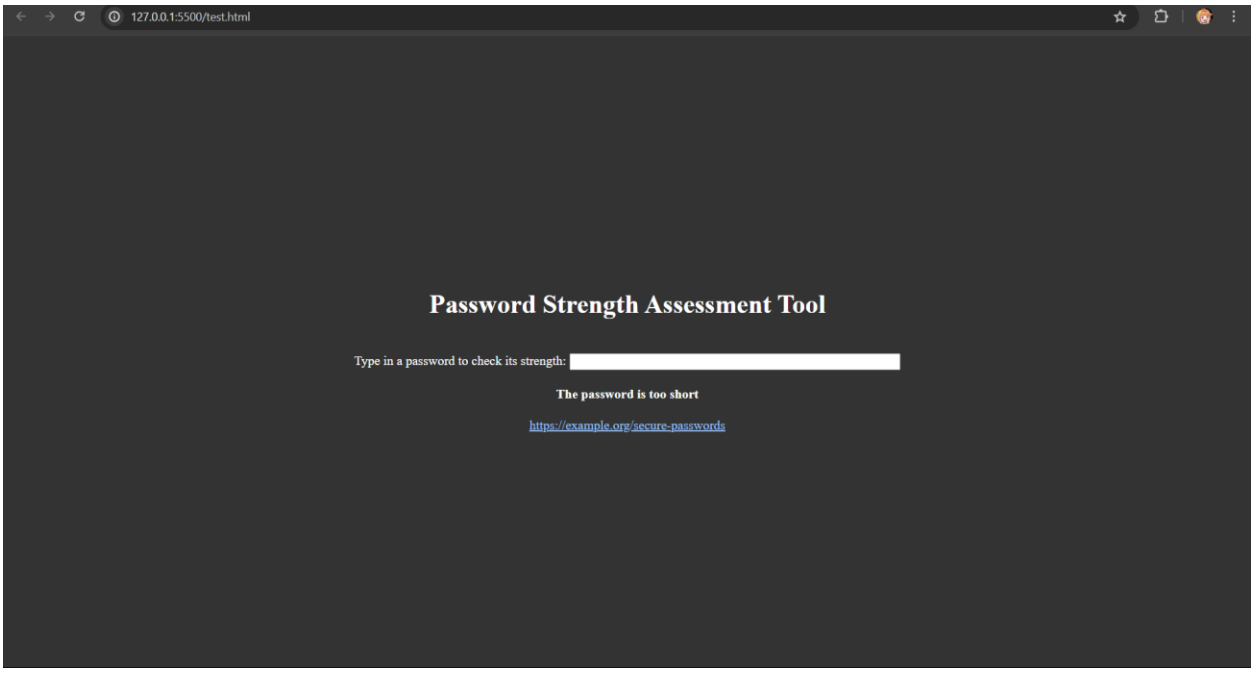


Figure 4.7: Interface Design

The figure above shows the main page of the running Password Strength Assessment Tool system. This page allows user to type in their password to check its strength. This page will also show the revolving links to useful password strength related sites.

4.9 Execution

The password strength assessment tool is a web-based application designed to help users create secure and robust passwords by evaluating password strength and providing feedback. The tool aims to raise awareness about password security practices and encourage users to adopt stronger passwords, thereby enhancing the overall security of their online accounts and digital assets.

The application is built using a combination of HTML, CSS, JavaScript, and the jQuery library. The front-end user interface is implemented using HTML and styled with CSS, providing a clean and intuitive layout for the password input field and the strength assessment feedback. The jQuery library is utilized to simplify DOM manipulation and event handling, allowing for efficient and cross-browser compatible code (Kinsta, 2023).

The core functionality of the password strength assessment is encapsulated within a JavaScript file, ‘password.js’. This file defines a jQuery plugin called ‘password’ that can be applied to any password input field on the web page. The plugin creates an instance of the ‘Password’ class, which is responsible for evaluating the strength of the entered password based on various criteria.

There are several implementations of methods in the ‘Password’ class to calculate the password strength score. The ‘calculateScore’ method considers factors such as password length, presence of repetitive characters, inclusion of numbers, symbols, uppercase and lowercase letters, and combinations of different character types. The score is then mapped to a corresponding strength text message using the ‘getScoreText’ method, which relies on predefined thresholds defined in the ‘steps’ object.

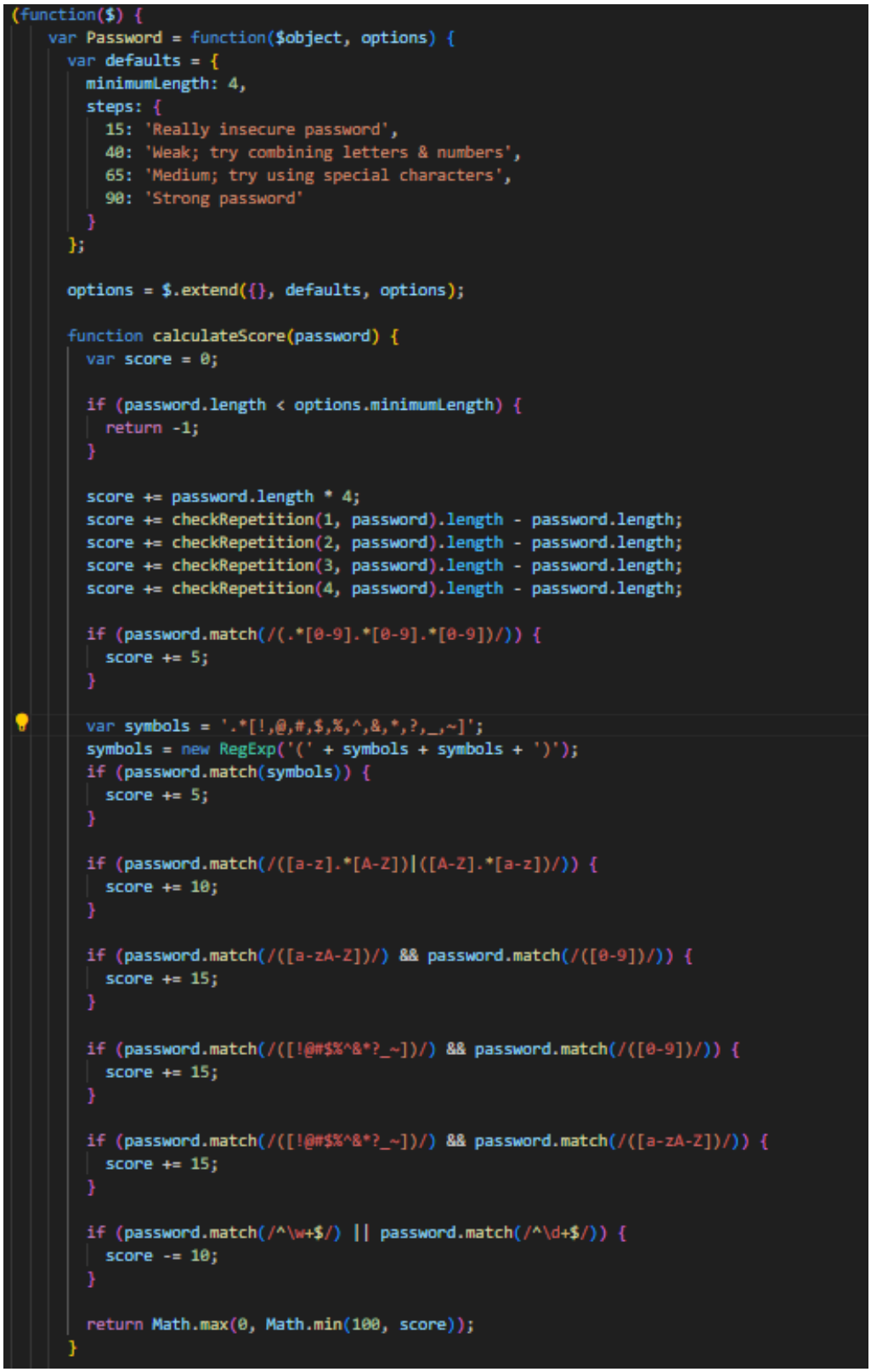
In addition to the core password strength assessment functionality, the application also includes an educational component. A revolving set of links to password security best practices and informative resources is displayed below the input field. These links cycle at a predefined interval, allowing users to explore and learn about effective password security practices.

Overall, the password strength assessment tool is a practical and educational application that aims to promote stronger password security practices among users. By providing real-time feedback and educational resources, the tool empowers users to create more robust passwords, thereby enhancing the security of their online accounts and protecting their digital assets from unauthorized access.

4.10 System Screenshot

```html
<!DOCTYPE html>
<html>
<head>
    <title>Password Strength Assessment Tool</title>
    <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
    <script src="1pass.js"></script>
    <style>
        body {
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
            background-color: #333;
            color: #fff;
        }
        .container {
            text-align: center;
        }
        input {
            width: 400px;
            margin-top: 20px;
            margin-bottom: 20px;
        }
        .pass-strength-text {
            font-weight: bold;
        }
        .revolving-text {
            margin-top: 20px;
        }
        .revolving-text a {
            color: #99c2ff;
            text-decoration: underline;
            cursor: pointer;
        }
    </style>
</head>
<body>
    <div class="container">
        <h1>Password Strength Assessment Tool</h1>
        <div>
            <label for="password">Type in a password to check its strength:</label>
            <input id="password" type="password" />
        </div>
        <div class="revolving-text"></div>
    </div>

    <script>
        $(document).ready(function() {
            $('#password').password();

            var links = [
                'https://example.com/password-tips',
                'https://example.org/secure-passwords',
                'https://example.net/password-best-practices'
            ];

            var currentIndex = 0;
            var $revolvingText = $('.revolving-text');

            function displayNextLink() {
                var link = links[currentIndex];
                $revolvingText.html('<a href="' + link + '" target="_blank">' + link + '</a>');
                currentIndex = (currentIndex + 1) % links.length;
            }

            setInterval(displayNextLink, 5000); // Change link every 5 seconds
        });
    </script>
</body>
</html>
```

Figure 4.8: HTML File



```
(function($) {
    var Password = function($object, options) {
      var defaults = {
        minimumLength: 4,
        steps: {
          15: 'Really insecure password',
          40: 'Weak; try combining letters & numbers',
          65: 'Medium; try using special characters',
          90: 'Strong password'
        }
      };

      options = $.extend({}, defaults, options);

      function calculateScore(password) {
        var score = 0;

        if (password.length < options.minimumLength) {
          return -1;
        }

        score += password.length * 4;
        score += checkRepetition(1, password).length - password.length;
        score += checkRepetition(2, password).length - password.length;
        score += checkRepetition(3, password).length - password.length;
        score += checkRepetition(4, password).length - password.length;

        if (password.match(/(.*[0-9].*[0-9].*[0-9])/)) {
          score += 5;
        }

        var symbols = '.*[!,@,#,$,%,^,&,*,?,_,~]';
        symbols = new RegExp('(' + symbols + symbols + ')');
        if (password.match(symbols)) {
          score += 5;
        }

        if (password.match(/([a-z].*[A-Z])|([A-Z].*[a-z])/)) {
          score += 10;
        }

        if (password.match(/([a-zA-Z])/) && password.match(/([0-9])/)) {
          score += 15;
        }

        if (password.match(/([!@#$%^&*?_~])/) && password.match(/([0-9])/)) {
          score += 15;
        }

        if (password.match(/([!@#$%^&*?_~])/) && password.match(/([a-zA-Z])/)) {
          score += 15;
        }

        if (password.match(/^\w+$/) || password.match(/^\d+$/)) {
          score -= 10;
        }

        return Math.max(0, Math.min(100, score));
      }
```

Figure 4.9: 1st Part of JavaScript File

```
    function checkRepetition(length, str) {
      var res = "", repeated = false;
      for (var i = 0; i < str.length; i++) {
        repeated = true;
        for (var j = 0; j < length && (j + i + length) < str.length; j++) {
          repeated = repeated && (str.charAt(j + i) === str.charAt(j + i + length));
        }
        if (j < length) {
          repeated = false;
        }
        if (repeated) {
          i += length - 1;
          repeated = false;
        } else {
          res += str.charAt(i);
        }
      }
      return res;
    }

    function getScoreText(score) {
      if (score === -1) {
        return 'The password is too short';
      }

      score = score < 0 ? 0 : score;

      var sortedStepKeys = Object.keys(options.steps).sort();
      for (var step of sortedStepKeys) {
        if (step > score) {
          return options.steps[step];
        }
      }

      return 'Strong password';
    }

    var $strengthText = $('<div>').addClass('pass-strength-text');
    $object.after($strengthText);

    $object.on('keyup', function() {
      var score = calculateScore($object.val());
      var text = getScoreText(score);
      $strengthText.text(text);
    });
  };

  $.fn.password = function(options) {
    return this.each(function() {
      new Password($(this), options);
    });
  };
})(jQuery);
```

Figure 4.10: 2nd Part of JavaScript File

4.11 Summary

The system I designed is a web-based application that follows a modular and object-oriented design approach, separating concerns between the user interface and the core application logic. The high-level design adopts a client-side architecture, with the user interface implemented using HTML and CSS, and the application functionality encapsulated within JavaScript files.

The low-level design of the user interface comprises an HTML structure with the necessary elements and placeholders for displaying content and user interactions. While the core application logic is implemented in a JavaScript class, which defines methods for handling the essential functionality, such as data processing, calculations, and user input validation. This class is designed to be reusable and extensible, following best practices in object-oriented programming.

The application logic is integrated into the web application through a JavaScript library or framework architecture. This architecture creates instances of the core class and attaches event listeners to the relevant user interface elements. As users interact with the application, the event handlers trigger the corresponding application logic, and the results are dynamically rendered within designated elements in the user interface.

To enhance the user experience and provide additional value, the application incorporates educational and informative components. These components can take the form of rotating content, such as links to relevant resources or best practices, displayed within designated areas of the user interface. These components can cycle at predefined intervals, encouraging users to explore and learn more about the application's subject matter.

CHAPTER 5: RESULT AND DISCUSSION

5.1 Introduction

A test plan is a detailed document that outlines the testing strategy, scope, objectives, and approach for ensuring the quality and correctness of a software system. It serves as a blueprint for the testing activities and helps ensure that all critical aspects of the system are thoroughly tested (BrowserStack, n.d.). In the context of the password strength assessment tool, I will be using 2 test plans of different techniques, a unit testing plan and a user acceptance testing plan. By combining these 2 test plans together, I can ensure that both the individual components and the overall system functionality are thoroughly tested, which will in the end increasing the likelihood of delivering a high-quality and reliable password strength assessment tool.

5.2 Unit Testing

A unit testing plan focuses on testing individual units or components of the system in isolation (SmartBear, n.d.). In the case of the password strength assessment tool, I will design the unit test to verify the correctness of the individual methods and functions within the system, such as the score calculations, the password plugin, and the password strength level display. Unit tests help ensure that each component works as expected before integrating it into the larger system.

Test Case ID	Test Case Name	Description	Expected Results	Actual Results	Status	Priority
1.1	Calculate Score (Valid Password)	Test the calculateScore method with a valid password	The method should return strength text message based on the defined thresholds	The method returns the strength text message based on the defined thresholds	Approved	High
1.2	Calculate Score (Invalid Password)	Test the calculateScore method with an invalid password (e.g., too short)	The method should return a “too short” message	The method returns a “too short” message	Approved	High

1.3	Initialize Password Plugin (Valid Input)	Test the initialization of the password plugin with a valid input field	The plugin should create an instance of the Password class and attach event listeners to the input field	The plugin creates an instance of the Password class and attach event listeners to the input field	Approved	High
1.4	Display Strength Text (Valid Password)	Test the display of the strength text with a valid password	The strength text should be displayed in the designated area with the correct message	The strength text is displayed in the designated area with the correct message	Approved	High
1.5	Display Strength Text (Invalid Password)	Test the display of the strength text with an invalid password	The strength text should be displayed in the designated area with the appropriate error message	The strength text is displayed in the designated area with the appropriate error message	Approved	High

Table 5.1: Unit Testing Plan

5.3 User Acceptance Testing

Another test plan I used is user acceptance testing (UAT), it is a type of testing that involves multiple end-user or representatives of the target audience. The goal of UAT is to validate that the system meets the specified requirements and functions as expected from the user's perspective (Setter, 2023). In the case of the password strength assessment tool, I would involve testing the overall user experience, including the user interface, password strength feedback, and educational resources in the UAT. This will helps ensure that the application is user-friendly, intuitive, and meets the intended goals and objectives.

Tester Name: Chan Cay Shen		Date: 21st April 2024				
Criteria		Please tick the box for a rating of 1 to 5 (✓)				
		1	2	3	4	5
1	User Interface Validation - the user interface elements are properly displayed and positioned - design is pleasing to the users					✓
2	Password Strength Feedback - the tool provides accurate feedback on password strength - weak password such as "password" will indicate as a weak or insecure password - strong password such as "Str0ngP@ssw0rd!" will indicate as a strong or secure password					✓
3	Educational Resources Display - the educational resource links are displayed and cycled appropriately - clicking on the educational resource links opens the respective resources					✓
Tester Comments		-				

Table 5.2: 1st UAT

Tester Name: Low Kit Xheng		Date: 21st April 2024				
Criteria		Please tick the box for a rating of 1 to 5 (✓)				
		1	2	3	4	5
1	User Interface Validation - the user interface elements are properly displayed and positioned - design is pleasing to the users				✓	
2	Password Strength Feedback - the tool provides accurate feedback on password strength - weak password such as "password" will indicate as a weak or insecure password - strong password such as "Str0ngP@ssw0rd!" will indicate as a strong or secure password					✓
3	Educational Resources Display - the educational resource links are displayed and cycled appropriately - clicking on the educational resource links opens the respective resources				✓	
Tester Comments		-				

Table 5.3: 2nd UAT

Tester Name: Chan Khai Chung		Date: 23rd April 2024				
Criteria		Please tick the box for a rating of 1 to 5 (✓)				
		1	2	3	4	5
1	User Interface Validation - the user interface elements are properly displayed and positioned - design is pleasing to the users			✓		
2	Password Strength Feedback - the tool provides accurate feedback on password strength - weak password such as "password" will indicate as a weak or insecure password - strong password such as "Str0ngP@ssw0rd!" will indicate as a strong or secure password					✓
3	Educational Resources Display - the educational resource links are displayed and cycled appropriately - clicking on the educational resource links opens the respective resources				✓	
Tester Comments		The UI is simple.				

Table 5.2: 3rd UAT

5.4 System Testing and Discussion

I had the password strength assessment tool went through rigorous testing using a comprehensive unit testing plan and a user acceptance testing plan. I will be discussing about the execution and results of these test plans, while highlighting the key findings and outcomes.

The first technique, unit testing plan was executed to check on the correctness of each individual components and methods within the system. Overall, the unit testing plan yielded satisfactory results. Most of the test cases passed successfully, indicating that the core functionality of the system was implemented correctly.

However, it is unfortunately that a minor issue was spotted during the unit testing process. It was in the initial of the testing phase, the implementation of the ‘password’ plugin was not able to handle invalid input scenarios correctly, which result in exceptions being thrown. But this issue was quickly resolved by adding proper error handling and validation checks.

The second technique, the user acceptance testing plan aimed to validate the application from the end-user's perspective, the test cover aspects such as user interface, password strength feedback, and educational resources. I was able to receive 3 results, and these test plan yielded positive results with most of the test cases passing with a full mark. The end-users found the user interface intuitive and visually appealing, and the password strength feedback was accurate and helpful in creating secure passwords.

