Bachelor's thesis

Information and Communications Technology

2024

Jigar Parekh

# Development of an Appoint Nord with Data Security

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2024 | 40

Jigar Parekh

# Development of an Appoint Nord with Data Security

This thesis describes the design, implementation, and evaluation of a scheduler for appointment booking, which tries to improve the scheduling process, Furthermore, improving customer´s experience and satisfaction towards various service provider scenarios. Strong data security is an essential part of the development process in this thesis. The application has been specifically designed to protect sensitive user information. It has employed advanced methods to secure and protect personal data of users alongside employing improved techniques of encryption, secure transmission protocols and multifactor authentication systems without requirement of password storage.

For enhanced data security, the application used a tier-based system. For Front-end development, the application has implemented use of various HTML/CSS and Bootstrap elements to achieve security of the data goal. Additionally, for Back-end development, PHP and Laravel have been used for security modules. This approach has ensured confidentiality, integrity, and availability of information for the users on the platform.

The aim to ensure data security for user information has been based on principle of confidentiality, integrity, and accessibility. This method enables sustainable protections against unsolicited and unauthorized access, data theft, and malicious actions. Key feature of the application is safeguarding user´s data and making the booking system a safe and reliable platform.

Keywords: Data Security, Appointment Scheduling, Data Protection, Encryption, Authentication, Authorization, MySQL, HTML/CSS, Bootstrap, PHP, Laravel.

# Contents

# Figures

## List of abbreviations

AES Advanced Encryption Standard

CSS Cascading Style Sheet

CSRF Cross-Site Request Forgery

GDPR General Data Protection Regulation

HTML Hypertext Markup Language

IDS Intrusion Detection Systems

MySQL My Structured Query Language

MITM Man In The Middle

MFA Multi-Factor Authentication

ORM Object Relational Mapping

OTP One Time Password

PHP Hypertext Preprocessor

PACS Physical Access Control System

RSA Rivest Shamir Adleman

RBAC Role Based Access Control

SSL Secure Sockets Layer

SMS Short Message Service

SPs Service Providers

SIEM Security Information and Event Management

TLS Transport Layer Security

# 1 Introduction

With the constant pace of the digital age today, effective scheduling is becoming increasingly important in numerous industries including healthcare, hospitality, and personal services. The new normal for appointment booking is an intuitive, reliable system that customers anticipate rather than merely hope for as reliance on online systems increases more than ever to manage their appointments. Brands that cannot deliver simple scheduling solutions will see customers going to competitors with more sophisticated, consumer-centric scheduling software.

However, as demand for convenience increases, so does concern about data security. Cyber threats are advancing, and organizations need to safeguard confidential information to prevent it from unauthorized access and breaches. Maintaining a core security for personal data must be kept confidential, integral to the services they provide and made available to as highly trusted in any online service, even more for an appointment booking platform.

The thesis explores the methods to design and develop a secure appointment booking system which helps to book time for businesses and also focuses on protecting the user data. Using strong security features such as encryption, multi-factor authentication, and role-based access control, thus it seeks to improve aspects such as operational efficiency, lower no-show costs, and confidence in the customer by protecting sensitive data at every stage of the booking process.

## 1.1 Introduction to Data Security Concerns

The rise of online appointment scheduling platforms has brought concerns about data security. For example, the username and contact information or appointment details are confidential. Data breaches are dangerous as they can cost an organization financial losses, reputation damage and also legal penalties (Sobers, 2022).

User data protection requires stable security measures. There need to be strong measures in place for identity theft or data breaches, especially in industries

handling (and storing) sensitive personal information; these industries include healthcare but also finance and services. The main canons of data security include confidentiality, integrity, availability, and authentication (Alder, 2024; European Union, 2016).

## 1.2 Scope and Objective

A proficient appointment booking system is a vital factor in the success of operational and client satisfaction. Businesses that automate and streamline this booking process ensure a better user experience as well as save time. Additionally, in a technologically inclined world here today where the demand for convenience is prioritized in every aspect convenience out of everything, an easy-to-use and safer booking system is also undoubtedly obligatory.

This thesis focuses on the incorporation of sophisticated security controls such as data encryption, secure communication protocols, and multi-factor authentication. These security measures are essential to retain user data safely while it is being stored and moved through the internet, thus avoiding unauthorized acquisition or a leak of this information. Moreover, the system's handling of personal data is aligned with existing legal requirements, balancing the dual priorities of security and usability. The proposed system seeks to enhance user confidence while providing an efficient appointment booking experience.

# 2 Data Security Overview

Data security is a big concern today because people are creating more data online than ever before, and it's happening at an incredibly fast pace. This worry is exacerbated by the skills and experience of threats facing such forms, as these are becoming more frequent, a growing threat actor sophistication poses. This means stricter methods are needed for the security of confidential data. This chapter introduces the concept of information security, covering its importance and the challenges systems face without adequate security. It also examines the necessity of implementing stronger security measures for online applications.

## 2.1 What is Data Security?

Data security means ensuring digital information protection against unauthorized access, disruption, and corruption over the entire lifecycle of it. It includes actions, programs, and procedures designed to minimize unauthorized access to and transmission of confidential information while retaining the associated risks. Central to all data protection systems are the three core pillars: Insightful when personal data management is in an appointment scheduling system (Vacca, 2020).

### Confidentiality

This is the property that ensures sensitive information will not be disclosed to others who are unauthorized. This is critical for an appointment booking system, as only authorized users and service providers should have access to appointment schedules (Microsoft, 2022).

### Integrity

This means that the data stored in the database is always accurate and does not change. In the context of an appointment system, integrity means making sure

that booking records cannot be modified without having proper credentials (NIST 2022).

### Availability

Availability ensures that access to data or resources is maintained whenever required by authority users. For instance, if the website used by customers to book their appointments is unexpectedly unavailable for several hours, as occurred with Hostinger a few days earlier, and service providers also encounter issues accessing Slot Appointment, it indicates that something is malfunctioning right (Vacca, 2020).

Availability involves the employment of data security measures techniques such as encryption, access control, and other authentication methods to secure stored information from those with malicious intent. For example, employing encryption to secure data at rest and in transmission could store the plaintext of such data; a ciphered copy would be made unusable without knowledge of how to retrieve its decrypted key (Microsoft, 2022). The identity of users is confirmed, and the exact level of permissions that their roles in this system imply are through process checks such as authentication and authorization (Alder, 2024).

## 2.2 Challenges faced in Data Security

While the number of potential points for breaches has increased as technology adoption continues at an unprecedented rate, enforcing data security is critical, but then the enforcement has a suite of a number of complexities that concern scale-out threats and modern systems. Here are some of the issues that mattered most.

### Sophistication of Cyber Attacks

The security system faces a tough battle with the continuous development that cybercriminals perform every minute they are awake trying to hack it. Methods like phishing, ransomware, or Man-in-the-Middle (MITM) attacks have been on a

rampant rise in attacking both users and the system where sensitive data resides (Sobers, 2022). As a result of these dynamic threats, organizations will have real difficulties continuing their security protocols.

HumanError

Human error accounts for a large percentage of data breaches, from poor password hygiene to a lack of phishing awareness training to no proper controls around sensitive information. The authors suspect the album could be especially sensitive in connection to online appointment systems, which represent a two-way pipe for data breaches and involve not just service users but also providers (Verizon, 2023).

Credential compromise, phishing, and exploiting vulnerabilities as three of the major attack vectors that allow initial access to the breaches (Figure 1). These tactics are commonly associated with ransomware and extortionary threat actors, significantly increased in prevalence, with a 180% rise in the exploitation of vulnerabilities due to incidents such as MOVEit and zero-day exploits. Web applications remain a primary target for these methods.

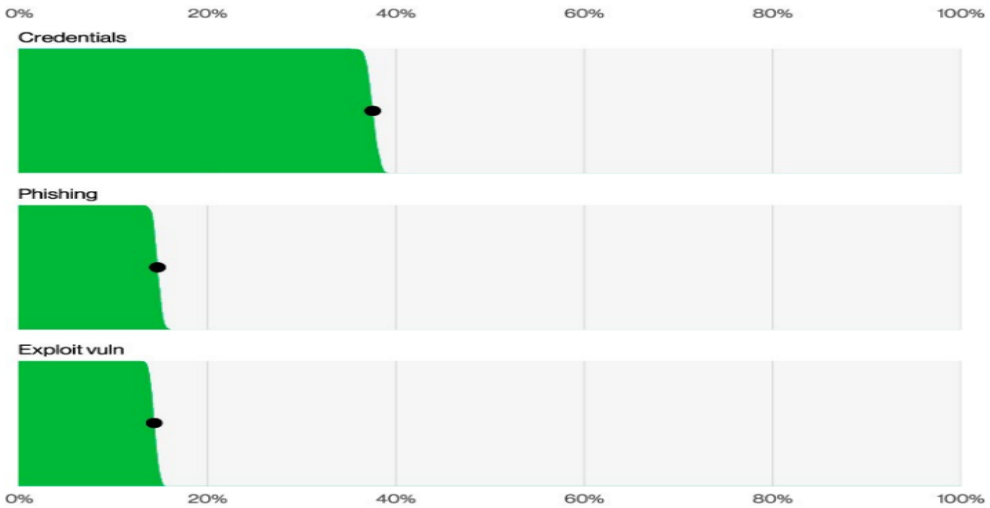

Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963) (Verizon, 2023).

Implementing better password policies, phishing education for users, and proper patching systems to be on constant alert for new vulnerabilities, which target web applications. Concentrating upon these elements can deter several breaches due to human error and software flaws. (Figure 1).

## Data in Transit

Another important aspect is the security of data, as it may pass from client to server and vice versa. If encryption is not used, data sent over a channel can be read and, in the worst case, repurposed or leaked. Running commands in a shell or unencrypted traffic for communicating is discouraged; data at rest must be encrypted, and the management of applications using secure protocols like TLS (Transport Layer Security) is imperative (Microsoft, 2022).

## Data at Rest

Data in rest is any information that is not transmitted between the source and destination, i.e., an actual storage of this data on various devices or even databases, say the user's own stored info at servers or within storage systems. Ensuring data at rest is secure; it is information that may be vulnerable to unauthorized access and so represents the long-term storage of such an item. By encrypting the data itself using some kind of encryption protocol, such as AES-256 in this case, it ensures that even if someone steals hard drive, they will not be able to access anything on there without having the appropriate decryption key.

Moreover, Tamper-proof, or log-able controls may be used to ensure that only authorized individuals can access the data stored on and viewed through PACS (NIST, 2001).