5.6 Summary

After implementing both the unit testing plan and the user acceptance testing plan, I can understand that unit testing plan was focused on verifying the correctness of individual components and methods within the system. It covered various aspects of the password strength assessment functionality. The execution of the unit testing plan revealed a minor issue, but the issue was promptly addressed, and the same test case were updated and re-executed to ensure successful completion.

The user acceptance testing plan on the other hand was aimed to validate the application from the end-user's perspective, encompassing aspects such as user interface, password strength feedback, and educational resources. This user acceptance testing phase involved representative end-users, who provided valuable feedback on their experience with the application.

Overall, the execution of both the unit testing plan and the user acceptance testing plan played a crucial role in my project since it helps ensuring the quality and reliability of the password strength assessment tool. The identified issues were deal with, and the necessary improvements were implemented, resulting in a more robust and user-friendly application.

CHAPTER 6: CONCLUSION

6.1 Critical Evaluation

The Advanced Password Strength Assessment Tool project has successfully achieved its primary objective of developing a user-friendly application for individuals to create and maintain robust passwords. It is the implementation of advanced algorithms and using innovative approaches, that this tool can finally provide accurate evaluations of password strength, which will definitely help in addressing a critical aspect of cybersecurity in this cyber age.

I can safely say that one of the project's most notable strengths lies in its comprehensive approach to password assessment. Unlike many existing online solutions or tools that only rely on fundamental length and complexity checks, this tool I employ have sophisticated pattern matching techniques and entropy calculations to identify a wide array of predictable password patterns, making sure of a thorough evaluation of password strength.

Furthermore, the project's emphasis is also a part on heighten user education. By integrating online educational resources and best practices within the tool, users are encouraged to actively learn and adopt secure password habits. Not only does this approach enhance the immediate impact of the tool but it also cultivates a long-term culture of cybersecurity awareness among users of all ages.

6.2 Limitation

While this current project of mine has achieved significant milestones, it is still essential to acknowledge its limitations. I found out the one constraint lies in the scope of the target audience, as the tool I designed is primarily utilized by individual users rather than the whole enterprises or organizations. Consequently, advanced features such as account login, centralized credential management or group policy enforcement are not incorporated, limiting its applicability in larger-scale deployments.

I also located another potential limitation revolves around the computational demands of the algorithms inside the advanced password strength assessment overtime. In theory, if the tool

gains widespread adoption and is used too many times, the computational overhead associated with processing vast quantities of passwords may become a bottleneck, potentially affecting the system's performance and scalability.

6.3 Recommendation

It is true that the Advanced Password Strength Assessment Tool has immense potential for further enhancement and expansion in future iterations. One key recommendation I obtained is to adapt the tool's functionality to cater to the unique needs of enterprises and organizations, broadening its applicability beyond individual users. This could involve incorporating features such as login, centralized credential management, role-based access controls, and even integration with existing identity and access management systems. By catering to enterprise-level requirements, the tool can become a comprehensive solution for password security across diverse organizational contexts.

Another crucial recommendation is performance optimization. As the tool has been adopted to the world for a long time, the computational demands associated with processing vast quantities of passwords may become a choke point, potentially affecting the system's performance and scalability. To address this, continually optimizing the computational efficiency of the password strength assessment algorithms is imperative. This could involve exploring parallel processing techniques, leveraging graphics processing units (GPUs), or implementing distributed computing architectures to handle large-scale password processing loads efficiently.

Incorporating contextual awareness into the password strength assessment process could also yield more tailored and relevant feedback. By considering factors such as the intended use case for example, creating financial accounts, social media, and corporate systems, the tool could provide customized recommendations for different users and diverse guidelines that aligned with industry-specific best practices, enhancing its value and relevance across diverse domains.

Furthermore, I can try to implement machine learning techniques to analyze password breach data and study evolving cybersecurity trends to enable the tool to continuously refine its algorithms and adapt to new emerging threats. This approach would ensure that the password

strength level assessments remain relevant and effective in the ever-changing landscape of cybersecurity, making it the future-proof tool solution at the forefront of password security.

It is by addressing these recommendations, the Advanced Password Strength Assessment Tool can continue to evolve, maintaining its position as a cutting-edge solution in the realm of password security and contributing to the broader goal of fostering a secure and resilient digital infrastructure.

REFERENCES

Alexander, Z. (2018, October 21). Is Microsoft's "password checker" a reliable tool to test the strength of your password?: Alexander's blog. Alexander's Blog | Sharing knowledge with the global IT community since November 1, 2004. https://www.zubairalexander.com/blog/is-microsofts-password-checker-a-reliable-tool-to-test-the-strength-of-your-password/

Atlassian. (n.d.). Waterfall methodology for project management. https://www.atlassian.com/agile/project-management/waterfall-methodology

BrowserStack. (n.d.). *What is a test plan: Importance, components, how to create test plan*. https://www.browserstack.com/test-management/features/test-run-management/what-is-test-plan

California, S. E. U. of, Egelman, S., California, U. of, California, S. J. U. of, Jain, S., Rebecca S. Portnoff University of California, Portnoff, R. S., Google, K. L., Liao, K., Google, Google, S. C., Consolvo, S., California, D. W. U. of, Wagner, D., University, A. S., University, G.-C., University, P., & Metrics, O. M. A. (2014, November 1). Are you ready to lock?: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM Conferences. https://dl.acm.org/doi/abs/10.1145/2660267.2660273

Groeneveld, R. (2022, October 17). The password problem. Nomios Group. https://www.nomios.com/news-blog/password-problem/

Itexus. (2024, March 19). *Implementation phase in SDLC*. https://itexus.com/glossary/implementation-phase-in-sdlc/

Kinsta. (2023, September 11). *What is jQuery? A look at the web's most-used JavaScript library*. https://kinsta.com/knowledgebase/what-is-jquery/

Kovalenko, O. (2023, February 21). *SDLC design phase: Definition, activities, goals*. IDAP Blog. https://idapgroup.com/blog/sdlc-design-phase/

Literature review. The University of Edinburgh. (2020, August 23). https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review

Pandey, S. (2024, March 27). *What is Low Level Design?*. Code 360. https://www.naukri.com/code360/library/what-is-low-level-design

Setter, M. (2023, October 20). *What is user acceptance testing (UAT): Meaning, definition*. Usersnap Blog. https://usersnap.com/blog/user-acceptance-testing-right/

Sharma, A. (2024, February 19). *What is high level design*. PrepBytes Blog. https://www.prepbytes.com/blog/system-design/what-is-high-level-design/

SmartBear. (n.d.). *What is unit testing?* https://smartbear.com/learn/automated-testing/what-is-unit-testing/

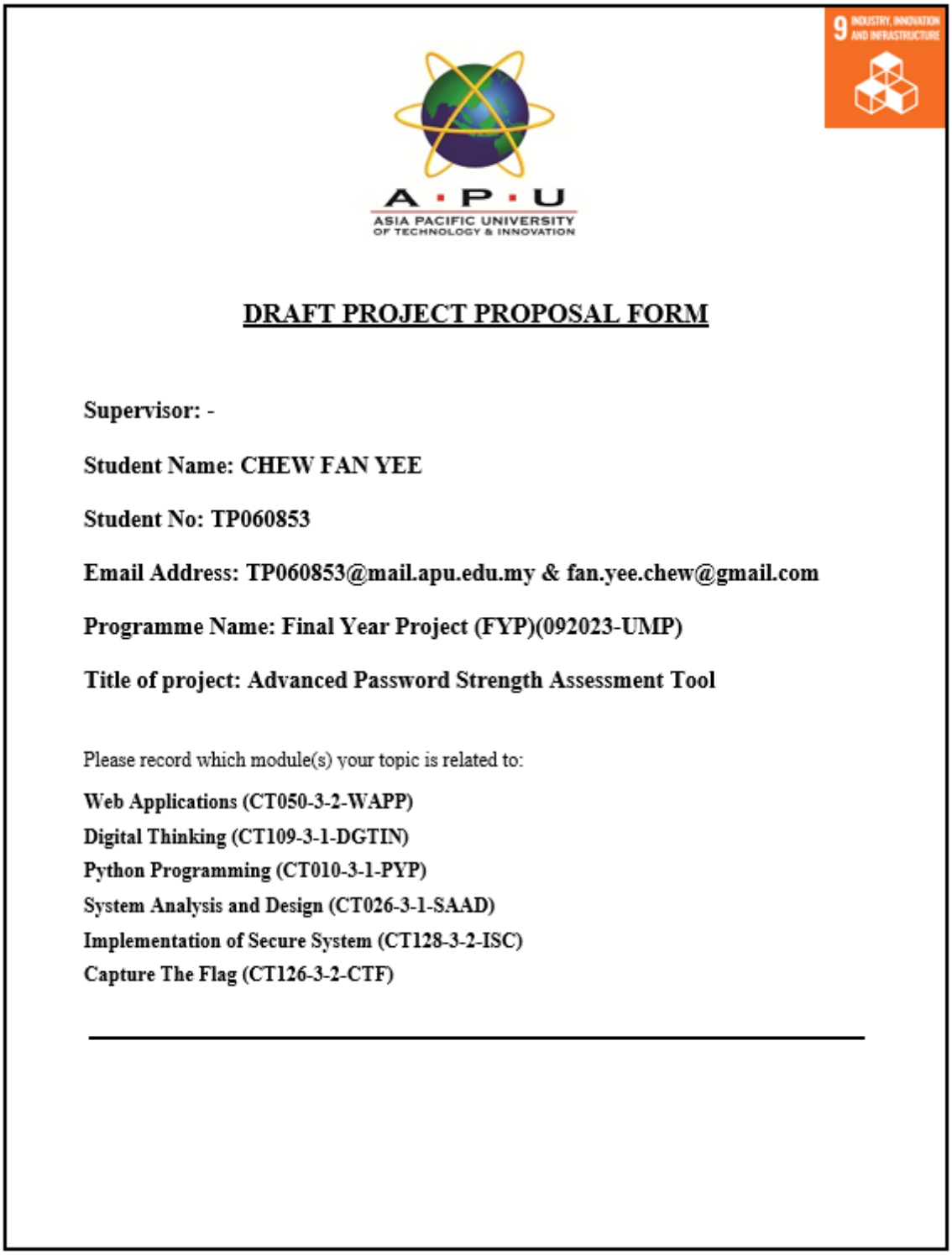
The consequences of weak banking passwords. Australian Mutual Bank. (2023, June 6). Retrieved September 16, 2023, from https://australianmutual.bank/news-blog/articles/consequences_of_weak_passwords/

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., & Cranor, L. F. (n.d.). How does your password measure up? the effect of strength meters on password creation. USENIX. Retrieved October 29, 2023, from https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur

Wheeler, D. L. (2016, August 10). Zxcvbn: Low-Budget Password Strength Estimation. USENIX. Retrieved November 12, 2023, from https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler

APPENDIX

PPF – Title Registration Proposal



A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

DRAFT PROJECT PROPOSAL FORM

Supervisor: -

Student Name: CHEW FAN YEE

Student No: TP060853

Email Address: TP060853@mail.apu.edu.my & fan.yee.chew@gmail.com

Programme Name: Final Year Project (FYP)(092023-UMP)

Title of project: Advanced Password Strength Assessment Tool

Please record which module(s) your topic is related to:

Web Applications (CT050-3-2-WAPP)
Digital Thinking (CT109-3-1-DGTIN)
Python Programming (CT010-3-1-PYP)
System Analysis and Design (CT026-3-1-SAAD)
Implementation of Secure System (CT128-3-2-ISC)
Capture The Flag (CT126-3-2-CTF)

1. Introduction

In today's digital landscape, where technology permeates nearly every aspect of our lives, the need for robust cybersecurity measures has never been more critical. Passwords are the first line of defence against unauthorized access to sensitive information, and their strength directly impacts our online security. Yet, the alarming reality is that a significant portion of the global population continues to use weak or easily guessable passwords, leaving them vulnerable to cyber threats.

The sector of business and industry we are concerned with in this project is the rapidly evolving landscape of cybersecurity. With the increasing frequency and sophistication of cyberattacks, individuals and organizations alike must adopt proactive measures to safeguard their digital assets. This is where this project comes into play.

Weak passwords pose a substantial risk to personal and organizational security. Breaches of sensitive data can lead to financial losses, identity theft, and even compromise the privacy and safety of individuals and communities (Groeneveld, 2022). Addressing this issue is not just a matter of convenience; it is a fundamental aspect of digital citizenship in today's interconnected world.

In line with the 9th Sustainable Development Goal (SDG), "Industry, Innovation and Infrastructure", this project is a testament to the power of innovation in the realm of cybersecurity. By providing a user-friendly, efficient, and accessible means to assess password strength, well aiming for the contribution to a safer digital environment. Stronger passwords, in turn, help fortify the infrastructure of digital systems and protect individuals and organizations from potential threats.

To successfully develop and implement this project, I will undertake comprehensive research in the following areas such as practices and standards for password security, existing assessment methods and algorithms for password strength. By addressing these research areas, I aim to create an innovative solution that not only empowers individuals to protect their digital identities

but also contributes to the broader goal of building secure, innovative, and resilient digital infrastructure in line with the 9th SDG.

2. Problem Statement

In the digital age, the security of personal and organizational data hinges on the strength of passwords, yet despite the growing awareness of cybersecurity risks, the majority of users still struggle to create and maintain strong passwords. AustralianMutualBank (2023) stated that the core issue lies in the users' knowledge, motivation, and effort, which are often insufficient to generate passwords that can withstand modern cyber threats. Existing research has identified several challenges related to password security:

1. User Knowledge Gap

   One significant challenge in password security is the gap in user knowledge. Many users hold the misconception that password strength solely depends on complexity, often equating it with a jumble of letters, numbers, and special characters. This misunderstanding can lead to the creation of passwords that are difficult to remember and prone to errors. Moreover, users often lack clear guidance on what truly makes a password strong, including factors like length, uniqueness, and unpredictability.

2. User Motivation

   User motivation is another hurdle in password security. Often, users prioritize convenience over security. Remembering complex passwords for numerous accounts can be burdensome, prompting individuals to opt for simpler, more easily memorable passwords. Additionally, some users underestimate the potential risks associated with weak passwords, assuming that they are unlikely targets for cyberattacks.

3. User Effort

   The effort required to create and manage strong passwords is a significant challenge. Maintaining unique, strong passwords for each account can be time-consuming, particularly when individuals have numerous accounts to oversee. The constant need to

change passwords and manage them effectively can lead to "password fatigue," where users become overwhelmed and may resort to reusing passwords or using weak ones.

4. Password Reuse

   Password reuse is a widespread practice and a major security concern. Many users reuse passwords across multiple accounts for the sake of simplicity and convenience. Unfortunately, this practice greatly amplifies the potential impact of a security breach. When one password is compromised, it can grant unauthorized access to multiple accounts, magnifying the security risks (Josh, 2022).

5. Cybersecurity Threats

   The ever-evolving landscape of cybersecurity threats presents a persistent challenge. Cybercriminals continually develop new methods and technologies to crack passwords, including brute force attacks, dictionary attacks, and advanced cracking software. These threats necessitate constant adaptation of password practices. Moreover, the prevalence of data breaches has led to vast databases of compromised passwords being available on the dark web. Cybercriminals can leverage these databases to launch attacks against accounts that reuse passwords, further highlighting the need for improved password security practices.

The proposed project builds upon and complements the existing body of work in the field of password security. Notably, previous research has primarily focused on educating users about password best practices and recommending complex password creation rules. While these efforts have been valuable in raising awareness, they have not fully addressed the challenges of user knowledge, motivation, and effort.

This project takes a novel approach by providing users with a tangible tool to evaluate their password strength comprehensively. It goes beyond prescribing password complexity rules and instead empowers users with real-time feedback and suggestions tailored to their unique

passwords. By bridging the gap between theoretical knowledge and practical implementation, this project aims to address the root causes of weak password security.

Furthermore, this project aligns with recent advancements in the field of cybersecurity that emphasize the importance of user-centric security solutions. Rather than solely relying on users to make informed decisions, the available tools will leverage innovative algorithms to objectively assess password strength, helping users make more informed choices.

In conclusion, while previous work has laid the foundation for password security awareness, the proposed project represents a significant step forward by offering a practical solution that directly addresses user knowledge, motivation, and effort concerns. By enhancing the user experience and promoting strong password practices, this project aims to contribute to a more secure digital environment in line with contemporary cybersecurity needs.

3. Project Aim and Objectives

The aim of this project is to develop a user-friendly and effective tool that empowers individuals to create and maintain strong passwords, thereby enhancing their digital security. This project strives to bridge the gap between user knowledge, motivation, and effort in password security. In alignment with the 9th SDG, the overarching goal is to contribute to the development of innovative solutions that bolster digital security and, by extension, support the broader objectives of a secure and resilient digital infrastructure.

The objectives of this project are:

1. To design and implement a user-friendly application for accessing password strength. The application will involve the creation of a user-centric interface.
2. To develop robust password strength assessment algorithms capable of providing accurate and real-time feedback by considering multiple factors such as password length, character diversity, predictability, and resistance to common cracking techniques.
3. To offer recommendations and tips to users for strengthening their passwords by developing a system that can ensure that users receive actionable advice relevant to their password's current state.
4. To educate users about practices of password security by integrating educational and informative resources to raise the awareness of the users.

4. Literature Review

Password security is a foundational element of digital life, yet it remains a persistent challenge for users. Weak passwords are a common vulnerability, often resulting from a lack of knowledge, motivation, and effort on the part of users. To address these issues, we can explore the "Advanced Password Strength Assessment Tool" project that is conceived as a user-friendly web/desktop application with the primary objective of helping users assess and improve the strength of their passwords. This tool aims to bridge the gap between user knowledge and password security by offering real-time feedback, personalized recommendations, and educational resources.

The application will operate by prompting users to input their passwords for assessment. It will employ advanced algorithms to evaluate password strength, taking into account factors such as length, character diversity, predictability, and resistance to common hacking techniques. The tool will then provide users with a detailed analysis of their password, including a strength score and actionable suggestions for improvement. Educational content will be integrated to inform users about password security best practices.

This project will offer a range of compelling benefits to users and the broader cybersecurity landscape. Firstly, it significantly improves password security by providing users with an accessible means to assess and enhance their passwords. By offering real-time feedback and tailored recommendations, it actively reduces the risk of unauthorized access and data breaches. Moreover, the tool empowers users by equipping them with knowledge and practical tools to safeguard their digital identities effectively. Beyond its functionality, the simplicity and user-friendliness of the interface ensure that individuals with varying technical backgrounds can easily access and utilize the application. In essence, the application serves as a valuable ally in the ongoing battle to fortify digital security.

Nulab (2023) stated that user motivation to engage with the "Advanced Password Strength Assessment Tool" stems from several key factors. Firstly, it allows users to actively assess and improve their passwords, fostering a sense of control over their digital security. The ability to gauge the strength of one's passwords and receive actionable guidance provides users with a

tangible means to enhance their cybersecurity posture. Furthermore, the inclusion of educational resources and insights into password security practices adds intrinsic value to the application. Users seeking to deepen their understanding of digital security will find the tool informative and empowering. Finally, the application's convenience, coupled with its user-friendly design, encourages regular usage as an integral component of users' routine cybersecurity practices.

The implementation strategy for this project encompasses several critical components. The core of the project involves the development of advanced password strength assessment algorithms capable of real-time analysis (Bitwarden, n.d.). These algorithms are the cornerstone of the application's ability to provide accurate feedback to users. Concurrently, user interface design plays a pivotal role in ensuring that users can intuitively navigate and engage with the tool. The interface will guide users through the assessment process seamlessly, making the experience both efficient and user-friendly. Additionally, the integration of educational content and interactive features within the application will require meticulous planning and execution to ensure that users gain valuable insights into password security practices. Finally, rigorous usability testing will be conducted to fine-tune the application, ensuring that it meets the diverse needs of users and functions optimally in practice. Together, these elements comprise a comprehensive implementation strategy that aims to create a powerful, user-centric, and effective tool for improving password security and promoting cybersecurity awareness.

The overarching purpose of the "Advanced Password Strength Assessment Tool" is to contribute to a more secure digital environment. It aligns with broader cybersecurity goals by addressing the root causes of weak password security practices. By providing users with the means to create and maintain strong passwords and by fostering awareness of best practices, the project supports the development of a secure and resilient digital infrastructure, ultimately contributing to the 9th SDG. In conclusion, this project is poised to make significant strides in enhancing password security, empowering users, and promoting cybersecurity awareness, which is a timely and critical mission in today's interconnected digital landscape.

5. Deliverables

The "Advanced Password Strength Assessment Tool" caters to individual users. It offers various functionalities and features tailored to the specific needs and objectives of each user, ultimately contributing to enhanced password security and cybersecurity awareness across different domains.

The "Advanced Password Strength Assessment Tool" will allow Individual Users:

- to assess the strength of their passwords and receive real-time feedback.
- to understand the weaknesses in their passwords and receive personalized recommendations to strengthen them.
- to access educational materials and resources about password security practices.
- to regularly monitor and enhance their password security in an accessible and user-friendly manner.

6. References

Groeneveld, R. (2022, October 17). The password problem. Nomios Group.
Retrieved September 16, 2023, from
https://www.nomios.com/news-blog/password-problem/

The consequences of weak banking passwords. Australian Mutual Bank. (2023, June 6).
Retrieved September 16, 2023, from
https://australianmutual.bank/news-blog/articles/consequences_of_weak_passwords/

Josh. (2022, April 4). 16 bad online habits you need to break today. All Things Secured.
Retrieved September 16, 2023, from
https://www.allthingssecured.com/tips/online-bad-habits-how-to-break-them/

Why password strength is crucial in Tech. Nulab. (2023, September 15).
Retrieved September 17, 2023, from
https://nulab.com/learn/software-development/password-strength/

Password strength testing tool. Bitwarden. (n.d.).
Retrieved September 17, 2023, from
https://bitwarden.com/password-strength/

Ethic Forms

Office Record	Receipt
Date Received: Received by whom:	Student name: CHEW FAN YEE Student number: TP060853 Received by: Date:

ACADEMIC RESEARCH ETHICS DISCLAIMER

Declaration about ethical issues and implications of research project/assignment proposals to be included on project/assignment application forms

Project/Assignment Title:

..... Advanced Password Strength Assessment Tool.....

.....

The following declaration should be made in cases where research project/assignment applicants for a particular project/assignment and the supervisor(s)/lecturer(s) for that project/assignment conclude that it is not necessary to apply for ethical approval for the research project/assignment.

We confirm that the University's guidelines for ethical approval have been consulted and that all ethical issues and implications in relation to the above project/assignment have been considered. We confirm that ethical approval need not be sought.

Chew Fan Yee	Chew	17-11-2023
Name of Research Project/Assignment Applicant	e-signature	Date
David Tan	David Tan	17-11-2023
Name of Research Project Supervisor/ Assignment Lecturer	e-signature	Date

Office Record	Receipt – Fast-Track Ethical Approval
Date Received:	Student name: CHEW FAN YEE Student number: TP060853
Received by whom:	Received by: Date:

APU / APIIT FAST-TRACK ETHICAL APPROVAL FORM (STUDENTS)

Tick one box (level of study):

☐ POSTGRADUATE (PhD / MPhil / Masters)

☑ UNDERGRADUATE (Bachelors degree)

☐ FOUNDATION / DIPLOMA / Other categories

Tick one box (purpose of approval):

☑ Thesis / Dissertation / FYP project

☐ Module assignment

☐ Other: _____

Title of Programme on which enrolled: B.SC. (HONS) IN COMPUTER SCIENCE (CYBER SECURITY)

Tick one box: ☑ Full-Time Study or ☐ Part-Time Study

Title of project / assignment: Advanced Password Strength Assessment Tool

Name of student researcher: CHEW FAN YEE

Name of supervisor / lecturer: Mr. DAVID TAN GEI KAR

Student Researchers- please note that certain professional organisations have ethical guidelines that you may need to consult when completing this form.

Supervisors/Module Lecturers - please seek guidance from the Chair of the APU Research Ethics Committee if you are uncertain about any ethical issue arising from this application.

		YES	NO	N/A
1	Will you describe the main procedures to participants in advance, so that they are informed about what to expect?	√		
2	Will you tell participants that their participation is voluntary?	√		
3	Will you obtain written consent for participation?	√		
4	If the research is observational, will you ask participants for their consent to being observed?	√		
5	Will you tell participants that they may withdraw from the research at any time and for any reason?	√		
6	With questionnaires and interviews will you give participants the option of omitting questions they do not want to answer?	√		
7	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	√		
8	Will you give participants the opportunity to be debriefed i.e. to find out more about the study and its results?	√		

If you have ticked **No** to any of Q1-8 you should complete the full Ethics Approval Form.

		YES	NO	N/A
9	Will your project/assignment deliberately mislead participants in any way?		√	
10	Is there any realistic risk of any participants experiencing either physical or psychological distress or discomfort?		√	
11	Is the nature of the research such that contentious or sensitive issues might be involved?		√	

If you have ticked **Yes** to 9, 10 or 11 you should complete the full Ethics Approval Form. In relation to question 10 this should include details of what you will tell participants to do if they should experience any problems (e.g. who they can contact for help). You may also need to consider risk assessment issues.

			YES	NO	N/A
12	Does your project/assignment involve work with animals?			√	
13	Do participants fall into any of the following special groups? **Note that you may also need to obtain satisfactory clearance from the relevant authorities**	Children (under 18 years of age)		√	
		People with communication or learning difficulties			
		Patients			
		People in custody			
		People who could be regarded as vulnerable			
		People engaged in illegal activities (eg drug taking)			
14	Does the project/assignment involve external funding or external collaboration where the funding body or external collaborative partner requires the University to provide evidence that the project/assignment had been subject to ethical scrutiny?			√	

If you have ticked **Yes** to 12, 13 or 14 you should complete the full Ethics Approval Form. There is an obligation on student and supervisor to bring to the attention of the APU Research Ethics Committee any issues with ethical implications not clearly covered by the above checklist.

STUDENT RESEARCHER

Provide in the boxes below (plus any other appended details) information required in support of your application, THEN SIGN THE FORM.

Please Tick Boxes

I consider that this project/assignment has no significant ethical implications requiring a full ethics submission to the APU Research Ethics Committee.	√
Give a brief description of participants and procedure (methods, tests used etc) in up to 150 words. The study will involve participants aged 18 and above, targeting a diverse demographic. A survey will be administered through social media platforms, ensuring voluntary participation. The questionnaire is designed to gather insights on participants' experiences with existing password assessment tools and assess their knowledge of password strength. To maintain confidentiality, the Google Form emphasizes the voluntary nature of participation, assuring respondents that their provided information will be kept confidential. The data collected will be anonymized and securely stored, complying with ethical standards and privacy regulations.	
I also confirm that: i) All key documents e.g. consent form, information sheet, questionnaire/interview are appended to this application. Or	
ii) Any key documents e.g. consent form, information sheet, questionnaire/interview schedules which need to be finalised following initial investigations will be submitted for approval by the project/assignment supervisor/module lecturer before they are used in primary data collection.	√

E-signature... ... ... Chew .... Print Name: CHEW FAN YEE Date: 9th November 2023

(Student Researcher)

Please note that any variation to that contained within this document that in any way affects ethical issues of the stated research requires the appending of new ethical details. New ethical consent may need to be sought.
The completed form (and any attachments) should be submitted for consideration by your Supervisor/Module Lecturer

SUPERVISOR/MODULE LECTURER
PLEASE CONFIRM THE FOLLOWING:

	Please Tick Box
I consider that this project/assignment has no significant ethical implications requiring a full ethics submission to the APU Research Ethics Committee	√
i) I have checked and approved the key documents required for this proposal (e.g. consent form, information sheet, questionnaire, interview schedule) Or	
ii) I have checked and approved draft documents required for this proposal which provide a basis for the preliminary investigations which will inform the main research study. I have informed the student researcher that finalised and additional documents (e.g. consent form, information sheet, questionnaire, interview schedule) must be submitted for approval by me before they are used for primary data collection.	√

SUPERVISOR AND SECOND ACADEMIC SIGNATORY

STATEMENT OF ETHICAL APPROVAL (please delete as appropriate)

1) **THIS PROJECT/ASSIGNMENT HAS BEEN CONSIDERED USING AGREED APU/SU PROCEDURES AND IS NOW APPROVED**

2) **THIS PROJECT/ASSIGNMENT HAS BEEN APPROVED IN PRINCIPLE AS INVOLVING NO SIGNIFICANT ETHICAL IMPLICATIONS, BUT FINAL APPROVAL FOR DATA COLLECTION IS SUBJECT TO THE SUBMISSION OF KEY DOCUMENTS FOR APPROVAL BY SUPERVISOR (see Appendix A)**

David Tan — David Tan — 17-11-2023

E-signature... ... ... Print Name... ... ... Date... ... ...
(Supervisor/~~Lecturer~~)

E-signature... ... ... Print Name... ... ... Date... ... ...
(Second Academic Signatory)

Office Record	Receipt – Appendix A (Fast-Track Ethics Form)
Date Received: Received by whom:	Student name: CHEW FAN YEE Student number: TP060853 Received by: Date:

APPENDIX A
AUTHORISATION FOR USE OF KEY DOCUMENTS

Completion of Appendix A is required when for good reasons key documents are not available when a fast track application is approved by the supervisor/module lecturer and second academic signatory.

I have now checked and approved all the key documents associated with this proposal e.g. consent form, information sheet, questionnaire, interview schedule

Title of project/assignment… …Advanced Password Strength Assessment Tool … … … … … … … …

… ……………………

Name of student researcher … Chew Fan Yee… … … … … … … … … … … … … … … … … …

Student ID: …TP060853…………………   Intake: … APU3F2308CS(CYB) … … … … … … … …

David Tan   David Tan   17-11-2023

E-signature… … … … … … … … … … … Print Name… … … … … … … … … … … … Date… … ……. …
(Supervisor/~~Lecturer~~)

Log Sheets

(APU: Serial Number)

PLS V1.0

Project Log Sheet – Supervisory Session

Notes on use of the project log sheet:

1. This log sheet is designed for meetings of more than 15 minutes duration, of which there must be at minimum SIX (6) during the course of the project (SIX mandatory supervisory sessions).
2. The student should prepare for the supervisory sessions by deciding which question(s) he or she needs to ask the supervisor and what progress has been made (if any) since the last session, and noting these in the relevant sections of the form, effectively forming an agenda for the session.
3. A log sheet is to be brought by the STUDENT to each supervisory session.
4. The actions by the student (and, perhaps the supervisor), which should be carried out before the next session should be noted briefly in the relevant section of the form.
5. The student should leave a copy (after the session) of the Project Log Sheet with the supervisor and to the administrator at the academic counter. A copy is retained by the student to be filed in the project file.
6. It is recommended that students bring along log sheets of previous meetings together with the project file during each supervisory session.
7. The log sheet is an important deliverable for the project and an important record of a student's organisation and learning experience. The student **must** hand in the log sheets as an appendix of the final year documentation, with sheets dated and numbered consecutively.

Student's name: CHEW FAN YEE **Date: 17th NOVEMBER 2023** **Meeting No: 1**

Project title: Advanced Password Strength Assessment Tool **Intake: APU3FS308CS(CYB)**

Supervisor's name: DAVID TAN **Supervisor's signature:** David Tan

Items for discussion (noted by student before mandatory supervisory meeting):

1. **Introduction**
2. **Request for ethic form signature**
3.
4.

Record of discussion (noted by student during mandatory supervisory meeting):

1.
2.
3.
4.

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1.
2.
3.

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.

Poster

Advanced Password Assessment Tool

Strong passwords are the first line of defense against cyber threats.

CHEW FAN YEE	TP060753	B.Sc. (Hons) Computer Science Specialism in Cyber Security

Supervisor: Mr. David Tan

Second Marker: Mr. Yogeswaran Nathan

Problem Statements:

- Weak passwords are a major vulnerability, leaving users susceptible to data breaches and identity theft.
- Many users lack knowledge of password security best practices.
- Managing multiple strong passwords across accounts is a significant burden.

Objectives:

- Develop a user-friendly application
- Implement advanced algorithms to evaluate passwords against various attack vectors.
- Educate users on effective password practices through integrated resources.

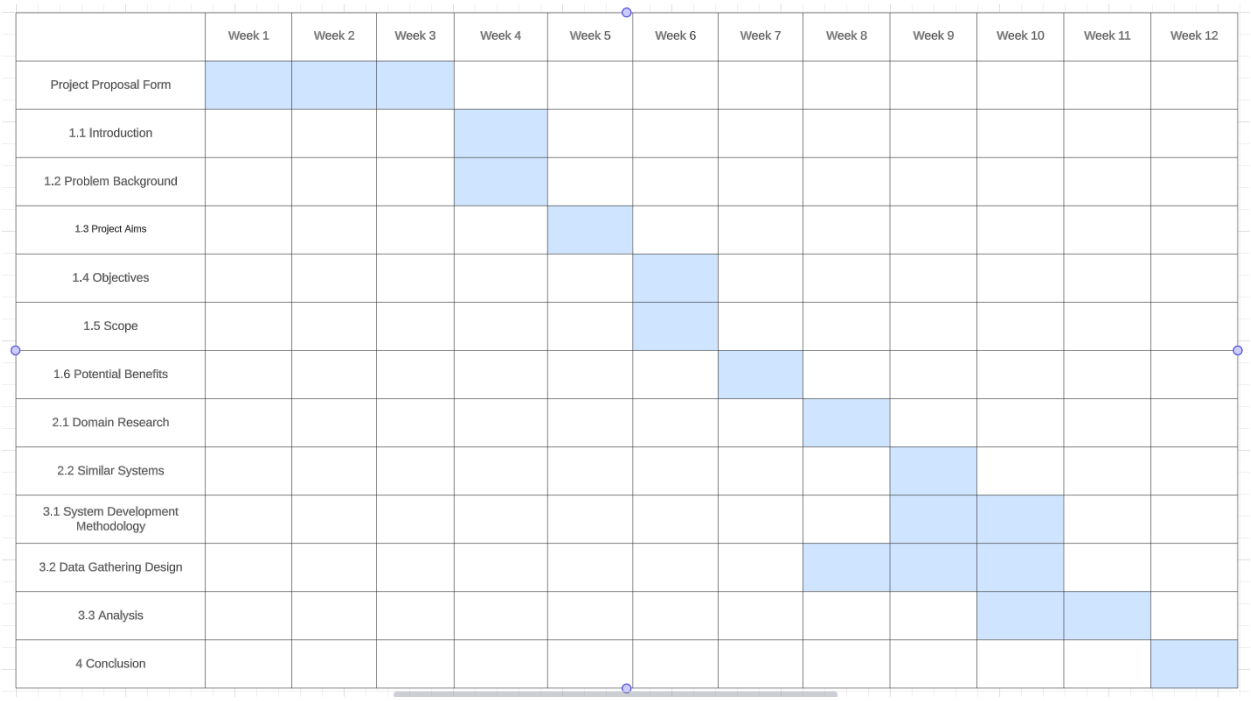
Key Features:

- Real-time password strength evaluation
- Instantly identify predictable password constructions
- Simple interface for seamless user experience
- Educational tips on password security best practices

Benefits:

- Enhance personal cybersecurity by adopting stronger passwords
- Improve password hygiene through interactive guidance
- Cultivate long-term security awareness and proactive habits
- Convenient tool for testing password strength

Gantt Chart



	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13
4.1 Design and Implementation													
4.2 Design													
4.3 Interface Design													
4.4 Execution													
5.1 Result and Discussion													
5.1 Testing Design/Plan													
5.2 System Testing													
6.1 Critical Evaluation													
6.2 Limitation													
6.3 Recommendation													

Sample Code Implementation

```html
<!DOCTYPE html>
<html>
<head>
    <title>Password Strength Assessment Tool</title>
    <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
    <script src="1pass.js"></script>
    <style>
        body {
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
            background-color: #333;
            color: #fff;
        }
        .container {
            text-align: center;
        }
        input {
            width: 400px;
            margin-top: 20px;
            margin-bottom: 20px;
        }
        .pass-strength-text {
            font-weight: bold;
        }
        .revolving-text {
            margin-top: 20px;
        }
        .revolving-text a {
            color: #99c2ff;
            text-decoration: underline;
            cursor: pointer;
        }
    </style>
</head>
<body>
    <div class="container">
        <h1>Password Strength Assessment Tool</h1>
        <div>
            <label for="password">Type in a password to check its strength:</label>
            <input id="password" type="password" />
        </div>
        <div class="revolving-text"></div>
    </div>

    <script>
        $(document).ready(function() {
            $('#password').password();

            var links = [
                'https://example.com/password-tips',
                'https://example.org/secure-passwords',
                'https://example.net/password-best-practices'
            ];

            var currentIndex = 0;
            var $revolvingText = $('.revolving-text');

            function displayNextLink() {
                var link = links[currentIndex];
                $revolvingText.html('<a href="' + link + '" target="_blank">' + link + '</a>');
                currentIndex = (currentIndex + 1) % links.length;
            }

            setInterval(displayNextLink, 5000); // Change link every 5 seconds
        });
    </script>
</body>
</html>
```

```
(function($) {
    var Password = function($object, options) {
      var defaults = {
        minimumLength: 4,
        steps: {
          15: 'Really insecure password',
          40: 'Weak; try combining letters & numbers',
          65: 'Medium; try using special characters',
          90: 'Strong password'
        }
      };

      options = $.extend({}, defaults, options);

      function calculateScore(password) {
        var score = 0;

        if (password.length < options.minimumLength) {
          return -1;
        }

        score += password.length * 4;
        score += checkRepetition(1, password).length - password.length;
        score += checkRepetition(2, password).length - password.length;
        score += checkRepetition(3, password).length - password.length;
        score += checkRepetition(4, password).length - password.length;

        if (password.match(/(.*[0-9].*[0-9].*[0-9])/)) {
          score += 5;
        }

        var symbols = '.*[!,@,#,$,%,^,&,*,?,_,~]';
        symbols = new RegExp('(' + symbols + symbols + ')');
        if (password.match(symbols)) {
          score += 5;
        }

        if (password.match(/([a-z].*[A-Z])|([A-Z].*[a-z])/)) {
          score += 10;
        }

        if (password.match(/([a-zA-Z])/) && password.match(/([0-9])/)) {
          score += 15;
        }

        if (password.match(/([!@#$%^&*?_~])/) && password.match(/([0-9])/)) {
          score += 15;
        }

        if (password.match(/([!@#$%^&*?_~])/) && password.match(/([a-zA-Z])/)) {
          score += 15;
        }

        if (password.match(/^\w+$/) || password.match(/^\d+$/)) {
          score -= 10;
        }

        return Math.max(0, Math.min(100, score));
      }
```

```
    function checkRepetition(length, str) {
      var res = "", repeated = false;
      for (var i = 0; i < str.length; i++) {
        repeated = true;
        for (var j = 0; j < length && (j + i + length) < str.length; j++) {
          repeated = repeated && (str.charAt(j + i) === str.charAt(j + i + length));
        }
        if (j < length) {
          repeated = false;
        }
        if (repeated) {
          i += length - 1;
          repeated = false;
        } else {
          res += str.charAt(i);
        }
      }
      return res;
    }

    function getScoreText(score) {
      if (score === -1) {
        return 'The password is too short';
      }

      score = score < 0 ? 0 : score;

      var sortedStepKeys = Object.keys(options.steps).sort();
      for (var step of sortedStepKeys) {
        if (step > score) {
          return options.steps[step];
        }
      }

      return 'Strong password';
    }

    var $strengthText = $('<div>').addClass('pass-strength-text');
    $object.after($strengthText);

    $object.on('keyup', function() {
      var score = calculateScore($object.val());
      var text = getScoreText(score);
      $strengthText.text(text);
    });
  };

  $.fn.password = function(options) {
    return this.each(function() {
      new Password($(this), options);
    });
  };
})(jQuery);
```

Respondence Demographic Profile

	Gender	Age Group	Current Occupation
1	Male	18 - 21	Student
2	Male	18 - 21	Student
3	Male	18 - 21	Student
4	Female	18 - 21	Student
5	Male	18 - 21	Student
6	Male	22 - 25	Employed
7	Male	18 - 21	Student
8	Female	18 - 21	Student
9	Male	18 - 21	Student
10	Female	18 - 21	Student
11	Male	22 - 25	Unemployed
12	Male	18 - 21	Student
13	Female	22 - 25	Employed
14	Male	18 - 21	Student
15	Female	22 - 25	Unemployed
16	Male	18 - 21	Student
17	Male	18 - 21	Student
18	Male	18 - 21	Student
19	Male	18 - 21	Student
20	Male	18 - 21	Student
21	Male	18 - 21	Student
22	Male	18 - 21	Student
23	Male	18 - 21	Student

PORTFOLIO

COMPREHENSIVE DATABASE SECURITY IMPLEMENTATION FOR AIS

INTRODUCTION

Designed and implemented a secure, layered architecture for the Academic Information System (AIS) database to protect sensitive student and staff data.