### Data in Process

Data in process refers to data currently being used or operated on by some software. This happens when a user of an app inputs information or the system performs calculations on existing data. Data is housed temporarily in memory to support the processing phase, but that makes it vulnerable too because stored unencrypted data can be easily scraped from its residing space by a type of threat called memory scraping. The way to lock up data in this state is through secure coding practices and access control mechanisms, which keep it safe even while an application has a live connection (NIST, 2018).

### Complexity of Security Management

This includes anything from cloud services to distributed databases and real-time applications that form some sort of end-to-end pile, having several layers. Protection depends on the tier being used to store or process data, which complicates matters by adding different vulnerabilities at each tier. If a network module communicates with the web server, it can be hard to ensure safety for all devices (Vacca, 2020).

## 2.3 Importance of Data Security for Online Applications

It is also very important that data security should be a priority for the user so that their information shall be safe. Most of the time, online applications process volumes of sensitive personal and financial information. For instance, in an appointment scheduling application, the scheduler will collect the user's name, location address, and contact number along with the desired time slot. In many cases, this could also be payment information or sensitive private health procedures, depending on the service. Data protection policies must be enforced, not only to comply with legal requirements but also to foster user trust and confidence.

### Customer Trust and Satisfaction

Awareness of the risks involved in sharing personal data online has fortunately grown extensively over the years. Exactly, and when a service provider gets breached, that trust is extremely hard to gain back. Findings show that in 2023, over 85% of individuals say they are not doing business with companies who have been the victims of a data breach (Ponemon Institute, 2023). As such, appointment booking platforms should maintain customer confidence by keeping user data safe to a greater extent of irreversibility in terms of business loss.

### Preventing Financial Losses

The fiscal impact of a breach goes beyond merely fines and, in this day-and-age litigious society, can also cause lawsuits from individuals who experienced the incident as well. According to the Ponemon Institute, an average data breach costs around $4 million (Ponemon Institute, 2023), which is why a majority of organizations consider money spent on security protocols as preventive finance more than spending.

### Strengthening Overall Security Posture

Persistent systems rely on data security. Encryption, firewalls, and intrusion detection systems (IDS) are other measures that help cause an organization to be difficult (or impossible) to conquer by cyber threats. By encrypting data, cybercriminals, even if they managed to get through, will not be able to access the stolen information either due to encryption keys that are necessary for decryption (Vacca, 2020). IDS also gives insightful monitoring for unusual patterns or activity, helping protect the network environment against outside attacks as well as inside vulnerabilities (Microsoft, 2022).

### Data-Driven Decision Making and Business Continuity

Data security is essential to prevent data loss, aiding companies in making their decisions based on secure and correct inputs. Businesses can be certain that

their data is reliable and thus have confidence in the information it provides, which allows them to make effective decisions, and not conduct business based on inaccurate or out-of-date info (Vacca 2020). When it comes to the world of appointment scheduling systems, this means logging on to user requirements successfully, analyzing booking trends, and improving operational efficiency. Above that, secured systems are important for ensuring business continuity in the face of security breaches or cyberattacks shutting down a system and thus causing financial damages.

# 3 Project

This chapter thoroughly evaluates the novel way of implementing the appointment booking system in this project. It includes the architecture design part of the system and gives an idea over what needs to be considered during designing and how security protocols can maintain user data privacy settings. The final implementation aims to address common scheduling challenges while providing a secure platform for service providers (SPs) and their clients.

## 3.1 Project Description

Designed amidst a growing requirement for streamlined, convenient scheduling options, this appointment booking system is developed to cater toward numerous industries, such as healthcare and legal services in addition to the beauty industry. This system will help to schedule appointments with service providers and allow a prominent level of security in data encryption during the entire operation. The main objective of this technological scheme is to provide a secure, scalable, and self-service platform that protects confidential client data, which includes personal information or doctor visit records, from unauthorized access or intrusion by cyber threats (Sobers, 2022).

Appointment Booking System Basic functionality of the system to book, cancel, and amend an appointment. It includes customer appointment tracking, schedule management, and operational reporting in single software. In addition, the system allows different user roles, such as customers and service providers, to be given specific access privileges within the online platform so that data is kept secret while ensuring continuity (Alder, 2024).

## 3.2 System Architecture and Design

The system architecture is designed using multiple layers to enhance functionality and security. It works by using an assortment of technologies on the

web to make development easier, more responsive, and adaptable. The Overall System consists of three main parts:

### Front-End

Responsive and user-friendly interface, work on all devices developed the front-end in HTML5, CSS3, Bootstrap. It uses JavaScript for client-side validation to make sure that the input of users is secure, and they get it processed by the back end (Microsoft, 2022).

### Back-End

The back end is developed using PHP with the help of Laravel framework, a framework that has built-in security practices like Cross-Site Request Forgery (CSRF) protection, password hashing & secure session management out-of-box (Laravel, 2024). Laravel leveraging the ORM (Object-Relational Mapping) capabilities of Laravel, database interactions can be executed much easier for safer data handling.

### Database

It is based on MySQL as a database service that approaches encryption-at-rest (encrypting all data in the disk) to secure sensitive information like customer details, appointment records and so forth. Use of Prepared Statements for Executing Database Queries: Express prepared statement is a feature that helps to reduce the risk of SQL injection attacks (Vacca, 2020).