OBJECTIVE

Enhance the security posture of the AIS database, safeguarding sensitive information through access control, encryption, monitoring, and recovery.

KEY COMPONENTS

- User Role Management & Permissions: Developed RBAC policies and tailored permissions for roles like Administrators, Students, and Lecturers.
- Data Classification & Protection: Categorized data and applied encryption (symmetric and transparent) for confidentiality.
- Activity Monitoring & Auditing: Used triggers and stored procedures to log critical actions and maintain comprehensive audit logs.
- Backup & Recovery: Automated backups and ensured reliable recovery strategies to minimize data loss and downtime.
- Security Enhancements: Implemented password policies, monitored suspicious activity, and reinforced the CIA triad (confidentiality, integrity, availability).

OUTCOME

A secure, compliant, and resilient AIS database capable of preventing breaches and maintaining data integrity through role-based and policy-driven security controls.

Kindly follow this link for more information:

Full Github Documentation

DATABASE SECURITY

Table of Contents

1. Introduction

The purpose of this project is to strengthen the safety of the database that is part of the Academic Information System (AIS). In spite of the fact that the institution relies on this system to handle its day-to-day operations, the database was discovered with significant security flaws in the design and implementation of the database.

The establishment of comprehensive auditing processes to monitor all database activity and user logins, the implementation of automatic and regular backups to minimize the amount of data that is lost, and the guaranteeing of data categorization and protection are key areas of attention. It is necessary for the security model to contain role-based access management, which must carefully follow the principle of least privilege, in order to effectively handle various user roles, such as Database Administrators, Students, and Lecturers, each of which has a unique set of authority and restrictions.

1.1. Data Dictionary

1.1.1. Database Tables

1. Student

- ID (varchar(6)): Primary key. Unique identifier for each student.
- SystemPwd (varbinary(max)): Encrypted password for the student's system access.
- Name (varchar(100)): Full name of the student.
- Phone (varchar(20)): Contact phone number of the student.

2. Lecturer

- ID (varchar(6)): Primary key. Unique identifier for each lecturer.
- SystemPwd (varbinary(max)): Encrypted password for the lecturer's system access.
- Name (varchar(100)): Full name of the lecturer.
- Phone (varchar(20)): Contact phone number of the lecturer.
- Department (varchar(30)): Department to which the lecturer belongs.

3. Subject

- Code (varchar(7)): Primary key. Unique code for each subject.
- Title (varchar(40)): Title or name of the subject.

4. Result

- ID (int): Primary key. Auto-incrementing identifier for each result entry.
- StudentID (varchar(6)): Foreign key referencing Student(ID).
- LecturerID (varchar(6)): Foreign key referencing Lecturer(ID).
- SubjectCode (varchar(7)): Foreign key referencing Subject(Code).
- AssessmentDate (date): Date when the assessment was conducted.
- Grade (varchar(2)): Grade awarded for the subject.
- CreatedBy (varchar(6)): ID of the user who created this record.
- Department (varchar(30)): Department associated with the result.

5. AuditLog

- AuditLogID (int): Primary key. Auto-incrementing identifier for each audit log entry.
- EventType (nvarchar(100)): Type of event (e.g., INSERT, UPDATE, DELETE).
- EventData (xml): Detailed XML data describing the event.
- EventDateTime (datetime): Date and time when the event occurred.
- UserName (nvarchar(128)): Username of the user who triggered the event.
- SchemaName (nvarchar(128)): Schema name where the event occurred.
- ObjectName (nvarchar(128)): Name of the database object affected.
- SqlStatement (nvarchar(max)): SQL statement executed that triggered the log entry.

6. LoginHistory

- ID (int): Primary key. Auto-incrementing identifier for each login attempt.
- UserID (nvarchar(100)): Identifier of the user who logged in.
- LoginTime (datetime): Timestamp of the login.
- LogoutTime (datetime): Timestamp of the logout.
- Succeeded (bit): Indicates whether the login attempt was successful (1) or not (0).

1.1.2. Database Views

1. StudentInfo

- Provides a view of students' IDs, names, and phone numbers, excluding sensitive data like passwords.

2. LecturerInfo

- Provides a view of lecturers' IDs, names, phone numbers, and departments, excluding sensitive data like passwords.

3. StudentAcademicData

- Provides a view for individual students to access their own academic records.

4. AllStudentsInfo

- View accessible by lecturers to view basic information of all students.

5. DepartmentResults

- View showing results entered by lecturers from the same department, including detailed result information.

1.1.3. Stored Procedures and Security Policies

- AddNewStudent: Adds a new student record with encrypted password.
- AddNewLecturer: Adds a new lecturer record with encrypted password.
- UpdateStudentDetails: Allows students to update their own information securely.
- UpdateLecturerDetails: Allows lecturers to update their own information securely.

1.1.4. Triggers

- AuditDataChanges: Triggers that capture and log changes in Student, Lecturer, Subject, and Result tables.

2. Permission Management

2.1. Authorization Matrix

Role	Permission Type	Object	Privilege
DB Admins	Grant	Database: AIS	Create
DB Admins	Grant	Security: Users	Create, Alter
DB Admins	Grant	Tables: Student, Lecturer	Select, Insert, Update

DB Admins	Deny	Columns: Student.SystemPwd, Lecturer.SystemPwd	Select, Insert, Update, Delete
DB Admins	Deny	Tables: Result	Select, Insert, Update, Delete
Students	Grant	Tables: Student (Own)	Select, Update
Students	Grant	Tables: Result	Select
Students	Deny	Tables: Result (Other Students)	Select, Insert, Update, Delete
Lecturers	Grant	Tables: Lecturer (Own)	Select, Update
Lecturers	Grant	Tables: Student	Select
Lecturers	Grant	Tables: Result (They added)	Update, Delete
Lecturers	Grant	Tables: Result (Same Department)	Select
Lecturers	Grant	Tables: Result (Subject and Students they teach)	Insert, Select, Update, Delete
Lecturers	Deny	Column: Student.SystemPwd	Select

The authorization matrix is an indispensable security part of the database security strategy for the Academic Information System (AIS). It ensures that permissions are given in accordance with user roles, and therefore, the security and confidentiality of the database is maintained. The matrix is set up in compliance with the least privilege principle. This implies giving DB admins, students, and lecturers the minimum access required to do their job. Such as providing the DB Admins with the permission to add and manage the student and lecturer details but are not allowed to delete them. In the provided authorization matrix, DB Admins are given access to create new table, view, or procedure and they are responsible for the creation and the management of user roles. Restrictions are however limited to only areas where it necessary, such as not granting them the ability to view or change sensitive information which include password and academic data like results. Students are granted privileged access to their own data, but they are not allowed to view and edit other students' details. It allows for privacy, making sure that forgery and unauthorized changes are avoided. Lecturers are granted the right to control the data related to their lectures, but

they are unable to access or manipulate the student security passwords, preserving both the data integrity and system security.

2.2. User Management Solutions

2.2.1. Access Control

Access control is one of the basic security features of databases and requires users to be granted access to data adequate to their roles. In the scope of Academic Information System (AIS), a powerful access control model has been implemented, built upon Role-Based Access Control (RBAC) and additionally strengthened with Row-Level Security (RLS). This combination was selected to ensure a holistic and multi-layered approach to security which includes both prevention of specific threats and application of the principle of least privilege.

RBAC was one of the methods that was used because it precisely follows the organizational structure of the universities environment, evident from the fact that people take on distinctive roles such as students, lecturers, and database administrators. Instead of just focusing on individuals and providing them with specific roles and permissions, AIS will create roles within the organization such as DB Admins, Students, and Lecturers with the respective permissions assigned to them thus retaining manageability and scalability.

The RBAC model is also chosen for its security and efficiency reasons in allowing users to alter permission management processes (SecurePass, 2021). In an academic setting, when roles may change such as students may graduate and lecturers may take administrative positions, a RBAC allows for instant and effortless adjustments, reflecting such changes without the need of lengthy re-configuration processes.

```
-- Create roles for DB Admins, Students, and Lecturers
CREATE ROLE DBAdmins;
CREATE ROLE Students;
CREATE ROLE Lecturers;
```

The first step in establishing RBAC in this database is to create different roles within the database. Each of these roles is then assigned to different permission to allow them to perform their responsibilities. The ‘CREATE ROLE’ statement will define a role for the database which in this case is DBAdmins, Students, and Lecturers. Their specific permission will be discussed later.

DBAdmins

```
-- DB Admins
-- Create schema for dbadmins
CREATE SCHEMA DBAdminsSchema;
GRANT ALTER ON SCHEMA::DBAdminsSchema TO DBAdmins;
-- Grant DB Admins to alter create user, alter the roles, and create login for them
GRANT ALTER ANY USER TO DBAdmins;
GRANT ALTER ON ROLE::Students TO DBAdmins;
GRANT ALTER ON ROLE::Lecturers TO DBAdmins;
GRANT ALTER ANY LOGIN TO DBAdminLogin;
-- Grant DBAdmins on the view created
GRANT SELECT, INSERT, UPDATE ON dbo.StudentInfo TO DBAdmins;
GRANT SELECT, INSERT, UPDATE ON dbo.LecturerInfo TO DBAdmins;
-- Deny DBAdmins on the base table
DENY SELECT, INSERT, UPDATE, DELETE ON dbo.Student TO DBAdmins;
DENY SELECT, INSERT, UPDATE, DELETE ON dbo.Lecturer TO DBAdmins;
DENY SELECT, INSERT, UPDATE, DELETE ON dbo.Result TO DBAdmins;
-- Grant the EXECUTE permission to DB Admins
GRANT EXECUTE ON dbo.AddNewStudent TO DBAdmins;
GRANT EXECUTE ON dbo.AddNewLecturer TO DBAdmins;
-- Grant DB Admins to daily generate daily audit
GRANT EXEC ON dbo.GenerateLoginLogoutReport TO DBAdmins;
GRANT SELECT, Insert ON AuditLog TO DBAdmins;
```

Figure above shows the permission assigned to DB Admins with '*GRANT*', and '*DENY*'. First, the '*CREATE SCHEMA*' creates a schema in the database follow by granting DB Admins to modify the schema structure such as creating or altering the objects within the schema. Next, DB Admins can alter any user and role like Students and Lecturers indicates that DB Admins are responsible for managing access control by creating new roles or altering existing roles and users. This is essential for performing user onboarding and altering roles to fit the current access requirements. The '*GRANT ALTER ANY LOGIN TO DBAdminLogin*' permission allows DB Admins to create or modify logins for other roles. Since logging into the database required username and password and DB Admins are not allowed to add password for Students and Lecturers in their table. Therefore, DB Admins will create a temporary password for them and require them to change on their first login and update their details accordingly. Furthermore, DB Admins is also granted permission to access the view created to limit the information that they can view from the students and lecturers' table which will be discussed later this part. Then, direct access to the base table will be denied for DB Admins. DB Admins are also granted the permission to execute the stored procedure created like '*AddNewStudent*', '*AddNewLecturer*', and '*GenerateLoginLogoutReport*' which will ensure consistency and security and will be discussed later in this report. The DB Admins are also provided with the ability to generate reports on user login and logout activities and the changes made to the database including structural, data, and permissions.

Students

```
-- Students
 -- Grant EXECUTE on their own details. This is controlled by the row-level security policy.
GRANT EXECUTE ON ViewOwnDetails TO Students, Lecturers;
 -- Grant the necessary permissions on the view to the Students role.
 GRANT SELECT ON dbo.StudentAcademicData TO Students;
 -- Grant the EXECUTE permission to students to update only own details
 GRANT EXECUTE ON dbo.UpdateStudentDetails TO Students;
 -- Grant Students to record login and logout information
 GRANT EXECUTE ON dbo.RecordLogin TO Students, Lecturers;
 GRANT EXECUTE ON dbo.RecordLogout TO Students, Lecturers;
```

The figure above shows the students' permission. First, students are granted to view their personal details in the '*Student*' table. This access is further controlled by a row level security which will be discussed later to ensure they can only see their own details but not others. With '*GRANT SELECT ON dbo.StudentAcademicData TO Students;*', students are granted read access to the '*StudentAcademicData*' view. This view is designed to display academic information that is directly related to the student who is logged in. The view ensures that students have access to their academic records without exposing the data of other students, adhering to privacy requirements. The execution permission on '*dbo.UpdateStudentDetails*' granted by '*GRANT EXECUTE ON dbo.UpdateStudentDetails TO Students;*' empowers students to update their own details. It encapsulates the update operation within a stored procedure, which not only streamlines the process but also adds a layer of security by ensuring that the update operation is performed in a controlled manner, preventing any unauthorized updates to student records. The students are also granted permission to record their login and logout activities by executing the stored procedure created. This feature is necessary for functioning with the purpose of keeping safe records of user activities within the system.

Lecturers

```
-- Lecturers
-- Grant SELECT on their own details. This is controlled by the row-level security policy.
GRANT EXECUTE ON ViewOwnDetails TO Students, Lecturers;
-- Grant SELECT, INSERT, UPDATE, DELETE on dbo.Subject TO Lecturers;
GRANT SELECT, INSERT, UPDATE, DELETE ON dbo.Subject TO Lecturers;
-- Grant SELECT on the view to Lecturers.
GRANT SELECT ON dbo.AllStudentsInfo TO Lecturers;
-- Grant SELECT on the results from same department view to Lecturers.
GRANT SELECT ON dbo.DepartmentResults TO Lecturers;
-- Grant permissions to add new academic data (Result Table).
GRANT EXECUTE ON AddResult TO Lecturers;
-- Granting execute permission on update and delete to the results they added to Lecturers on the Result table.
GRANT EXECUTE ON UpdateResult TO Lecturers;
GRANT EXECUTE ON DeleteResult TO Lecturers;
-- Grant the EXECUTE permission to lecturers to update only own details
GRANT EXECUTE ON dbo.UpdateLecturerDetails TO Lecturers;
-- Grant Lecturers to record login and logout information
GRANT EXECUTE ON dbo.RecordLogin TO Students, Lecturers;
GRANT EXECUTE ON dbo.RecordLogout TO Students, Lecturers;
```

The figure above shows the permission management for Lecturers. Similarly to student permission, lecturers are granted to view their personal details in the '*Lecturer*' table. This is also further controlled by a row level security policy to avoid them viewing other lecturers' details. The lecturers are then granted the permission to have full control on the '*Subject*' table, allowing them to add new subject or modify the existing one. A view is then created specifically for lecturers to view all students' non sensitive information and to view only the result from the same department. Lecturers are then granted execute permission on the stored procedure such as '*AddResult*', '*UpdateResult*', '*DeleteResult*', '*RecordLogin*', and '*RecordLogout*' stored procedure. Each of the procedures has its own security measures implemented such as in '*AddResult*', lecturers are only allowed to enter for the subject and student they taught. Whereas in '*UpdateResult*' and '*DeleteResult*', lecturers are only allowed to perform this action for the result that they added.

2.2.2. Row Level Security Policy

Row-Level Security (RLS) is a model which prevents access to records in any particular table at the row level of the database (Berning, 2023). Unlike traditional access control mechanisms at the table level or the column level, RLS allows you to apply restrictions directly on data access from any table in the database through which the data is accessed. It implies that RLS can implement a uniform access strategy whenever different applications are fetching the same data. In AIS, the rule of row level security is enforced by security functions and policies that can be altered so that only certain rows are accessible. These functions are user-based instances of a query that restrict data visibility in query results to only the requested information. An instance can be when students and lecturers can only access their own personal data.

RLS is a layer above RBAC, providing another security control that complements database data security. The system is therefore capable of restricting data access at the row-level within the database. This was the priority of the AIS project, which there was no doubt deterred students and lecturers from accessing information and data that did not belong to them. Via RLS, this can resolve the issue of authorized access attempts to confidential records. Besides, RLS provides strong security in privacy data, being a precondition in a learning environment where data about both students and assistant professors should be protected. Through granting data access only at the lowest level, RLS reduces the chance of unprotected data leakage, which, in turn, improves data privacy (Zahid, 2023). The next important consideration is that universities are subject to highly regulated standards that require the confidentiality of student information. RLS plays a role in proper compliance with these regulations by directing access restrictions to the database and ensuring that exposure of data is limited to the authorized users as well as thus significantly reducing possibilities of compliance violations. Moreover, the principle of least privilege is a key aspect in the security policy of AIS. Implementing RLS helps to block the chance for users of acquiring data that is not relevant to their educational or administrative purposes thus reducing the attack surface and the possibility for data misuse (Zahid, 2023).

```
-- Create the row-level security policy function for student to view only own details
ALTER FUNCTION dbo.fn_securitypredicate_Student(@StudentID AS VARCHAR(6))
RETURNS TABLE
WITH SCHEMABINDING
AS
RETURN SELECT 1 AS result
WHERE @StudentID = CAST(SYSTEM_USER AS VARCHAR(6))
   OR IS_SRVROLEMEMBER('sysadmin') = 1
   OR IS_ROLEMEMBER('DBAdmins') = 1
   OR IS_ROLEMEMBER('Lecturers') = 1;
GO

-- Apply the row-level security policy to the Student table.
CREATE SECURITY POLICY StudentRowLevelSecurity
ADD FILTER PREDICATE dbo.fn_securitypredicate_Student(ID) ON dbo.Student
WITH (STATE = ON);
GO
```

Figure above shows the RLS policy statement implemented to the database. The function '*dbo.fn_securitypredicate_Student*' is a security predicate that specifies the access conditions. This enabled displaying a row only if the student ID in the table matches the login ID. This makes sure that the students see their own data only, and not for others, so that the confidentiality and safety

of the personal details of the students are preserved. Moreover, certain privileged roles such as the system administrators (sysadmin), database administrators (DBAdmins), and lecturers (Lecturers) are allowed to bypass this restriction. This design creates an environment whereby the required functions can easily be managed without altering security principles. This approach is also utilized in the lecturers to ensure that they only access their personal information and cannot access other lecturers.

2.2.3. View

Views in database act very critical with user management by offering a wide range of abstraction and security shield. In the AIS, users are provided with the view capabilities to access and perform actions with only the data that is relevant for their role. Views act like a virtual table and are a sort of window through which a database can show only certain tables which have been carefully chosen (Pavel, 2022). For instance, the view can be created that shows only student names and contact details, which the lecturer can use to access the details of the student without having access to their passwords.

The rationale for employing views for managing the data a user can access within the AIS was based on several key considerations. First, views do such a job by adding a level of abstraction that improves security (TutorChase, 2023). By including only columns that users need to perform their tasks, like ID, Name, and Phone for students, and Department for lecturers, the system ensures that no confidential data is displayed accidentally. This is very important because the privacy of data ownership is not only an ethical issue but a legal standard in most academic institutions.

Additionally, views reduce the complexity of the DB interface (Team Post, 2022). Users, especially those with no digital skills and experience, can now employ data easily. For example, the view dbo.StudentAcademicData allows students to obtain their grades and academic history in a simple manner, without getting into the complexity of the underlying database´s schema.

In addition to that, the justification for choosing views is also related to keeping data integrity and lessening the complexity of the administrative effort. Interactions of users with the AIS will be channeled through the views, which will reduce the access to the base tables. This minimizes the possible risks that could occur during accidental or unauthorized data manipulation. It also provides a method for data centralized access control which lessens the burden of administration

procedure as changes to users' permissions can be made by adjusting view definitions instead of modifying permissions across many tables.

```
-- Create View for students and lecturers tables except for password for DBAdmins
CREATE VIEW dbo.StudentInfo AS
SELECT ID, Name, Phone
FROM dbo.Student;
GO

CREATE VIEW dbo.LecturerInfo AS
SELECT ID, Name, Phone, Department
FROM dbo.Lecturer;
GO
```

```
SELECT * FROM dbo.StudentInfo
SELECT * FROM dbo.LecturerInfo
```

90 %

Results | Messages

	ID	Name	Phone
1	ST1001	John Doe	012-2148759
2	ST1002	Aaron Chia	011-21512548
3	ST1003	Micheal Tan	018-8549876
4	ST1004	Stainly	012-5486219
5	ST1005	Katty	018-4251987
6	ST1006	Peter Park	012-3521687
7	ST1007	Lucas Green	012-9966587
8	ST1008	Emma Wilson	011-55698874
9	ST1009	Idris Elba	018-5488795
10	ST1010	Nora Khan	012-3322687
11	ST1011	Henry Adams	018-1548779
12	ST1012	Sophia Turner	012-6599887

	ID	Name	Phone	Department
1	LC1001	Alice Smith	012-1158764	Computer Science
2	LC1002	Bob Johnson	011-23548896	Cybersecurity
3	LC1003	Cathy Brown	018-5487225	Software Engineering
4	LC1004	David Clark	012-2459987	Artificial Intelligence
5	LC1005	Eva Adams	012-5482224	Data Science
6	LC1006	Frank Morris	011-54879655	Information Technology
7	LC1007	Jane Miller	018-5487762	Computer Science
8	LC1008	Mike Barnes	018-2266547	Cybersecurity
9	LC1009	Susan Lee	011-55487996	Software Engineering
10	LC1010	Alan Turing	012-5487966	Artificial Intelligence
11	LC1011	Carol White	012-2665487	Data Science
12	LC1012	Omar Reed	018-5551548	Information Technology

The creation of the '*dbo.StudentInfo*' and '*dbo.LecturerInfo*' views in the AIS database exemplifies a streamlined approach to data presentation and access control. These views provide a secure and simplified interface to the underlying tables by selecting only the non-sensitive columns such as ID, Name, and Phone for students, with the addition of Department for lecturers. By intentionally excluding the '*SystemPwd*' column, the views prevent the exposure of password data, enhancing the security of personal information stored in the database.

```sql
-- Create a view that students can use to see only their academic data.
CREATE VIEW dbo.StudentAcademicData AS
SELECT s.ID, s.Name, s.Phone, r.SubjectCode, r.AssessmentDate, r.Grade
FROM dbo.Student s
JOIN dbo.Result r ON s.ID = r.StudentID
WHERE s.ID = CAST(SYSTEM_USER AS VARCHAR(6));
GO
```

```sql
SELECT * FROM dbo.StudentAcademicData
```

esults | Messages

ID	Name	Phone	SubjectCode	AssessmentDate	Grade
ST1001	John Doe	012-2148759	CS101	2024-04-26	A+

Figure above shows the view created for students to access only their personal details without being exposed to the data belonging to the others. This view forms a virtual table and will select the ID, Name, Phone from student table and Subject Code, Assessment Date, Grade from result table. The two tables are linked by a student's ID that ensures that the report of academic results always matches the correct student. Privacy protection is achieved using the '*WHERE*' clause, which filters the data according to the current system user's login ID, which is obtained by the '*SYSTEM_USER*' function. What it means more specifically is that whenever a student signs in and goes to that view, they will see only their data because the view limits the dataset to the individual's records based on their secret login ID.

```sql
-- Create a view to view all students' details for lecturers.
CREATE VIEW dbo.AllStudentsInfo AS
SELECT ID, Name, Phone
FROM dbo.Student;
GO
```

```
SELECT * FROM dbo.AllStudentsInfo
```

90 %

Results | Messages

	ID	Name	Phone
1	ST1001	John Doe	012-2148759
2	ST1002	Aaron Chia	011-21512548
3	ST1003	Micheal Tan	018-8549876
4	ST1004	Stainly	012-5486219
5	ST1005	Katty	018-4251987
6	ST1006	Peter Park	012-3521687
7	ST1007	Lucas Green	012-9966587
8	ST1008	Emma Wilson	011-55698874

This view is configured to provide lecturers with access to certain details about all students. It specifically selects the ID, Name, and Phone columns from the '*dbo.Student*' table. The view excludes any sensitive columns that may be present in the student table, such as the Password column.

```
-- Create a view to view all marks entered by lecturers from the same department.
ALTER VIEW dbo.DepartmentResults AS
SELECT r.ID AS ResultID, r.StudentID, r.LecturerID, s.Name AS StudentName, s.Phone AS StudentPhone, r.SubjectCode, r.AssessmentDate, r.Grade, r.CreatedBy, r.Department
FROM dbo.Result r
JOIN dbo.Student s ON r.StudentID = s.ID
WHERE r.Department = (SELECT Department FROM dbo.Lecturer WHERE ID = SYSTEM_USER);
GO
```

```
SELECT * FROM dbo.DepartmentResults
```

esults | Messages

ResultID	StudentID	LecturerID	StudentName	StudentPhone	SubjectCode	AssessmentDate	Grade	CreatedBy	Department
25	ST1007	LC1002	Lucas Green	012-9966587	CYB101	2024-04-26	A	LC1002	Cybersecurity
26	ST1007	LC1002	Lucas Green	012-9966587	CYB102	2024-04-26	A+	LC1002	Cybersecurity
27	ST1010	LC1002	Nora Khan	012-3322687	CYB103	2024-04-26	A+	LC1002	Cybersecurity

This view's purpose is to consolidate and display academic results entered by lecturers, filtered to include only those pertaining to lecturers' own department. The view achieves this by selecting a range of columns: the result ID, student ID, lecturer ID, student name, student phone, subject code, assessment date, grade, creator of the result, and the department from the Result and Student tables. These tables are joined on the student ID to match students with their academic results.

Crucially, the view is tailored dynamically for each lecturer using it. When a lecturer queries the view, the results are filtered so that only the entries related to their department are returned. This is managed by a '*WHERE*' clause that matches the '*Department*' column from the Result table with the lecturer's department, which is obtained through a nested '*SELECT*' statement. This

subquery determines the department of the currently logged-in user, fetched from the Lecturer table based on the system user's ID.

2.2.4. Store Procedures

This process is a critical part of the AIS. This procedure covers primary database operations into predefined SQL statements that are run with more speed and a higher level of security than the standalone queries (Uikey, 2023). The selection of stored procedure in AIS is because of its performance, stored procedures are pre-compiled and optimized by the database system resulting in an efficient execution of queries when compared to dynamically generated SQL statements (Ravikiran, 2021). This is a most valued advantage in an educational system which may require an additional load of operations at times of high attendance like during student registrations or grade submissions.

Maintainability is also significant among the advantages of stored procedures (geeksforgeeks, 2020). All SQL code is placed under a single umbrella of the database to simplify updates and maintenance. When radical changes are needed, it is more beneficial to rewrite a single stored procedure than editing different occurrences of in-line SQL statements placed in countless applications. This centralized method enables the process to be conducted in a uniform manner and minimized the possibility of mistakes. Besides, stored procedures allow for controlling of data, assure business rules and data validation at the database level. This is necessary to keep the AIS consistent, which means that all transactions with the database take place under the same predefined rules, independently of the application through which the database is accessed.

```sql
-- Procedure to record login time
CREATE PROCEDURE dbo.RecordLogin
    @Succeeded BIT
AS
BEGIN
    DECLARE @UserID NVARCHAR(100);
    DECLARE @LoginName NVARCHAR(100) = ORIGINAL_LOGIN();

    -- Try to get the student ID
    SELECT TOP 1 @UserID = ID
    FROM dbo.Student
    WHERE ID = @LoginName;

    -- If not found, try to get the lecturer ID
    IF @UserID IS NULL
    BEGIN
        SELECT TOP 1 @UserID = ID
        FROM dbo.Lecturer
        WHERE ID = @LoginName;
    END

    -- If a match is found in either table, record the login
    IF @UserID IS NOT NULL
    BEGIN
        INSERT INTO LoginHistory (UserID, LoginTime, Succeeded)
        VALUES (@UserID, GETDATE(), @Succeeded);
    END
END;
GO
```

The '*dbo.RecordLogin*' procedure is very detail oriented as it records the exact time a user login to AIS. The process begins by capturing the user's login name through the '*ORIGINAL_LOGIN()*' function, which ensures that the true user account is logged, even if the context is switched within the session. It then attempts to identify whether the login name corresponds to a student or lecturer and records this information alongside the login time to '*LoginHistory*'. The logout procedure, though not included in the documentation for brevity, is conceptually similar to the login procedure. It captures the exact time a user logs out of the system, providing a complete picture of user session duration.

```sql
-- Procedure to generate login & logout report for DBAdmins
CREATE PROCEDURE dbo.GenerateLoginLogoutReport
AS
BEGIN
    IF IS_MEMBER('DBAdmins') = 1 OR IS_SRVROLEMEMBER('sysadmin') = 1
    BEGIN
        SELECT *
        FROM LoginHistory
        WHERE CAST(LoginTime AS DATE) = CAST(GETDATE() AS DATE);
    END
    ELSE
    BEGIN
        THROW 50000, 'You do not have permission to generate the report.', 1;
    END
END;
GO
```

```sql
4  EXEC dbo.GenerateLoginLogoutReport
5
```

sults | Messages

ID	UserID	LoginTime	LogoutTime	Succeeded
7	ST1002	2024-04-27 11:50:53.903	NULL	0
8	ST1001	2024-04-27 11:54:03.947	2024-04-27 11:54:11.650	1

The figure above shows the procedure created to generate login and logout history for DB Admins. The procedure will start by verifying whether the user running the job is a member of the 'DBAdmins' or 'sysadmin' roles, which the users with these roles can make the report. If the role of the user was any of these roles, the procedure proceeds to query the '*LoginHistory*' table. It allows the selection of all records where the '*LoginTime*' column is comparable to the current date. This results in a report that contains only the login and logout activities for that day with the help of '*CAST(LoginTime AS DATE) = CAST(GETDATE() AS DATE)*' statement.

As shown in the second figure, the result only shows the login and logout record of the day. The succeeded column is column indicates whether the login was successful or not, 0 means for failed login while 1 means for successful login.

```
-- Creating a procedure to handle updates, ensuring only own records can be updated
CREATE PROCEDURE UpdateResult
    @ResultID INT,
    @Grade VARCHAR(2),
    @LecturerID VARCHAR(6) -- The ID of the lecturer making the update
AS
BEGIN
    -- Only allow update if the lecturer is the one who created the record
    UPDATE dbo.Result
    SET Grade = @Grade
    WHERE ID = @ResultID AND CreatedBy = @LecturerID;
END;
GO

-- Creating a procedure to handle deletes, ensuring only own records can be deleted
CREATE PROCEDURE DeleteResult
    @ResultID INT,
    @LecturerID VARCHAR(6) -- The ID of the lecturer making the delete
AS
BEGIN
    -- Only allow delete if the lecturer is the one who created the record
    DELETE FROM dbo.Result
    WHERE ID = @ResultID AND CreatedBy = @LecturerID;
END;
GO
```

The '*UpdateResult*' stored procedure gives lecturers an opportunity to alter the grades of students in their courses. Through this method, a lecturer can only update the results which he/she entered, this is carried out by checking the '*CreatedBy*' data field against the lecturer's ID. This function is a vital securing mechanism to ensure that the student grades are not subjected to any unauthenticated alteration, promoting the security of academic records. Similarly, the 'DeleteResult' procedure allows instructors to remove only the academic results they themselves created. Using the CreatedBy field as a condition in the WHERE clause within the DELETE statement is vital to avoid the lecturers from removing the records of others. This limitation is crucial because it stops unintended or intentional information loss and protects historical consistency of the student performance data.

```sql
-- Stored Procedure automatically encrypt password when created new user.
-- Stored Procedure for adding Student
CREATE PROCEDURE dbo.AddNewStudent
    @StudentID VARCHAR(6),
    @TempPassword VARCHAR(100),
    @Name VARCHAR(100),
    @Phone VARCHAR(20)
AS
BEGIN
    OPEN SYMMETRIC KEY PasswordEncryptionKey
    DECRYPTION BY CERTIFICATE AISServerCert;

    INSERT INTO dbo.Student (ID, SystemPwd, Name, Phone)
    VALUES (
        @StudentID,
        EncryptByKey(Key_GUID('PasswordEncryptionKey'), @TempPassword),
        @Name,
        @Phone
    );

    CLOSE SYMMETRIC KEY PasswordEncryptionKey;
END;
GO
```

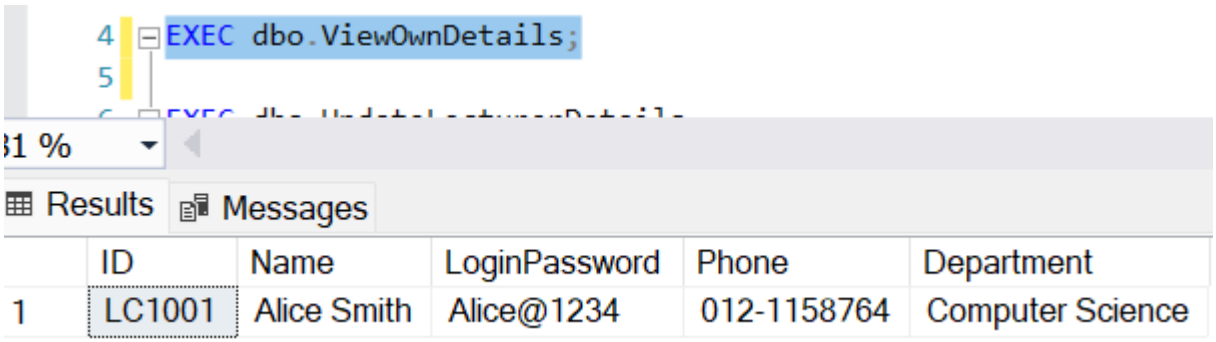
```sql
-- Create Student Login
CREATE LOGIN ST1001 WITH PASSWORD = 'ST1001@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1002 WITH PASSWORD = 'ST1002@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1003 WITH PASSWORD = 'ST1003@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1004 WITH PASSWORD = 'ST1004@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1005 WITH PASSWORD = 'ST1005@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1006 WITH PASSWORD = 'ST1006@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1007 WITH PASSWORD = 'ST1007@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1008 WITH PASSWORD = 'ST1008@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1009 WITH PASSWORD = 'ST1009@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1010 WITH PASSWORD = 'ST1010@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1011 WITH PASSWORD = 'ST1011@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
CREATE LOGIN ST1012 WITH PASSWORD = 'ST1012@1234' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON;
GO
```

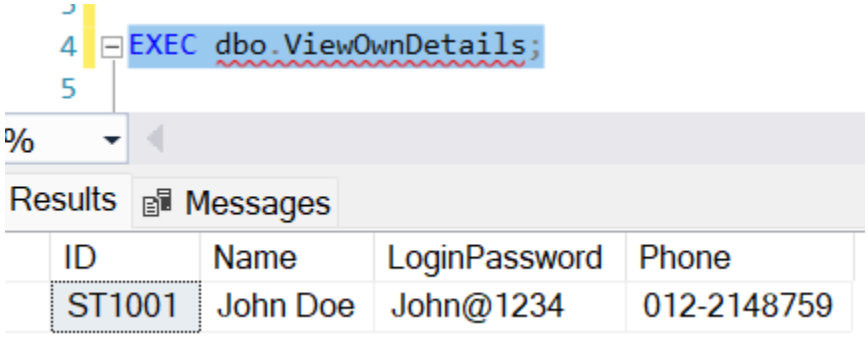
The '*dbo.AddNewStudent*' stored procedure is a secure method for database administrators (DBAdmins) to add new student records to the AIS. This procedure includes an essential security feature that is it automatically encrypts the temporary password assigned to the new user using the system's encryption key. Although it is a temporary password, the password will also be encrypted before inserting into the student table, ensuring the student password is secured. Similar approach is also use in creating new lecturer in the AIS. Both students and lecturers are required to change their password on their first login with the statement '*MUST_CHANGE*' to further secure their account.

```
-- Students to update their details on first login to update their password.
CREATE PROCEDURE dbo.UpdateStudentDetails
    @StudentID VARCHAR(6),
    @NewPassword VARCHAR(100),
    @NewName VARCHAR(100),
    @NewPhone VARCHAR(20)
AS
BEGIN
    -- Verify the executing user is the student whose details are being changed
    IF SYSTEM_USER = @StudentID
    BEGIN
        -- Open the symmetric key
        OPEN SYMMETRIC KEY PasswordEncryptionKey
        DECRYPTION BY CERTIFICATE AISServerCert;

        -- Update the student's password, name, and phone number
        UPDATE dbo.Student
        SET SystemPwd = EncryptByKey(Key_GUID('PasswordEncryptionKey'), @NewPassword),
            Name = @NewName,
            Phone = @NewPhone
        WHERE ID = @StudentID;

        -- Close the symmetric key
        CLOSE SYMMETRIC KEY PasswordEncryptionKey;
    END
    ELSE
    BEGIN
        -- Optionally handle the error case where the user does not have permission to update the record
        THROW 50001, 'You do not have permission to change these details.', 1;
    END
END;
GO
```

This process starts with making sure that the one who is trying to make the update is really the specific student by looking through the '*SYSTEM_USER*' and student ID. This is a mandatory security measure to keep aside the students from modifying data of others. After this validation, procedure carries out the '*PasswordEncryptionKey*' operation and allows for decryption by the '*AISServerCert*' certificate. This specifically provides that the modifications to any password made are performed securely using an encryption technique keeping all the confidential login details safe. Upon the completion of the update, the procedure closes the symmetric key to ensure that the encryption tools are secure. A similar approach is also utilized for lecturers to update their own details on their first login.

```sql
-- Procedure for Students and Lecturers to view own details
ALTER PROCEDURE dbo.ViewOwnDetails
AS
BEGIN
    DECLARE @UserID VARCHAR(6) = CAST(SYSTEM_USER AS VARCHAR(6));
    DECLARE @UserRole NVARCHAR(128);

    -- Determine the role of the user
    SELECT @UserRole = CASE
        WHEN EXISTS (SELECT * FROM dbo.Student WHERE ID = @UserID) THEN 'Student'
        WHEN EXISTS (SELECT * FROM dbo.Lecturer WHERE ID = @UserID) THEN 'Lecturer'
        ELSE NULL
    END;

    -- Open the symmetric key
    OPEN SYMMETRIC KEY PasswordEncryptionKey
    DECRYPTION BY CERTIFICATE AISServerCert;

    IF @UserRole = 'Student'
    BEGIN
        -- Return details for student
        SELECT
            ID,
            Name,
            CONVERT(VARCHAR, DECRYPTBYKEY(SystemPwd)) AS LoginPassword,
            Phone
        FROM
            dbo.Student
        WHERE
            ID = @UserID;
    END
    ELSE IF @UserRole = 'Lecturer'
    BEGIN
        -- Return details for lecturer
        SELECT
            ID,
            Name,
            CONVERT(VARCHAR, DECRYPTBYKEY(SystemPwd)) AS LoginPassword,
            Phone,
            Department
        FROM
            dbo.Lecturer
        WHERE
            ID = @UserID;
    END

    -- Close the symmetric key
    CLOSE SYMMETRIC KEY PasswordEncryptionKey;

    -- If @UserRole is NULL, then the user does not exist in either table
    IF @UserRole IS NULL
    BEGIN
        THROW 50001, 'User does not exist in the system or does not have permission to view details.', 1;
    END
END;
GO
```





The figure above shows the procedure to allow students and lecturers to view only their own details with the password shown in plain text for them. The procedure will start by identifying the current login user and check if they exist either in the student or lecturer table. Based on that, the user will then have their details retrieved and have their login password display as plain text for them. This is also controlled by RLS policy that discussed previously so that they are only allowed to view own details.