## 3.3 Security Measures

Solutions are partially a matter of designing security in. The following steps have been taken to ensure user data is kept confidential, and that the integrity and availability of this same data are maintained:

### Data Encryption

User information and appointment data are secured using AES-256 encryption. Data in transit is protected using TLS encryption to prevent interception of communications between the client and server (Microsoft, 2022).

### Multi-Factor Authentication (MFA)

MFA is used for service providers and administrators, which makes them authenticate multiple times to prove themselves as members (Alder, 2024).

### Role-Based Access Control (RBAC)

RBAC can work as a solution to make only such functionality and data available for the user that he needs according to his Role. Only customers are allowed to access their information the providers and administrators can see them as required by their roles (NIST, 2022).

### Audit Logging

All access and modifications to the system are fully monitored with detailed audit logs, recording who accessed or changed what. These logs are very instrumental in finding security issues, understanding user activity, and ensuring that the system is operating within set rules and regulations, according to (Ponemon Institute, 2023).

## 3.4 Technologies Used

The system is built using trusted tools and techniques to make sure it is secure, can handle growth, and works well. Here are the main technologies and platforms used:

PHP and Laravel

They are used for secure web development at the back-end, providing its users with several security features: CSRF protection as well password hashing which is layered (Laravel, 2023).

MySQL

This is a database management system with encryption-at-rest in place to secure the sensitive data (Vacca, 2020).

HTML5, CSS3, and Bootstrap

It is used for creating a modern website which helps in the seamless experience of users in different devices using these technologies on other parts, as it deals with responsive aspects (MDN Web Docs, 2023).

JavaScript

It Is used for client-side validation, to ensure data integrity before it is sent back-end (Microsoft, 2022).

TLS

This protocol is implemented for secure data transmission, guaranteeing that user information remains protected during its transfer between the client and the server (Cloudflare,2023).

## 3.5 Challenges and Solutions

Building a secure appointment booking system was not easy. The development of the booking system was particularly challenging due to the requirement to integrate various security features seamlessly. A major issue was also having an affordable and user-friendly multi-factor authentication (MFA). In the solution, MFA was put in place for convenience using simple verification methods, such

as OTP via email. The performance of a storage system that processes encrypted data was a significant challenge to address. This limitation was addressed by selecting encryption algorithms that achieve a balance between security and performance, for example, using AES-256 (Sobers, 2022).

### 3.6 Future Enhancements

While the system in place currently satisfies functionally all our project goals, there are various improvements that could be made to make things more secure and functional. Possible improvements might include using machine learning to automatically identify security threats on the fly, extending language support so that it is convenient for more potential users in different parts of the world, and implementing advanced capabilities ranging from appointment reminders via SMS all the way up to integration with 3rd party payment processors.

# 4 Business Objectives for Secure Appointment Booking

The advancement of a secure appointment booking system is driven by various business objectives. This section outlines the primary goals and aims, focusing specifically on the integration of user-friendly security features that adhere to relevant regulations and enhance business operations.

## 4.1 Improved User Convenience with Secure Data Handling

It begins with improving the quality of service for users by focusing on secure management of confidential data. It is essential to ensure that customers' confidential information, such as names, addresses, phone numbers, and booking details, remains safe from leaks or theft. The adoption of encryption and multi-factor authentication empowers users to book appointments without concerns about data theft or identity breaches. Studies have shown that 60% of online shoppers abandon a potential online purchase if they feel their data is too vulnerable (Ponemon Institute, 2023) A thoughtful security model accordingly strengthens user trust in addition to driving conversions and retention.

## 4.2 Enhanced Service Provider Visibility and Accessibility through Secure Data Storage

To make this a reality, there are only two answers: Service Providers would use robust storage solutions for handling the information effectively and to have great services, it will store all customer information. They securely store sensitive information such as appointment records and customer preferences to enable a personalized service that improves the company fitness level. In addition, protecting this information lowers the risk of data breaches and minimizes the operational repercussions of losing or having corrupted important business data. Data storage also allows service providers to understand data from their services (Vacca, 2020), which in turn aids them to improve upon customer preferences when and as needed while abiding by strict security policies.

### 4.3 Effective Administrative Control and Monitoring of Data Access

Above all, effective management is essential to protecting an appointment booking system since it confirms that the sensitive information available in these systems can only be accessed by authorized individuals. One common approach is using role-based access control (RBAC) for this. This makes it impossible for users to see only the relevant information pertaining to their roles. Managers might have access to more thorough data, and the regular employees would mostly be just provided with customer information basic enough for them to do their job (Anderson, 2020).

In addition to deploying role-based access control (RBAC), systems must deploy monitoring solutions that provide a data point for access and alert if there are any unauthorized attempts at accessing classified information. For instance, access logs constitute a full log of what each user interacts with on the system, and at times they did so. Going over the logs often allows administrators to see anything that is out of place and then act before any danger occurs. Monitoring is essential for security that guarantees user data security must not be fetched (Anderson, 2020).

### 4.4 Revenue Generation and Business Expansion through Secure Data Analytics

Secure data analytics have an undeniable impact on financial returns and business improvements. This provides companies with a way to collect and analyze customer data in connection with what a consumer wants or how they are using something. These insights can also assist in increasing service delivery and customer experience. For instance, a business can gauge the type of staff and required resources depending on when bookings occur. Marketing campaigns that offer feedback on their behavior promote them to be more engaged and enhance loyalty (Alder, 2024).