3. Data Protection

3.1. Data Classification Matrix

A Data Classification Matrix is a tool that is used for the purpose of organising and categorising various sorts of data in accordance with its significance, sensitivity, and secrecy. The matrix is a structure that resembles a grid and is used to classify data into several levels according to the amount of danger they pose. Additionally, the matrix will set security controls that correlate to each level. In most cases, data is divided into four distinct categories: public, internal, secret, and restricted. The access controls, authentication requirements, and permission constraints that are particular to each category are individual to that category. Through the use of suitable security measures that are determined by the categorization level of the data, the matrix assists organisations in effective management and protection of their sensitive data. (Szentgyorgyi-Siklosi, 2023)

In the AIS system, the data can be classified into several categories based on sensitivity and criticality as follows:

Data Item	Classification	Description	Protection Measures	Example Data
Student ID	Confidential	Unique identifier for students.	Encrypted storage; Access restricted to system and authorized personnel.	'S1001'
Student Password	Restricted	Authentication information for student access.	Encrypted storage and transmission; No direct access, even by database admins.	Encrypted binary
Student Name	Internal	Full name of the student.	Protected against unauthorized updates; viewable by students and staff.	'John Doe'

Student Phone	Internal	Contact number of the student.	Access restricted to authorized personnel; logged access.	'123-456-7890'
Lecturer ID	Confidential	Unique identifier for lecturers.	Encrypted storage; Access restricted to system and authorized personnel.	'L2001'
Lecturer Password	Restricted	Authentication information for lecturer access.	Encrypted storage and transmission; No direct access, even by database admins.	Encrypted binary
Lecturer Name	Internal	Full name of the lecturer.	Protected against unauthorized updates; viewable by students and staff.	'Jane Smith'
Lecturer Phone	Internal	Contact number of the lecturer.	Access restricted to authorized personnel; logged access.	'987-654-3210'
Lecturer Department	Internal	Department to which the lecturer belongs.	Access limited to university personnel; important for internal operations.	'Computer Science'
Subject Code	Public	Code identifying a subject.	Basic access controls; public information.	'CS101'
Subject Title	Public	Title of the subject.	Basic access controls; public information.	'Introduction to Programming'
Grade	Confidential	Academic grades of students.	Encrypted storage; access restricted to	'A', 'B', etc.

			students, relevant lecturers, and staff.	
Assessment Date	Internal	Dates on which assessments were held.	Protected to ensure data integrity; logged for changes.	'2023-12-01'
Audit Logs	Restricted	Logs containing details about data access and changes.	Access strictly controlled; monitored and audited regularly.	Log entries
Login/Logout Records	Restricted	Information about user authentication sessions.	Access strictly controlled; used for security monitoring and compliance audits.	Timestamps, user IDs
Created By (in Results)	Internal	Identifier of who created academic records.	Access controlled; necessary for audits and tracking academic record entries.	'L2001'
System Logs	Restricted	Logs that monitor and record system operations.	Access strictly controlled; critical for troubleshooting and security monitoring.	System event entries

As shown in the table above, data in the AIS system are classified into four types which are Public Data, Internal Data, Confidential Data and Restricted Data.

Public Data

```
22  Create Table Subject (
23  Code varchar(7) primary key,
24  Title varchar(40)
25  )
```

As shown in the figure above, subject codes and titles are examples of the types of information that are included in this category. Both of these types of information are permitted to be disclosed

to the general public without causing any negative effects. The level of security that is present here is rather low, and its major objective is to ensure that the data has both availability and integrity.

Internal Data

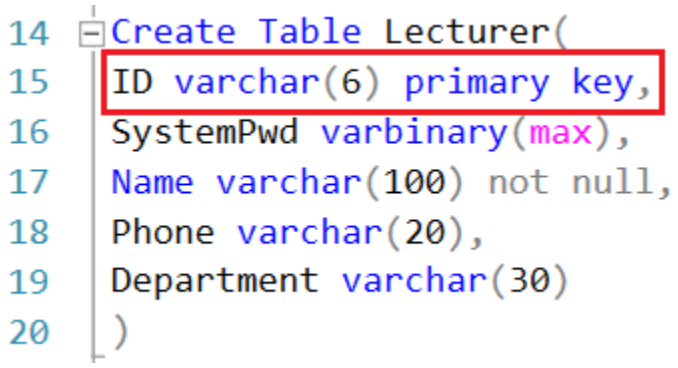
This category includes the bits of information that are necessary for day-to-day activities but are not particularly sensitive about the information they include. A few examples include the names and contact information of the students enrolled in the course. In order to prevent any unnecessary exposure, access is often restricted to those who are already employed by the organization.

```
14  Create Table Lecturer(
15  ID varchar(6) primary key,
16  SystemPwd varbinary(max),
17  Name varchar(100) not null,
18  Phone varchar(20),
19  Department varchar(30)
20  )
```

As shown in the figure above, the highlighted section is an example of internal data. Lecturers' names may usually be found on public platforms such as university websites or published papers. While they need security against unauthorized alterations and exploitation, they are not as sensitive as IDs or passwords. Lecturer phone numbers must be protected to avoid abuse or unauthorized disclosure, but they provide a smaller risk than password information. The department's information is important for internal organizational and operational reasons but does not cause major damage if leaked. It is largely used to organize and divide data and duties inside of the institution.

Confidential Data

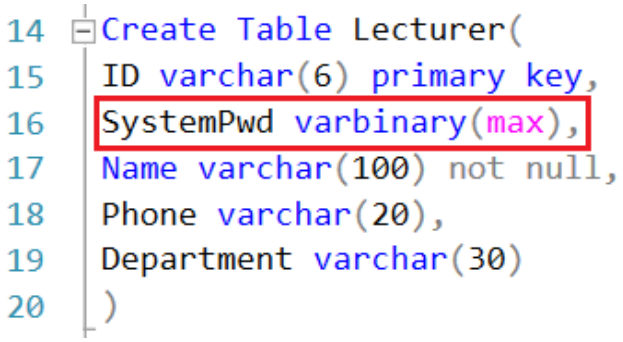
This includes very sensitive information that, if disclosed, has the potential to cause harm, such as the identification numbers of students and their grades. For the purpose of preventing unauthorized access to sensitive data and ensuring that it is kept confidential, stringent security measures, such as encryption and access limits, are carried out in order to safeguard it.



As shown in the figure above, the highlighted section is an example of confidential data. The Lecturer ID is a unique identifier that creates a connection between the system and each specific lecturer. The fact that it is used to access and manage lecturer-specific information and functions, which need to be secured in order to avoid unauthorized access and impersonation, which is the reason why it is categorized as confidential.

Restricted Data

All of this information, which includes audit logs and passwords, is safeguarded by the highest level of security technology that is currently available. In the event that it were possible to hack into this information, it may lead to significant legal and security complications. For the purpose of monitoring access alterations and changes, some examples of protection mechanisms that are used include encryption, strong access limits, and thorough audits.



As shown in the figure above, the highlighted section is an example of restricted data. This column is where the passwords for lecturer accounts are stored in an encrypted format. Due to the fact that it provides access to the lecturer's personal and professional information as well as administrative authorities inside the AIS, it is of the utmost importance to maintain this data under restricted practices.

3.2. Data Protection Solutions

3.2.1. Data Encryption

One method for protecting the confidentiality of data is known as data encryption. This technique involves converting the data into ciphertext, which can only be decoded by using a unique decryption key that was generated during the time of the encryption or before it. The process by which plaintext is transformed into ciphertext is referred to as encryption. (geeksforgeeks.org, 2022)

3.2.1.1 Symmetric Key Encryption

In cryptography algorithms, there are a few different tactics that may be applied. In order to perform encryption and decryption procedures, some algorithms make use of a unique key. In these kinds of operations, the unique key has to be protected due to the fact that the system or individual who holds the key possesses full authentication in order to decode the message for reading. The term "symmetric encryption" refers to this encryption method, which is used in the field of data encryption. (geeksforgeeks.org, 2022)

```
-- Creating Encryption Certificate for password encryption
USE AIS;
GO

-- Create a Master Key
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Xs3#v8S@pWqz!';
GO

-- Create a Certificate
CREATE CERTIFICATE AISServerCert WITH SUBJECT = 'AIS Certificate';
GO

-- Create a Symmetric Key
CREATE SYMMETRIC KEY PasswordEncryptionKey
    WITH ALGORITHM = AES_256
    ENCRYPTION BY CERTIFICATE AISServerCert;
GO
```

The figure above shows how Symmetric Key Encryption is set up for data protection. Frist, a master key is created to protect the certificates and symmetric keys which are stored in the database. It serves as the primary defence when securing the encryption hierarchy within the SQL server. Next, a certificate will be created to manage and secure the symmetric key that encrypts passwords.

It adds an additional layer of complexity on top of the encryption keys, which makes the system more secure. Lastly, a symmetric key is created for password encryptions in the database. As shown in the figure, AES-256 has been chosen as the encryption algorithm as Advanced Encryption Standard (AES) 256 usus 256-bit key converter to encrypt plain texts into cipher texts, which makes it an almost uncrackable symmetric encryption algorithm. (Kananda, 2022)

```
CREATE PROCEDURE dbo.AddNewLecturer
    @LecturerID VARCHAR(6),
    @TempPassword VARCHAR(100),
    @Name VARCHAR(100),
    @Phone VARCHAR(20),
    @Department VARCHAR(30)
AS
BEGIN
    OPEN SYMMETRIC KEY PasswordEncryptionKey
    DECRYPTION BY CERTIFICATE AISServerCert;

    INSERT INTO dbo.Lecturer (ID, SystemPwd, Name, Phone, Department)
    VALUES (
        @LecturerID,
        EncryptByKey(Key_GUID('PasswordEncryptionKey'), @TempPassword),
        @Name,
        @Phone,
        @Department
    );

    CLOSE SYMMETRIC KEY PasswordEncryptionKey;
END;
GO
```

The figure above shows an example of how Symmetric Key Encryption takes action, focusing on sensitive data encryption such as passwords before storing it in the database. The symmetric key '*PasswordEncryptionKey'* is opened using the '*AISServerCert'* certificate before using it for encryptions which is done using the command '*OPEN SYMMETRIC KEY PasswordEncryptionKey'* followed by *'DECRYPTION BY CERTIFICATE AISServerCert'*. Next, the *'EncryptByKey'* command is used to encrypt the temporary password with the symmetric key opened previously. The *'(Key_GUID('PasswordEncryptionKey')'* is used as a function call to retrieve the unique key. Lastly, the symmetric key is closed using the command *'CLOSE*

SYMMETRIC KEY PasswordEncryptionKey' after the encryption and data insertion are completed to secure it.

```
804  SELECT * FROM dbo.Lecturer;
```

110 %

Results | Messages

	ID	SystemPwd	Name	Phone	Department
1	LC1001	0x00688007FB248C49B9A388AC7B24D2AA0200000068CECF...	Alice Smith	012-1158764	Computer Science
2	LC1002	0x00688007FB248C49B9A388AC7B24D2AA02000000ABCA2F...	Bob Johnson	011-23548896	Cybersecurity
3	LC1003	0x00688007FB248C49B9A388AC7B24D2AA020000006336609...	Cathy Brown	018-5487225	Software Engineering
4	LC1004	0x00688007FB248C49B9A388AC7B24D2AA020000000354B04...	David Clark	012-2459987	Artificial Intelligence
5	LC1005	0x00688007FB248C49B9A388AC7B24D2AA02000000BF9A14...	Eva Adams	012-5482224	Data Science
6	LC1006	0x00688007FB248C49B9A388AC7B24D2AA02000000098E9E...	Frank Morris	011-54879655	Information Techno...
7	LC1007	0x00688007FB248C49B9A388AC7B24D2AA02000000E120C5...	Jane Miller	018-5487762	Computer Science
8	LC1008	0x00688007FB248C49B9A388AC7B24D2AA02000000868482F...	Mike Barnes	018-2266547	Cybersecurity
9	LC1009	0x00688007FB248C49B9A388AC7B24D2AA0200000096D3322...	Susan Lee	011-55487996	Software Engineering
10	LC1010	0x00688007FB248C49B9A388AC7B24D2AA02000000212E3BF...	Alan Turing	012-5487966	Artificial Intelligence
11	LC1011	0x00688007FB248C49B9A388AC7B24D2AA020000002AC3FE...	Carol White	012-2665487	Data Science
12	LC1012	0x00688007FB248C49B9A388AC7B24D2AA020000009901C13...	Omar Reed	018-5551548	Information Techno...

As shown in the figure above, the passwords have been encrypted into ciphertext therefore securing the integrity of the user's data.

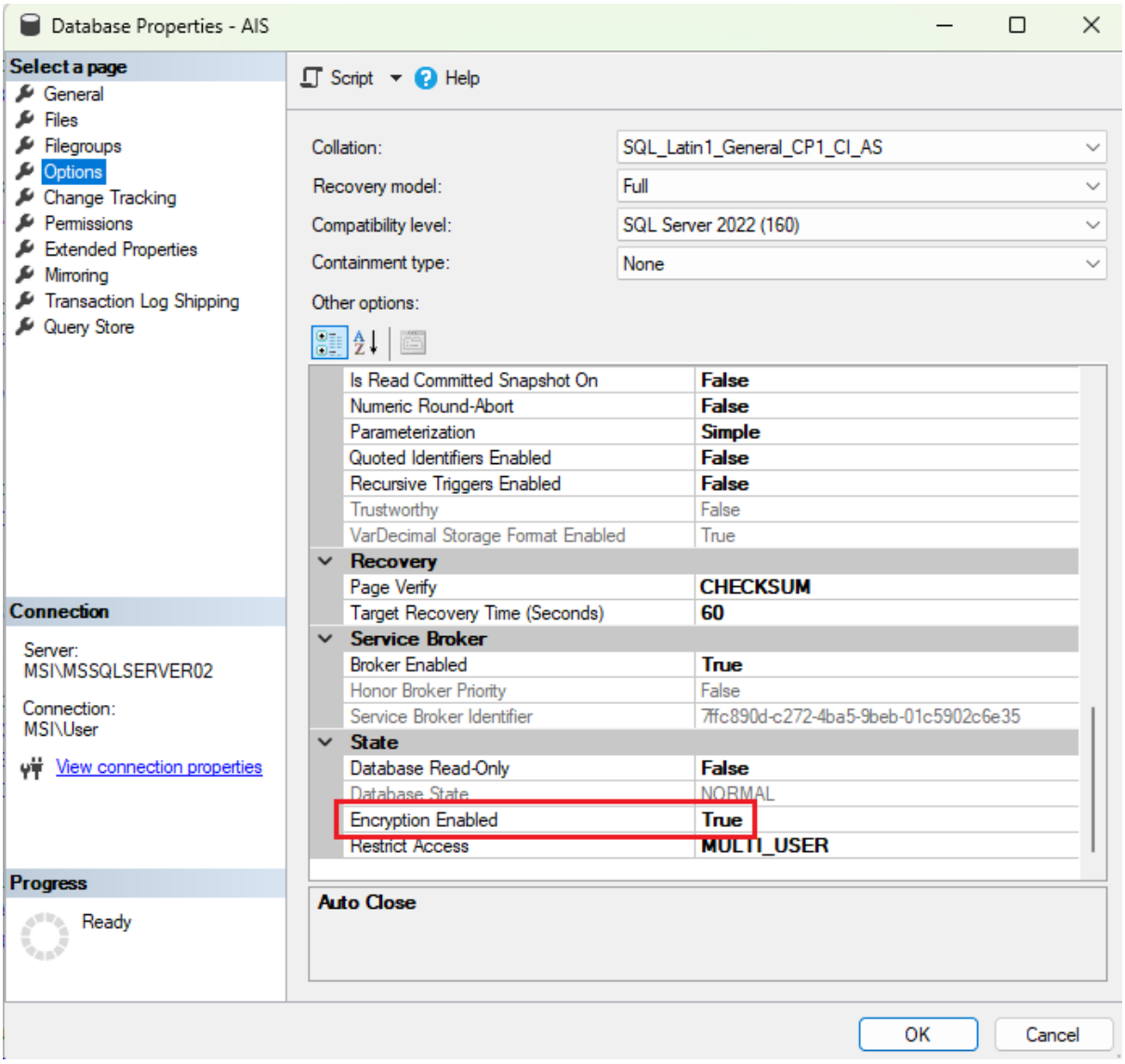
3.2.1.2 Transparent Data Encryption

Transparent Data Encryption (TDE) is a security solution that encrypts data at the storage layer. This protects sensitive data that is stored in database files that are stored on disc. The data is encrypted and decrypted on the fly using TDE while it is being written to or read from the storage. This is accomplished without the need for any changes to be made to the application's code. Not only does this ensure that data is encrypted while it is stored, but it also provides an essential layer of protection against unauthorized access, which is especially important in circumstances when physical security systems are ineffective. (Ahmed, 2022)

```
812  -- Create a Database Encryption Key (DEK) for TDE, protected by the certificate
813  USE master;
814  GO
815  CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MzF!0B$r3H6v&dK';
816  GO
817
818  -- Create a new certificate for TDE
819  CREATE CERTIFICATE TDEAISCertificate WITH SUBJECT = 'TDE AIS Certificate';
820  GO
821
822  USE AIS;
823  GO
824
825  -- Create a database encryption key (DEK) using the certificate from the master database
826 CREATE DATABASE ENCRYPTION KEY
827  WITH ALGORITHM = AES_256
828  ENCRYPTION BY SERVER CERTIFICATE TDEAISCertificate;
829  GO
830
831  -- Enable TDE on your AIS database
832 ALTER DATABASE AIS
833  SET ENCRYPTION ON;
834  GO
```

The figure above shows the process of how TDE is set up. First, the command *'CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MzF!0B$r3H6v&dK''* is used to create a master key in the master database, securing the encryption hierarchy in the SQL server. This key will be used for the encryption of certificates and symmetric keys stored. Next, a certificate is then created using the command *'CREATE CERTIFICATE TDEAISCertificate WITH SUBJECT = 'TDE AIS Certificate''* which will be used specifically for TDE only, which is responsible for protecting the Database Encryption Key (DEK). The command on line 826 to 828 shown in the above figure is used to create the DEK to encrypt the database using the TDE certificate created previously. Lastly, the command on line 832 and 833 as shown in the above figure is used to activate the TDE on the AIS database.

After enabling the TDE, we can then verify that TDE is enabled by right-click on the database and then clicking on Properties selection. Next, click on Options after Properties windows is opened, then scroll down to State section and look for Encryption Enabled. (Filip Holub , 2020) We can confirm that our TDE is in fact working as Encryption Enabled is indicated as True as shown in the following figure.



3.2.2. Backup and Recovery

The practice of generating and preserving copies of data that may be used as protection against the loss of data is known as backup and recovery or operational recovery. The process of recovering data from a backup often entails restoring the data to the spot where it was originally stored, or to a different location where it may be utilised in lieu of the data that was lost or destroyed. (NetApp.com, 2023)

A backup is created with the intention of producing a copy of the data that can be retrieved if the main data fails to be recovered. There are a number of factors that may lead to primary data failures. These include failures in hardware or software, data corruption, or events that are induced by

humans, such as an attack of virus or malware, or even the accidentally loss of data. The ability to restore data from an earlier point in time is made possible by backup copies. (NetApp.com, 2023)

3.2.2.1 Encrypted Backup

Encrypted Backup is the action of encrypting a backup file. It is important to encrypt backup files which are important and need a high level of integrity to ensure that no one will be able to access the data in the event of an attack or unauthorized access to the backup files.

```
836  -- Backup TDE
837  USE master;
838  GO
839
840  BACKUP CERTIFICATE TDEAISCertificate TO FILE = 'C:\Users\User\Desktop\year3 sem2\DBS\Assignment\
841  AIS_Database\SQL_Backups\TDE_Backup\TDEAISCertificateBackup'
842
843  WITH PRIVATE KEY (
844      FILE = 'C:\Users\User\Desktop\year3 sem2\DBS\Assignment\AIS_Database\SQL_Backups\
845      TDE_Backup\TDEAISCertificatePrivateKey',
846      ENCRYPTION BY PASSWORD = '7g@W5#hN!QpL8^J'
847  );
848  GO
849
850  -- Backup Password Encryption
851  USE AIS;
852  GO
853
854  BACKUP CERTIFICATE AISServerCert TO FILE = 'C:\Users\User\Desktop\year3 sem2\DBS\Assignment\AIS_Database\
855  SQL_Backups\Pwd_Encryption_Backup\AISServerCertBackup'
856
857  WITH PRIVATE KEY (
858      FILE = 'C:\Users\User\Desktop\year3 sem2\DBS\Assignment\AIS_Database\SQL_Backups\Pwd_Encryption_Backup\
859      AISServerCertPrivateKey',
860      ENCRYPTION BY PASSWORD = 'Y#8mCz!7$X3pLbQ'
861  );
862  GO
```

The figure above shows the creation of encrypted backups of certificate and private keys. These backups are crucial in the event of disaster recovery or moving encryptions to another server. The first block of SQL commands which is on line 840 to 848 in the figure above is used to backup the certificate used for the TDE. The next block of SQL commands which is on line 854 to 862 in the above figure is used to backup the certificate used for password encryptions in the AIS database.

3.2.2.2 Backup Automation

Automated Backup is also implemented in the AIS database with the help of SQL Server Agent. As shown in the following figure, the command on line 865 to 871 is used to create a new job in the SQL Server Agent named “Automated_Backup” which will then be assign tasks to run scripts later. Next, a job step will be added. The command on line 874 to 882 is used to add a step in the job, which specifies the actual backup command. A specified file path will be directed to the SQL

Server to backup the AIS database and is also configured to retry backups up to 5 times in an interval of 5 minutes if the backup fails. The next step is to schedule the job. As shown on line 885 to 893 in the figure below, the command is used to set up a schedule to run the job once every 6 hours every single day. After creating a schedule, it will then be link to the job to ensure the job runs according to the schedule created as shown on line 896 to 899. Lastly, the job will be enabled and start running along side with the SQL Server Agent as shown on line 902 to 907, and then added to the SQL Server Agent's active job list using the command shown in line 910 to 912.

```
-- Automated Backup every 6 hours
USE msdb ;
GO

-- Create a new job named 'Automated_Backup'
EXEC dbo.sp_add_job
    @job_name = N'Automated_Backup' ;
GO

-- Add a step named 'Backup_Database' to the job
EXEC sp_add_jobstep
    @job_name = N'Automated_Backup',
    @step_name = N'Backup_Database',
    @subsystem = N'TSQL',
    @command = N'BACKUP DATABASE AIS TO DISK = N''C:\Users\User\Desktop\year3 sem2\DBS\Assignment\AIS_Database\
    SQL_Backups\Database Backup\AIS.bak'' WITH NOFORMAT, NOINIT, NAME = N''AIS-Full Database Backup'', SKIP, NOREWIND, NOUNLOAD, STATS = 10',
    @retry_attempts = 5,
    @retry_interval = 5 ;
GO

-- Schedule the job to run every 6 hours
EXEC dbo.sp_add_schedule
    @schedule_name = N'Every_6_Hours',
    @freq_type = 8,
    @freq_interval = 1,
    @freq_recurrence_factor = 1,
    @freq_subday_type = 8,
    @freq_subday_interval = 6,
    @active_start_time = 000000 ;
GO

-- Attach the schedule to the job
EXEC sp_attach_schedule
   @job_name = N'Automated_Backup',
   @schedule_name = N'Every_6_Hours' ;
GO

-- Make the job start when the SQL Server Agent starts
EXEC dbo.sp_update_job
    @job_name = N'Automated_Backup',
    @enabled = 1,
    @start_step_id = 1,
    @delete_level = 0;
GO

-- Add the job to the SQL Server Agent
EXEC dbo.sp_add_jobserver
    @job_name = N'Automated_Backup' ;
GO
```

In conclusion, each of the steps that were mentioned above addresses different risks, such as unauthorised data access, data breaches, and unauthorised data alteration, and assures compliance with regulations and standards related to data protection. As a result of these solutions, the AIS database is made more secure against both internal and external attacks, while simultaneously preserving the data's integrity and confidentiality.

4. Auditing

4.1. Audit Matrix

Auditing, a process referred to tracking and logging any kind of events, actions, and activities that occur within a database server environment. Those kind of events, actions, and activities may include data modifications, access attempts, schema changes, login attempts, and more (ManageEngine, 2022).

In cases of a security incident or data breach, the database that has implemented auditing will be able to identify unauthorized access attempts or suspicious activities within the database. By monitoring and recording database activities, the database's admin can detect and prevent security breaches or unauthorized access to sensitive data. There are also situations where industries and organizations have regulatory requirements that mandate the auditing of database activities, making it easy for the authority to trace back the activities from the auditing logs, if something ever goes wrong or if malicious attacker accessed or modified the data unauthorized (SatoriCyber, 2023).

Audit Area	Audit Objectives	Audit Solution
Data Modifications	Capture data changes from the tables: Student, Lecturer, Subject, and Result	Create triggers for auditing data changes
Structural Modifications	Capture structural changes from the database objects: Tables, Procedures, Views, and Functions	Create trigger for auditing structural changes
Permission Modifications	Capture permission changes from the roles: DBAdmin, Student, and Lecturer	Create trigger for auditing permission changes
Login And Logout	Capture and generate login and logout event	Create trigger for login history table and stored procedures

In summary, the database security audit matrix above highlights the key audit areas of database activity that should be closely monitored for security, compliance, and troubleshooting purposes. Our group suggest that each of the audit area has their own specific auditing mechanisms to

effectively capture and log relevant information, such as triggers for data and structural modifications, as well as stored procedures and login history tables for tracking access attempts.

4.2. Auditing Data Modifications

Auditing for data change in the AIS database involves the creation of four separate triggers, one for each of the following tables: “Student”, “Lecturer”, “Subject”, and “Result”. These triggers serve the same purpose of auditing data modifications, and the SQL queries used to create them are also almost identical.

By having separate triggers for each table, the auditing process can capture data changes specific to each table, providing a comprehensive audit trail for the entire database. This auditing approach ensures that any unauthorized or unintended modifications to the data can be tracked and investigated, enhancing the overall security and integrity of the AIS database.

All the 4 triggers follow the same logic and structure as the “AuditDataChanges_Student” trigger in the figure below, with minor variations to accommodate the different table structures and columns. The core functionality remains the same, which are determining the type of DML operation including “INSERT”, “UPDATE”, or “DELETE”, capturing the relevant data and inserting a log entry into the centralized “AuditLog” table.

```
CREATE TRIGGER AuditDataChanges_Student
ON dbo.Student
AFTER INSERT, UPDATE, DELETE
AS
BEGIN
    SET NOCOUNT ON;

    DECLARE @EventType NVARCHAR(50);
    DECLARE @Data XML;
    DECLARE @SqlStatement NVARCHAR(MAX) = N'';

    -- Determine the type of DML operation that invoked the trigger
    IF EXISTS (SELECT * FROM inserted)
    BEGIN
        IF EXISTS (SELECT * FROM deleted)
        BEGIN
            SET @EventType = 'UPDATE';
            SET @Data = (SELECT * FROM (
                        SELECT 'inserted' AS [@Action], ID, Name, Phone, CAST('' AS XML) AS SystemPwd FROM inserted
                        UNION ALL
                        SELECT 'deleted' AS [@Action], ID, Name, Phone, CAST('' AS XML) AS SystemPwd FROM deleted
                        ) AS Changes
                        FOR XML PATH('row'), ELEMENTS XSINIL, TYPE
        );
        END
        ELSE
        BEGIN
            SET @EventType = 'INSERT';
            -- Capture inserted data for INSERT
            SET @Data = (SELECT ID, Name, Phone, CAST('' AS XML) AS SystemPwd, 'inserted' AS [Action] FROM inserted FOR XML PATH('row'), ELEMENTS XSINIL, TYPE);
        END
    END
    ELSE
    BEGIN
        SET @EventType = 'DELETE';
        -- Capture deleted data for DELETE
        SET @Data = (SELECT ID, Name, Phone, CAST('' AS XML) AS SystemPwd, 'deleted' AS [Action] FROM deleted FOR XML PATH('row'), ELEMENTS XSINIL, TYPE);
    END

    SET @SqlStatement = 'DML operation ' + @EventType + ' performed on Student table';

    -- Insert a log entry into the AuditLog table
    INSERT INTO dbo.AuditLog (EventType, EventDateTime, UserName, SchemaName, ObjectName, SqlStatement, EventData)
    SELECT
        @EventType,
        GETDATE(),
        SYSTEM_USER,
        SCHEMA_NAME(),
        OBJECT_NAME(@@PROCID),
        @SqlStatement,
        @Data;
END;
GO
```

The trigger determines the type of DML operation that invoked it by checking the presence of rows in the “inserted” and “deleted” virtual tables. If rows exist in both “inserted” and “deleted” tables, it means an “UPDATE” operation occurred. The “@Data” variable is populated with the inserted and deleted rows, along with an “[@Action]” attribute indicating whether the row was inserted or deleted. If only the “inserted” table has rows, it means an INSERT operation occurred, and the “@Data” variable is populated with the inserted rows and an “[@Action]” attribute set to “inserted”. If there are no rows in the “inserted” table, it means a DELETE operation occurred, and the “@Data” variable is populated with the deleted rows and an “[@Action]” attribute set to “deleted” (Malhotra, 2022).

The “@SqlStatement” variable is set to a descriptive string indicating the DML operation and the table it was performed on. Finally, a new row is inserted into the “AuditLog” table, capturing the event type, event date and time, username, schema name, object name, SQL statement, and the changed data in XML format. The “CAST(‘’ AS XML) AS SystemPwd” section in the “SELECT” statements is used to avoid capturing the encrypted password data in the audit log, as the “SystemPwd” column stores encrypted passwords, and it is excluded from the audit log to maintain data confidentiality (Richardson, 2019).

AuditLogID	EventType	EventData	EventDateTime	UserName	Schema...	ObjectName	SqlStatement
150	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:28:02.297	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
151	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:28:02.300	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
152	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:28:02.300	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
153	UPDATE	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:30:40.060	LC1002	dbo	AuditDataChanges_Lecturer	DML operation UPDATE performed on Student ta...
154	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:30:40.113	LC1002	dbo	NULL	DML operation INSERT performed on Student table
155	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:30:40.120	LC1002	dbo	NULL	DML operation INSERT performed on Student table
156	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:30:40.120	LC1002	dbo	NULL	DML operation INSERT performed on Student table
157	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:33:13.643	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
158	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:33:13.657	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
159	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:33:13.657	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
160	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:36:37.153	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
161	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:36:37.160	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
162	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:36:37.160	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
163	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:36:57.647	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
164	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:36:57.660	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
165	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:36:57.660	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation INSERT performed on Student table
166	DELETE	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:39:25.173	LAPTOP-8ULJHU...	dbo	AuditDataChanges_Result	DML operation DELETE performed on Student ta...
167	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:39:58.727	LC1001	dbo	NULL	DML operation INSERT performed on Student table
168	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:39:58.730	LC1001	dbo	NULL	DML operation INSERT performed on Student table
169	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:39:58.733	LC1001	dbo	NULL	DML operation INSERT performed on Student table
170	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:40:19.517	LC1002	dbo	NULL	DML operation INSERT performed on Student table
171	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:40:19.527	LC1002	dbo	NULL	DML operation INSERT performed on Student table
172	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:40:19.530	LC1002	dbo	NULL	DML operation INSERT performed on Student table
173	INSERT	<row xmlns:xsi="http://www.w3.org/2001/XMLSche...	2024-04-26 12:41:36.177	LC1007	dbo	NULL	DML operation INSERT performed on Student table

Based on the figure above, this trigger effectively captures all data modifications such as “INSERT”, “UPDATE”, and “DELETE” operations on the “Student” table and logs the relevant information in the centralized “AuditLog” table for auditing purposes.

4.3. Auditing Structural Modifications

The auditing mechanism for structural modifications in the AIS database is implemented through the "AuditStructuralChanges" trigger. This trigger is defined at the database level and captures events related to creating, altering, or dropping tables, procedures, views, and functions.

```
CREATE TRIGGER AuditStructuralChanges
ON DATABASE
FOR CREATE_TABLE, ALTER_TABLE, DROP_TABLE,
    CREATE_PROCEDURE, ALTER_PROCEDURE, DROP_PROCEDURE,
    CREATE_VIEW, ALTER_VIEW, DROP_VIEW,
    CREATE_FUNCTION, ALTER_FUNCTION, DROP_FUNCTION
AS
BEGIN
    SET NOCOUNT ON;

    DECLARE @EventData XML = EVENTDATA();
    DECLARE @SqlStatement NVARCHAR(MAX) = @EventData.value('(/EVENT_INSTANCE/TSQLCommand)[1]', 'NVARCHAR(MAX)');
    DECLARE @EventType NVARCHAR(100) = @EventData.value('(/EVENT_INSTANCE/EventType)[1]', 'NVARCHAR(100)');
    DECLARE @ObjectName NVARCHAR(128) = @EventData.value('(/EVENT_INSTANCE/ObjectName)[1]', 'NVARCHAR(128)');
    DECLARE @SchemaName NVARCHAR(128) = @EventData.value('(/EVENT_INSTANCE/SchemaName)[1]', 'NVARCHAR(128)');

    INSERT INTO dbo.AuditLog (EventType, EventDateTime, UserName, SchemaName, ObjectName, SqlStatement, EventData)
    VALUES
    (
        @EventType,
        GETDATE(),
        SYSTEM_USER,
        @SchemaName,
        @ObjectName,
        @SqlStatement,
        @EventData
    );
END;
GO
```

Based on the figure above, the "AuditStructuralChanges" trigger uses the "EVENTDATA()" function to retrieve the event data in XML format. The captured event data will contain information about the DDL operation that fired the trigger, including the SQL statement, event type, object name, and schema name. The trigger extracts the relevant information from the event data XML and declares variables to store these values.

Once the necessary information is extracted just like in the figure below, the trigger will insert a new row into the "AuditLog" table. This row captures the event type, event date and time, username, schema name, object name, SQL statement, and the complete event data in XML format. By logging these details, the trigger provides a comprehensive audit trail for any changes made to the database schema.