Given that a breach can led to financial and reputational harm for the firm, it is carrying out data collection right, then. They leverage it for operational decision-making and to maintain corporate trust with customers, who are increasingly

consumed by how their data is being utilized. In the data-driven market of today, utilizing geographically tabulated information can serve as a significant time-saver or provide a competitive advantage (Vacca, 2020).

### 4.5 Data-driven Decision-Making and Continuous Security Improvement

The most critical value data science brings in the age of the digital revolution are its abilities to analyze device data and convert that into intelligent action outputs as organizations continue their journey toward excellence. Advanced appointment systems provide organizations with unique insights to operate efficiently, understand customer behavior, and identify security threats. And with this knowledge, they can not only enhance their service offerings but also reinforce the security of those services. For example, a company should be able to notice usage or most frequent security weaknesses and fix these before they become bigger issues (Verizon, 2023). This approach ensures an incremental improvement in both security and service quality.

### 4.6 Compliance with Data Security Regulations

For businesses managing sensitive customer data, such as personal details and appointment records, compliance with regulations like the General Data Protection Regulation (GDPR) is essential. GDPR mandates how personal information should be securely handled, stored, and processed to ensure data privacy and protection against breaches.

The European Union's General Data Protection Regulation (GDPR) means that personal data must be responsibly and securely managed. Individuals have rights concerning their personal data, including the rights of access, correction, and opposition. Companies that fail to comply with the GDPR could receive heavy fines, which can be as high as 4% of an undertaking's turnover or €20 million (whichever is greater); however, other potential business impacts need to be considered too (European Union, 2016).

Personal information such as the name, contact information details of users, and scheduling are guaranteed securely encrypted and shall have access to users with authorization only. This explanation discloses how user details shall be used while maintaining this control over the user through applicable means of consent. There may also be a follow-on program in data retention policies for storing information no longer than called upon for operational use in functions. In that respect, solid security measures have been implemented, including encryption, multi-factor authentication, and role-based access control, to ensure full compliance with the GDPR by building trust with its users regarding preventing unauthorized access and any breach of data. That also goes in line with the role of this system: it is supposed to be an easy, user-friendly, secure platform for scheduling.

### 4.7 Customer Satisfaction and Retention through Secure Data Protection

Protecting information is important to uphold the needs of customers and gain loyal clients. In an era marked by frequent data breaches, consumers are increasingly concerned about the security of their personal information. By instituting secure appointment booking applications, organizations signify dedication to guard customer details, hence increasing trust and loyalty (Ponemon Institute, 2023). Even though customers will tend to stay with a business longer when they trust them, it enhances their satisfaction as well since people usually keep using services from companies that have shown reliability.

# 5 Comprehensive Data Security Policy

A comprehensive data security plan is crucial to securing confidential information against unauthorized access, breaches, and cyber threats. This chapter describes data security planning; respectively, this is the use of encryption, which means passwords for access control, but also to protect user privacy and compliance with certain standards that must be taken into account when creating an appointment system.

## 5.1 Introduction to Data Security Measures

It ensures privacy, accuracy, and usability of the data. These controls help mitigate the risk of improper access, unauthorized changes, and potential exposure to cyber threats. Encryption and access control ensure that unauthorized individuals cannot read or write sensitive data. These mechanisms, combined with authentication protocols, verify user identities and protect sensitive information as it is transmitted between systems and access points (Vacca, 2020).

## 5.2 Data Encryption and Secure Transmission

The simplest way of securing data is encryption. Data encryption is the process of converting plain text into an unreadable format, i.e., ciphertext, using algorithms like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). So even if data is intercepted in transit, the unauthorized party has no ability to make sense of it and use it for anything because they lack access (Kozierok, 2005).

These methods used for secure data transmission use TLS, which encrypts the transferred data from client to server. This encryption uses the same end-to- end data encryption and secure transmission methods as Microsoft 365 to safeguard sensitive user information like personal details and booking data from potential threats (Microsoft, 2022).

## 5.3 Access Control and Authentication Mechanisms

The implementation of such access control protocols ensures that certain pieces of information or components in functional systems can only be accessed by individuals who have already been specified and pre-authorized. First, the data should be organized into structured layers but with sufficient access restrictions according to needs, for example, a departmental hierarchy can be created using role-based access control (RBAC). It is critical to clearly define and control access to specific data based on user roles In addition to this protection, the use of multi-factor authentication (MFA) further secures and protects user accounts by requiring users to provide two or more forms of verification types, such as a password along with a one-time code sent on their mobile phones (Anderson, 2020)

## 5.4 Data Backup and Recovery Procedures

Backups are necessary in case of a system crash, power failure, or data corruption, as backups allow recovery of information. Specially scheduled backups are filed in secure locations and usually encrypted so they cannot be easily hijacked. A meticulously planned archival backup and retrieval system is designed to minimize downtime and ensure the appointment system is restored promptly after any incident. The data recovery of the previous schedules and personal information will also minimize the possibility of losing sensitive user details (Vacca, 2020).

## 5.5 User Consent and Data Privacy

This uses the Axios library and is based on explicit user consent. It is important to notify the users about the data being collected, its use, and storage, and to obtain explicit permission before processing such information. This ensures the security framework is far stronger in the overall trust model. An efficient appointment booking system should enable users to manage their private information and data collection policies effectively. To enable this, user information should be subject to modification or erasure at the whims of users

(Vacca 2020), thereby fostering a transparent and user-centric data privacy practice.

The system must contain user interfaces that support easy and successful management of privacy settings, allowing users to easily make informed decisions about their data. Enabling a way for the users to cancel their agreement and request removal of information aligning with security best practices can improve user confidence (Sobers, 2022). This model enhances security even further because it protects sensitive data while giving individuals full control of their personal data.

### 5.6 Data Retention and Disposal Policies

Data retention policies address how long personal data will be retained, and disposal policies explain the process to follow when deleting unnecessary information in a secure manner. Data should not be kept any longer than is required to achieve the purposes for which records have been collected. The establishment of a period of retention creates an obligation firstly for data destruction after the specified date so as to prevent recovery or misuse (King and Vidas, 2011).

### 5.7 User Rights and Data Protection

Users have their own rights as to what can be done with and how it should be treated, etc., when it comes to personal information. These rights enable the user to pull out his/her personal information, modify, or erase it, but also decide how the information is used and split. Moreover, users can request their data in a portable format and take it to another provider. Organizations should provide users with tools and processes that enable the exercise of these rights. Businesses should also enhance system transparency by providing explicit pathways to accessing, correcting, or removing data, as it helps in building user trust within this mechanism (Vacca, 2020).

### 5.8 Data Controller and Processor Responsibilities

The data controller is the one who decides why and how personal data will be processed, while a processor processes such information on behalf of the former. It is important since they both maintain the protection of information (keeping data safe), which are duties fulfilled responsibly by responsible positions. This consists of performing regular security audits, encrypting data, requiring access controls, and ensuring that the information is used only for legitimate purposes. It is paramount to create and implement clear protocols and secured mechanisms for ethical data access with structural standards in combating against the danger of unethical handling or unauthorized breaches (Sobers, 2022).

Both the data controller and processor are responsible for security measures that must be put in place to ensure that personal data is protected throughout its lifecycle, from collection to deletion. This also requires transparency with users on how their data is processed and where it may be held (Microsoft, 2022).

### 5.9 Policy Updates and Compliance

This highlights the importance of comparatively evaluating data security policies more often as cyber threats mutate and new or modified regulations are enacted. Continuous audits to verify adherence to laws such as GDPR should be carried out by organizations. Security strategies should evolve to incorporate these advancements so that new risks are not able to progress and attempt against user data (Alder, 2024).

### 5.10 Outcomes and Findings

The data security policy had a number of meaningful outcomes, proving that it is effective in safeguarding sensitive user information and earning trust.

One of the biggest milestones dealt with data security, mainly through strong encryption techniques applied to the data. Using AES-256 for data in storage and TLS for the data in transit, all sensitive information was protected with the system

at all points in time, whether storage or sharing. This added an extra layer of security to which an unauthorized breach was almost impossible to achieve.

Another big role in strengthening security was played by the access controls. Role-based access control made sure that the user could view or interact with only that data which was relevant to his or her role. For example, a customer could see only their information, and an administrator could see what he needed to see for oversight. This not only minimized the risk of misuse but also maintained the integrity of the data.

The system also put a significant emphasis on user privacy: it gave users control of their data, allowed them to decide how their information is used, update it in time, or request deletion. This transparency and empowerment mean a lot for trust enhancement between users and the platform.

Another important outcome was the introduction of explicit data retention and disposal policies. The system ensured that personal information was retained only to the extent necessary and, when no longer required, disposed of in a very secure manner. This practice helped prevent the risk of data being recovered or misused after its purpose had been fulfilled.

It also puts extra emphasis on backup and restoration processes. These measures enabled the system to quickly recover, in case of data failure or corruption, to minimize possible downtime and keep users operational without interruptions.

Other major milestones were related to compliance with different regulations, such as GDPR. By being in line with legal standards, the system would avoid penalties but also show the users how responsibly and ethically their data was being dealt with. Features that would help users access, correct, or delete personal information helped in instilling confidence among users about the platform.

Finally, the real-time detection and response to potential threats that the system was capable of were a huge leap forward. The ability to continuously monitor and

have detailed audit logs enabled administrators to identify unusual activity and take action before it could become a problem.

All In all, the data security policy not only protected information but also improved the user experience by making the platform more trustworthy and transparent. Set up in this way, users could be certain that their personal information was secure while the system itself became resilient, ready for whatever the future might bring.

# 6 Development Challenges

The foundation of an appointment booking system largely relies on selecting the right technology stack and implementing a set of functionality paradigms that ensure secure data handling. This chapter describes the fundamental functional requirements for secure data management and national security mechanisms zero-trust using trusted platforms and integrated tools for strong protection.

## 6.1 Functional Requirements for Secure Data Handling

### Data Encryption

Sensitive data (user personal information and appointment records) must be encrypted at rest, in storage, as well as during transmission. At rest, it should use AES-256 encryption, while during transit, TLS (Transport Level Security) must be used for data. This approach ensures that unauthorized individuals cannot access confidential information, even if the transmitted data is intercepted. (Microsoft, 2022).

### Authentication and Authorization

Validating user identities is done using authentication methods, and this should be as secure with strong options like multi-factor (MFA). The core idea of MFA is that three elements are integrated into it: something the user knows (password), what the user has (mobile phone), and between these two singularly unique IDs, there is a property as biometric. The application of role-based access control (RBAC) is also required to enforce access control according to the roles users represent (NIST, 2022).