Results Messages

	AuditLogID	EventType	EventData	EventDateTime	UserName	SchemaName	ObjectName	SqlStatement
1	1	CREATE_TABLE	<EVENT_INSTANCE><EventType>CREATE_T...	2024-04-23 19:40:16.363	LAPTOP-8ULJHU...	dbo	LoginHistory	CREATE TABLE LoginHistory (ID INT IDENTITY(1,1) PRI...
2	2	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:40:20.807	LAPTOP-8ULJHU...	dbo	RecordLogin	CREATE PROCEDURE dbo.RecordLogin @Succeeded ...
3	3	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:40:28.360	LAPTOP-8ULJHU...	dbo	RecordLogout	-- Procedure to record logout time CREATE PROCEDURE ...
4	4	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:40:32.163	LAPTOP-8ULJHU...	dbo	GenerateLoginLogoutReport	CREATE PROCEDURE dbo.GenerateLoginLogoutReport A...
5	9	CREATE_VIEW	<EVENT_INSTANCE><EventType>CREATE_VI...	2024-04-23 19:40:48.797	LAPTOP-8ULJHU...	dbo	StudentInfo	-- Create View for students and lecturers tables except for p...
6	10	CREATE_VIEW	<EVENT_INSTANCE><EventType>CREATE_VI...	2024-04-23 19:40:48.800	LAPTOP-8ULJHU...	dbo	LecturerInfo	CREATE VIEW dbo.LecturerInfo AS SELECT ID, Name, Ph...
7	17	CREATE_FUNCTION	<EVENT_INSTANCE><EventType>CREATE_F...	2024-04-23 19:41:01.150	LAPTOP-8ULJHU...	dbo	fn_securitypredicate_Student	CREATE FUNCTION dbo.fn_securitypredicate_Student(@St...
8	18	CREATE_VIEW	<EVENT_INSTANCE><EventType>CREATE_VI...	2024-04-23 19:41:05.930	LAPTOP-8ULJHU...	dbo	StudentAcademicData	CREATE VIEW dbo.StudentAcademicData AS SELECT s.ID...
9	22	CREATE_FUNCTION	<EVENT_INSTANCE><EventType>CREATE_F...	2024-04-23 19:41:12.747	LAPTOP-8ULJHU...	dbo	fn_securitypredicate_Lecturer	CREATE FUNCTION dbo.fn_securitypredicate_Lecturer(@I...
10	23	CREATE_VIEW	<EVENT_INSTANCE><EventType>CREATE_VI...	2024-04-23 19:41:17.247	LAPTOP-8ULJHU...	dbo	AllStudentsInfo	CREATE VIEW dbo.AllStudentsInfo AS SELECT ID, Name, ...
11	25	CREATE_VIEW	<EVENT_INSTANCE><EventType>CREATE_VI...	2024-04-23 19:41:22.537	LAPTOP-8ULJHU...	dbo	DepartmentResults	-- Create a view to view all marks entered by lecturers from t...
12	26	ALTER_VIEW	<EVENT_INSTANCE><EventType>ALTER_VIE...	2024-04-23 19:41:24.617	LAPTOP-8ULJHU...	dbo	DepartmentResults	ALTER VIEW dbo.DepartmentResults AS SELECT r.ID AS ...
13	30	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:41:37.190	LAPTOP-8ULJHU...	dbo	UpdateResult	CREATE PROCEDURE UpdateResult @ResultID INT, ...
14	31	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:41:39.940	LAPTOP-8ULJHU...	dbo	DeleteResult	CREATE PROCEDURE DeleteResult @ResultID INT, ...
15	35	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:42:00.367	LAPTOP-8ULJHU...	dbo	AddNewStudent	-- Stored Procedure for adding Student CREATE PROCED...
16	36	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:42:05.860	LAPTOP-8ULJHU...	dbo	AddNewLecturer	CREATE PROCEDURE dbo.AddNewLecturer @Lecture...
17	39	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:42:14.257	LAPTOP-8ULJHU...	dbo	UpdateStudentDetails	CREATE PROCEDURE dbo.UpdateStudentDetails @St...
18	42	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-23 19:42:23.080	LAPTOP-8ULJHU...	dbo	UpdateLecturerDetails	-- Lecturers to update their details. CREATE PROCEDURE ...
19	55	ALTER_FUNCTION	<EVENT_INSTANCE><EventType>ALTER_FU...	2024-04-23 19:57:38.687	LAPTOP-8ULJHU...	dbo	fn_securitypredicate_Student	-- Alter the function ALTER FUNCTION dbo.fn_securitypredi...
20	56	ALTER_FUNCTION	<EVENT_INSTANCE><EventType>ALTER_FU...	2024-04-23 19:57:48.917	LAPTOP-8ULJHU...	dbo	fn_securitypredicate_Lecturer	ALTER FUNCTION dbo.fn_securitypredicate_Lecturer(@ID ...
21	138	CREATE_TABLE	<EVENT_INSTANCE><EventType>CREATE_T...	2024-04-23 20:26:44.267	DBAdminLogin	dbo	test	Create Table dbo.test (Code varchar(7) primary key, Title v...
22	139	DROP_TABLE	<EVENT_INSTANCE><EventType>DROP_TAB...	2024-04-23 20:27:58.213	DBAdminLogin	dbo	test	Drop Table dbo.test
23	142	CREATE_TABLE	<EVENT_INSTANCE><EventType>CREATE_T...	2024-04-23 20:37:42.897	DBAdminLogin	DBAdminsSchema	Test	Create Table DBAdminsSchema.Test(name varchar(100) p...
24	143	DROP_TABLE	<EVENT_INSTANCE><EventType>DROP_TAB...	2024-04-23 20:38:26.610	DBAdminLogin	DBAdminsSchema	Test	Drop Table DBAdminsSchema.Test
25	144	CREATE_TABLE	<EVENT_INSTANCE><EventType>CREATE_T...	2024-04-26 12:01:48.400	LAPTOP-8ULJHU...	dbo	LecturerSubjects	CREATE TABLE LecturerSubjects (LecturerID varchar(6) ...
26	145	CREATE_PROCEDURE	<EVENT_INSTANCE><EventType>CREATE_P...	2024-04-26 12:10:52.417	LAPTOP-8ULJHU...	dbo	AddResult	CREATE PROCEDURE AddResult @StudentID varchar(6

4.4. Auditing Permissions Modifications

The auditing mechanism for permission modifications in the AIS database is implemented through the "AuditPermissionChanges" trigger. This trigger is defined at the database level and captures events related to granting, denying, or revoking database-level permissions, as well as adding or removing role members. It is executed whenever any of these permission-related operations occur.

```
CREATE TRIGGER AuditPermissionChanges
ON DATABASE
FOR GRANT_DATABASE, DENY_DATABASE, REVOKE_DATABASE, ADD_ROLE_MEMBER, DROP_ROLE_MEMBER
AS
BEGIN
    SET NOCOUNT ON;

    DECLARE @EventData XML = EVENTDATA();
    DECLARE @SqlStatement NVARCHAR(MAX) = @EventData.value('(/EVENT_INSTANCE/TSQLCommand)[1]', 'NVARCHAR(MAX)');
    DECLARE @EventType NVARCHAR(100) = @EventData.value('(/EVENT_INSTANCE/EventType)[1]', 'NVARCHAR(100)');
    DECLARE @ObjectName NVARCHAR(128) = @EventData.value('(/EVENT_INSTANCE/ObjectName)[1]', 'NVARCHAR(128)');
    DECLARE @SchemaName NVARCHAR(128) = @EventData.value('(/EVENT_INSTANCE/SchemaName)[1]', 'NVARCHAR(128)');
    DECLARE @PrincipalName NVARCHAR(128) = @EventData.value('(/EVENT_INSTANCE/PrincipalName)[1]', 'NVARCHAR(128)');

    INSERT INTO dbo.AuditLog (EventType, EventDateTime, UserName, SchemaName, ObjectName, SqlStatement, EventData)
    VALUES
    (
        @EventType,
        GETDATE(),
        SYSTEM_USER,
        @SchemaName,
        @ObjectName,
        @SqlStatement,
        @EventData
    );
END;
GO
```

Based on the figure above, the "AuditPermissionChanges" trigger is extremely alike to the "AuditStructuralChanges" trigger. This similarity in structure and implementation promotes code reusability and consistency within the auditing mechanisms of the AIS database. By leveraging a common approach, the database administrators can ensure a uniform auditing process across different types of events, simplifying the maintenance and future enhancements of the auditing system.

Results | Messages

AuditLogID	EventType	EventData	EventDateTime	UserName	SchemaName	ObjectName	SqlStatement
72	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.740	DBAdminLogin	NULL	AaronChia	ALTER ROLE Students ADD MEMBER AaronChia;
73	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.743	DBAdminLogin	NULL	MichealTan	ALTER ROLE Students ADD MEMBER MichealTan;
74	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.750	DBAdminLogin	NULL	Stainly	ALTER ROLE Students ADD MEMBER Stainly;
75	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.750	DBAdminLogin	NULL	Katty	ALTER ROLE Students ADD MEMBER Katty;
76	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.760	DBAdminLogin	NULL	PeterPark	ALTER ROLE Students ADD MEMBER PeterPark;
77	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.767	DBAdminLogin	NULL	LucasGreen	ALTER ROLE Students ADD MEMBER LucasGreen;
78	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.773	DBAdminLogin	NULL	EmmaWilson	ALTER ROLE Students ADD MEMBER EmmaWilson;
79	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.777	DBAdminLogin	NULL	IdrisElba	ALTER ROLE Students ADD MEMBER IdrisElba;
80	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.780	DBAdminLogin	NULL	NoraKhan	ALTER ROLE Students ADD MEMBER NoraKhan;
81	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.783	DBAdminLogin	NULL	HenryAdams	ALTER ROLE Students ADD MEMBER HenryAdams;
82	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:02:36.787	DBAdminLogin	NULL	SophiaTurner	ALTER ROLE Students ADD MEMBER SophiaTurner;
95	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.813	DBAdminLogin	NULL	AliceSmith	ALTER ROLE Lecturers ADD MEMBER AliceSmith;
96	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.820	DBAdminLogin	NULL	BobJohnson	ALTER ROLE Lecturers ADD MEMBER BobJohnson;
97	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.850	DBAdminLogin	NULL	CathyBrown	ALTER ROLE Lecturers ADD MEMBER CathyBrown;
98	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.853	DBAdminLogin	NULL	DavidClark	ALTER ROLE Lecturers ADD MEMBER DavidClark;
99	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.857	DBAdminLogin	NULL	EvaAdams	ALTER ROLE Lecturers ADD MEMBER EvaAdams;
100	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.860	DBAdminLogin	NULL	FrankMorris	ALTER ROLE Lecturers ADD MEMBER FrankMorris;
101	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.860	DBAdminLogin	NULL	JaneMiller	ALTER ROLE Lecturers ADD MEMBER JaneMiller;
102	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.863	DBAdminLogin	NULL	MikeBarnes	ALTER ROLE Lecturers ADD MEMBER MikeBarnes;
103	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.867	DBAdminLogin	NULL	SusanLee	ALTER ROLE Lecturers ADD MEMBER SusanLee;
104	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.870	DBAdminLogin	NULL	AlanTuring	ALTER ROLE Lecturers ADD MEMBER AlanTuring;
105	ADD_ROLE_MEM...	<EVENT_INSTANCE><EventType>ADD_ROLE_MEMBER</Ev...	2024-04-23 20:03:04.870	DBAdminLogin	NULL	CarolWhite	ALTER ROLE Lecturers ADD MEMBER CarolWhite;

Based on the figure above, by implementing this auditing mechanism, the AIS database enhances its overall security and compliance by providing a detailed record of who made what changes to permissions and when, enabling effective monitoring and investigation of potential security incidents or policy violations.

4.5. Auditing Login and Logout

The last auditing mechanism for the login and logout events in the AIS database is implemented through a combination of a table and stored procedures. This approach ensures that login and logout activities are properly recorded and monitored, providing valuable information for security and compliance purposes.

```
-- Auditing for login and logout
-- Create Table to store login history
CREATE TABLE LoginHistory (
    ID INT IDENTITY(1,1) PRIMARY KEY,
    UserID NVARCHAR(100),
    LoginTime DATETIME,
    LogoutTime DATETIME NULL, -- Initially NULL, to be updated on logout
    Succeeded BIT -- 1 for successful login, 0 for failed login
);
```

Firstly, a “LoginHistory” table is created to store the login and logout records for all the users in the AIS database. In the figure above, the table contains columns to store either the student’s ID or the lecturer’s ID, the login time, the logout time, and a “bit”, to indicate whether the login attempt was successful or not (Gigoyan, n.d.).

```
-- Procedure to record login time
CREATE PROCEDURE dbo.RecordLogin
    @Succeeded BIT
AS
BEGIN
    DECLARE @UserID NVARCHAR(100);
    DECLARE @LoginName NVARCHAR(100) = ORIGINAL_LOGIN();

    -- Try to get the student ID
    SELECT TOP 1 @UserID = ID
    FROM dbo.Student
    WHERE ID = @LoginName;

    -- If not found, try to get the lecturer ID
    IF @UserID IS NULL
    BEGIN
        SELECT TOP 1 @UserID = ID
        FROM dbo.Lecturer
        WHERE ID = @LoginName;
    END

    -- If a match is found in either table, record the login
    IF @UserID IS NOT NULL
    BEGIN
        INSERT INTO LoginHistory (UserID, LoginTime, Succeeded)
        VALUES (@UserID, GETDATE(), @Succeeded);
    END
END;
GO
```

```
CREATE PROCEDURE dbo.RecordLogout
AS
BEGIN
    DECLARE @UserID NVARCHAR(100);
    DECLARE @LoginName NVARCHAR(100) = ORIGINAL_LOGIN();
    DECLARE @HistoryID INT;

    -- Try to get the student ID
    SELECT TOP 1 @UserID = ID
    FROM dbo.Student
    WHERE ID = @LoginName;

    -- If not found, try to get the lecturer ID
    IF @UserID IS NULL
    BEGIN
        SELECT TOP 1 @UserID = ID
        FROM dbo.Lecturer
        WHERE ID = @LoginName;
    END

    -- If a user ID is found, update the logout time for the most recent login record
    IF @UserID IS NOT NULL
    BEGIN
        SELECT TOP 1 @HistoryID = ID
        FROM LoginHistory
        WHERE UserID = @UserID AND LogoutTime IS NULL
        ORDER BY LoginTime DESC;

        -- Update the LogoutTime for the identified record
        IF @HistoryID IS NOT NULL
        BEGIN
            UPDATE LoginHistory
            SET LogoutTime = GETDATE()
            WHERE ID = @HistoryID;
        END
    END
END;
GO
```

Then 2 procedures were created to store the record of login and logout, respectively in both "RecordLogin" and "RecordLogout" stored procedures in the AIS database. These 2 procedures in the figures above share a similarity in their implementation and work together to capture login and logout events for users of the system, with "RecordLogin" responsible for recording login attempts and "RecordLogout" for updating the logout time when a user logs out.

In the case of "RecordLogin", a new record is inserted into the "LoginHistory" table, capturing the user ID, current date and time as the login time, and the success status. On the other hand, "RecordLogout" updates the logout time for the most recent login record in the "LoginHistory" table, setting the "LogoutTime" column to the current date and time.

```sql
-- Procedure to generate login & logout report for DBAdmins
CREATE PROCEDURE dbo.GenerateLoginLogoutReport
AS
BEGIN
    IF IS_MEMBER('DBAdmins') = 1 OR IS_SRVROLEMEMBER('sysadmin') = 1
    BEGIN
        SELECT *
        FROM LoginHistory
        WHERE CAST(LoginTime AS DATE) = CAST(GETDATE() AS DATE);
    END
    ELSE
    BEGIN
        THROW 50000, 'You do not have permission to generate the report.', 1;
    END
END;
GO
```

Finally, the figure above is the "GenerateLoginLogoutReport" stored procedure, it is designed to generate a report of login and logout activities for the current day. This procedure checks if the executing user is a member of the "DBAdmins" role or has the "sysadmin" server role. If the user has the required permissions, it retrieves and displays all login and logout records from the "LoginHistory" table for the current date, just like in the figure below.

Results | Messages

	ID	UserID	LoginTime	LogoutTime	Succeeded
1	4	LC1002	2024-04-26 12:30:40.073	2024-04-26 12:30:40.087	1
2	5	LC1003	2024-04-26 19:44:53.627	2024-04-26 19:44:53.653	1
3	6	LC1003	2024-04-26 21:26:28.847	2024-04-26 21:26:28.850	1
4	7	ST1001	2024-04-26 21:27:32.133	2024-04-26 21:27:32.147	1

By implementing this auditing mechanism, the AIS database can keep track of all login and logout activities, including successful and failed login attempts. The centralized "LoginHistory" table serves as a repository for this information, while the stored procedures provide a structured way to record and retrieve login and logout data.

5. Summary

In the case for an educational institution like a school, the database will certainly contain sensitive data about students, lecturers, and academic records. If a database system did not utilize any kind of security measurement, malicious attackers could grant access to the data, which would lead to privacy breaches, data corruption, or even legal implications. Hence, the objective of this project is to ensure that the AIS database system can protect the sensitive data and the users can only access and change information based on their authorized roles and permissions.

This led to the need for implementing security features for the fundamental principle of the CIA triad. By implementing role-based access control (RBAC) and permission controls in the database, the system ensures that users can only perform operations that are within the scope of their assigned roles. The database also implements both symmetric key encryption and transparent data encryption, as well as enabling secure backup and recovery mechanisms to safeguard against data loss or unauthorized access.

The incorporation of features like temporary passwords for new accounts, password changes requirement upon first login, and audit logging further enhances the security of the database. By implementing multiple layers of security controls in the database, such as access control, encryption, auditing, and monitoring, the system can effectively mitigate various threats and vulnerabilities, ensuring the confidentiality, integrity, and availability of sensitive data within the database.

6. References

Ahmed, I. (2022, December 27). *Transparent Data Encryption (TDE)*. Percona Database Performance Blog. https://www.percona.com/blog/transparent-data-encryption-tde/

Berning, T. (2023, July 3). *What is Row-Level Security?* NextLabs. https://www.nextlabs.com/what-is-row-level-security/

Filip Holub. (2020). *Configure SQL Server Transparent Data Encryption with PowerShell*. Www.mssqltips.com. https://www.mssqltips.com/sqlservertip/6316/configure-sql-server-transparent-data-encryption-with-powershell/

GeeksforGeeks. (2020, June 5). *Advantages and Disadvantages of Using Stored Procedures - SQL*. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-using-stored-procedures-sql/

geeksforgeeks.org. (2022, January 16). *What is Data Encryption?* GeeksforGeeks. https://www.geeksforgeeks.org/what-is-data-encryption/

Gigoyan , S. (n.d.). *SQL Server Bit Data Type*. Www.mssqltips.com. https://www.mssqltips.com/sqlservertip/6447/sql-server-bit-data-type/

Kananda, V. (2022, June 22). *What is AES 256 Encryption & How Does it Work?* Progress Blogs. https://www.progress.com/blogs/use-aes-256-encryption-secure-data

Malhotra, H. (2022, December 9). *Data Activity Tracking Using SQL Triggers*. SQLServerCentral. https://www.sqlservercentral.com/articles/data-activity-tracking-using-sql-triggers

ManageEngine. (2022, February 10). *Understanding SQL Server Audit better*. ManageEngine. https://www.manageengine.com/products/eventlog/logging-guide/understanding-sql-%20server-audit.html

NetApp.com. (2023). *What Is Backup and Recovery? - Why It's Important | NetApp*. Www.netapp.com. https://www.netapp.com/cyber-resilience/data-protection/data-backup-recovery/what-is-backup-recovery/

Pavel, P. (2022, October 17). *Database Views: What You Need To Know*. Aristek Systems. https://aristeksystems.com/blog/database-views-what-you-need-to-know/

Ravikiran. (2021, May 10). *Stored Procedure in SQL: Benefits And How to Create It*. Simplilearn.com. https://www.simplilearn.com/tutorials/sql-tutorial/stored-procedure-in-sql

Richardson, B. (2019, October 11). *Working with XML Data in SQL Server*. SQL Shack - Articles about Database Auditing, Server Performance, Data Recovery, and More. https://www.sqlshack.com/working-with-xml-data-in-sql-server/

SatoriCyber. (2023, November 2). *Database Auditing*. Satori. https://satoricyber.com/cloud-data-governance/database-auditing/

SecurePass. (2021, March). *Role-Based Access Control Management System*. Www.thesecurepass.com. https://thesecurepass.com/blog/role-based-access-control-system

Szentgyorgyi-Siklosi, A. (2023, July 6). *What is a Data Classification Matrix?* Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/what-is-a-data-classification-matrix/

Team Post. (2022, April 7). *What is a Database View? (And How Does It Help Business Intelligence)*. Dashboardfox.com. https://dashboardfox.com/blog/what-is-a-database-view-and-how-does-it-help-business-intelligence/

TutorChase. (2023). *What are the advantages and disadvantages of using a view in SQL?* Tutorchase.com. https://www.tutorchase.com/answers/a-level/computer-science/what-are-the-advantages-and-disadvantages-of-using-a-view-in-sql

Uikey, P. (2023, March 17). *What is Stored Procedure in SQL? | DataTrained*. DataTrained. https://datatrained.com/post/stored-procedure-in-sql/#:~:text=A%20stored%20procedure%20is%20a

Zahid, A. (2023, April 13). *What is Row Level Security in SQL? What are Best Practices and How to Implement them?* Medium. https://mrasimzahid.medium.com/what-is-row-level-security-in-sql-what-are-best-practices-and-how-to-implement-them-696f016718bb