### Secure Data Storage

Providers will also need to strengthen data storage security so that it cannot be accessed from the outside through encryption at rest. It is very important to use database encryption methods, such as MySQL encryption or MongoDB field-level cryptography, by which users can keep the data confidential. Effective management of encryption keys involves storing hard copies offline or utilizing secure cloud storage solutions such as AWS Key Management Service (KMS) and Azure Key Vault (AWS, 2022).

### Audit Logging and Monitoring

Monitoring any access or changes to sensitive data type information is another requirement for a strong logging framework. Logs must be monitored continuously to detect any discrepancy, and SIEM (Security Information and Event Management) tools can help in automated threat detection and response. Audit logging is necessary for both adherence to security regulations and enforcement of a verifiable record of user activities (NIST, 2020).

### Data Retention and Disposal

Data Retention: Personal information is to be retained no longer than necessary for processing. When the retention period is over, data should be securely disposed of either using secure erasure technologies or physical destruction methods to prevent unauthorized access and even recovery (Microsoft, 2022).

### Compliance with Data Protection Regulations

It has to comply with rules and laws like the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act of 1996. These regulations require compliance with user consent, handling data access requests, and the right to erasure (European Union, 2016; Alder, 2024).

## 6.2 Platform and Tech Stack for Data Security

The technology stack and platform chosen for the priority appointment booking system must be according to security and scalability performance benchmarks. The technology stack mapped to achieve total data security is mentioned below:

### Front-End

HTML5/CSS3 and Bootstrap: Use of HTML to create the responsive UI. Combining CSS, everything can be responsive using media queries on custom as well as predefined class libraries by frameworks like bootstrap. MDN Web Docs (2023) HTTPs on the front-end make sure all requests and responses coming in/out from/to any user are encrypted (MDN Web Docs, 2023).

JavaScript: JavaScript is used for client-side input validation, which helps to prevent certain kinds of web exploits, including cross-site scripting (XSS) attacks (Microsoft, 2022).

### Back-End

PHP with Laravel Framework: The backend system has been built in PHP along with the framework of Laravel, which brings all its security-associated TV features such as CSRF (Cross-Site Request Forgery) protection, password hashing, and authentication layers (Laravel, 2024).

### Node.js

Server-side (used where event-driven, real-time processing at scale) Put libraries like Helmet within this component to implement security. headers, which provide several HTTP headers and prevent various types of attacks (Node.js Foundation, 2023).

Database

MySQL: Central database for saving appointments and user details Oracle used encryption-at-rest measures to protect personal data, and it protects against SQL injection by using prepared statements in the application code (Oracle, 2023).

MongoDB

MongoDB is used for some specific real-time operations or analytical tasks with encryption capabilities like field-level encryption to secure fields such as personal data (MongoDB, Inc., 2023).

Cloud Storage

Amazon Web Services (AWS): Secure data storing using AWS S3 and server-side encryption with Java SDK. In addition, AWS KMS (Key Management Service) takes care of the encryption keys to prevent unauthorized access by users and services (Amazon Web Services, 2023).

Microsoft Azure

Includes services such as Azure Key Vault to manage encryption keys or Blob Storage for secure file storage (Microsoft, 2023).

Encryption

AES-256: This encryption standard is used for the data at rest to make sure that every critical piece of information is secured enough (NIST, 2001).

## 6.3 Tackling Challenges in Secure System Development

The development of the secure appointment booking system had a lot of challenges, but those obstacles have provided great insights and enhancements for the system as a whole.

Among the big challenges was keeping sensitive user data safe during its life cycle. To handle this, the system is using AES-256 encryption at rest and TLS encryption while in transit. This gave strong protection against unauthorized access and a very solid ground for the secure handling of data.

Authentication and authorization were also critical focal points. Introducing multi-factor authentication (MFA) added an extra layer of security, making it more challenging for unauthorized users to gain access. Additionally, role-based access control (RBAC) restricted users to accessing only the information pertinent to their roles, minimizing the risk of data breaches.

Another challenge was to securely manage data storage complexity: the system had to embed encrypted database solutions, like MySQL and MongoDB, in case hardware was compromised. Effective encryption key management further bolsters this by preventing unauthorized decryption.

Monitoring and tracking system activity for security threats posed additional challenges. Detailed audit logging and automated monitoring tools were implemented, thus enabling the detection and response to unusual activity as quickly as possible. These solutions enhanced the overall security posture of the system.

Data retention and disposal were critical concerns. The clear retention policies and secure disposal methods were defined and implemented, ensuring that unnecessary data was not retained, thereby reducing the risk of misuse or recovery of obsolete information.

Compliance with the protection of data according to GDPR proved to be both a challenge and an opportunity. Compliance with such regulations required changes in system functionalities but also opened up an avenue for building user trust through ethical data handling and transparency.

In the end, though the development process was not without its significant challenges, addressing them resulted in a more secure, reliable, and user-friendly system. The solutions implemented resolved not only the immediate issues but

also set up a scalable and trustworthy platform for future adaptation to security and usability demands.

# Conclusion

In conclusion, this thesis concludes the primary objective of developing a secure appointment booking system with enhanced security elements which would be suitable for both users; the businesses and the customers. Rather than general literature of security, this thesis has employed a practical approach towards challenges by securing personal information with optimized scheduling features and user´s trust in the system. However, to achieve the objectives, the approach has opted relevant protocols and technologies and ensured user experience remains improved.

With usage of AES-256 encryption for data storage and TLS encryption of information transmission, the thesis objectives were achieved leading to prevention of unauthorized access or interceptions in terms of theft or attacks. Other key features include user´s consent pages, detailed audit logs, and secure cloud-based key management. These additional key features acted as enhanced layers of data protection for the application.

Alongside the objectives of security for the application, the approaches also ensured to align requirements of platform´s user-friendly and adaptability feature. Balanced between ease of use and robust data protection, the application has been upgraded to be a reliable tool for businesses and customers. The platform has been developed by focusing on the current requirements but also ensured that platform´s scalability is enabled for future requirements. The scalability will ensure seamless experience and also maintain the highest standards of security of the application. This thesis and practical work are laying foundation for trustworthy and effective solution for scheduling systems.

# References

Alder, S., 2024. What does HIPAA compliance mean? HIPAA Journal. [online] 25 September. Available at: https://www.hipaajournal.com/what-does-hipaa-compliance-mean/ [Accessed 01 May 2024].

Anderson, R., 2020. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken, NJ: Wiley. Available at: https://www.google.fi/books/edition/Security_Engineering/GNIHEAAAQBAJ?hl=en&gbpv=0 [Accessed 17 June 2024].

AWS, 2022. AWS KMS: Key Management Service. Amazon Web Services. [online] Available at: https://aws.amazon.com/kms/ [Accessed 13 July 2024].

Amazon Web Services, 2023. Amazon S3 Security Best Practices. AWS Documentation. [online] Available at: https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html [Accessed 26 October 2024].

Cloudflare, 2023. Transport Layer Security (TLS). Cloudflare Learning Center. [online] Available at: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ [Accessed 26 October 2024].

European Union, 2016. General Data Protection Regulation (GDPR). [online] Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 01 May 2024].

Kozierok, C.M., 2005. HTTP Data Transfer Content Encodings and Transfer Encoding. The TCP/IP Guide. [online] Available at: http://www.tcpipguide.com/free/t_HTTPDataTransferContentEncodingsandTransferEncodin.htm [Accessed 26 October 2024].

King, C. and Vidas, T., 2011. Empirical analysis of solid-state disk data retention when used with contemporary operating systems. Digital Investigation,

8(3-4), pp.111-120. Available at: https://doi.org/10.1016/j.diin.2011.05.013 [Accessed 26 October 2024].

Laravel, 2024. Security. Laravel Documentation. [online] Available at: https://laravel.com/docs/10.x/authentication [Accessed 15 October 2024].

Microsoft, 2022. Data Encryption in Azure. Microsoft Learn. [online] Available at: https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview [Accessed 10 May 2024].

Microsoft, 2023. Azure Security Best Practices and Patterns. Microsoft Learn. [online] Available at: https://learn.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns [Accessed 10 October 2024].

MDN Web Docs, 2023. HTML5, CSS3, and Responsive Design. Mozilla Developer Network. [online] Available at: https://developer.mozilla.org/en-US/docs/Learn/CSS/CSS_layout/Responsive_Design [Accessed 26 October 2024].

MongoDB, Inc., 2023. MongoDB Security. MongoDB Documentation. [online] Available at: https://www.mongodb.com/docs/manual/security/ [Accessed 10 October 2024].

National Institute of Standards and Technology (NIST), 2001. Advanced Encryption Standard (AES). NIST FIPS Publication 197. [online] Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 25 October 2024].

National Institute of Standards and Technology (NIST), 2018. NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology. [online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [Accessed 25 October 2024].

National Institute of Standards and Technology (NIST), 2020. NIST Special Publication 800-92: Guide to Computer Security Log Management. National Institute of Standards and Technology. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf [Accessed 26 October 2024].

NIST, 2022.Role-Based Access Control (RBAC). NIST Computer Security Resource Center. [online] Available at: https://csrc.nist.gov/publications/detail/sp/800-162/final [Accessed 10 May 2024].

Node.js Foundation, 2023. Node.js Security Best Practices. Node.js Foundation. [online] Available at: https://nodejs.org/en/docs/guides/security/ [Accessed 10 October 2024].

Oracle, 2023. MySQL Security. MySQL Documentation. [online] Available at: https://dev.mysql.com/doc/refman/8.0/en/security.html [Accessed 26 October 2024].

Ponemon Institute, 2023. Cost of a data breach climbs higher. [online] Available at: https://www.ponemon.org/research/ponemon-library/security/cost-of-a-data-breach-climbs-higher.html [Accessed 16 May 2024].

Savvy Security, 2021. SSL Meaning & Definition for Non-Techies. [online] CheapSSLsecurity. Available at: https://cheapsslsecurity.com/blog/ssl-meaning-definition-for-non-techies/ [Accessed 10 October 2024].

Sobers, R., 2022. Cybersecurity Threats 2022. [online] Available at: https://www.varonis.com/blog/cybersecurity-threats [Accessed 01 May 2024].

Verizon, 2023. Data Breach Investigations Report 2023. [online] Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed 14 May 2024].

Vacca, J.R. (ed.), 2017. Computer and Information Security Handbook. 3rd ed. Cambridge, MA: Elsevier. Available at:

https://www.sciencedirect.com/book/9780128038437/computer-and-information-security-handbook [Accessed 10 May 2024].