Information Security Measures for a Procrastination-Combatting Digital Solution*

Valentyna Pleskach[1,*], Irma Šileikienė[2] , Romanas Tumasonis[2,3] and Yevhenii Topolskov[1]

[1] *Taras Shevchenko National University of Kyiv, Volodymyrs'ka str. 64/13, Kyiv, 01601, Ukraine*
[2] *Vilniaus Gediminas Technical University, Saulėtekio al. 11, Vilnius, LT-10223 Lithuania*
[3] *Vilniaus Kolegija |Higher Education Institution Saltoniškių str. 58, Vilnius, LT-08105 Lithuania*

Abstract

This paper explores various security frameworks, threat modeling, and risk management techniques, the assignment provided a thorough theoretical backdrop against which practical security measures can be developed and implemented. Covering critical aspects of security such as authentication, data privacy, session management, and compliance with legal standards like GDPR, the work not only addressed potential vulnerabilities identified through threat modeling but also set a solid framework for implementing these security features practically. This comprehensive approach ensures that the prototype is not only functional but also secure from various cybersecurity threats. Moreover, it showcased how security and functionality can be balanced effectively, paving the way for potential future development and real-world application of the prototype.

Keywords

Information security, security frameworks, security requirements, security measures, risk management

1. Introduction

The integration of technology into every day has greatly improved personal and professional productivity. However, this digital expansion has also exposed users to complex cybersecurity challenges [3]. Applications designed to enhance productivity are particularly vulnerable, as they frequently manage large volumes of sensitive data, making them prime targets for cyber threats. In this context, the role of information security is paramount, safeguarding against data breaches, unauthorized access, and other threats that undermine user privacy and trust. Thus, robust information security measures are fundamental for maintaining the confidentiality, integrity, and availability of data.

Given the complexity of modern cyber threats, which now include advanced tactics like social engineering, ransomware, and sophisticated malware attacks, digital solutions require robust and comprehensive security protocols, as well as the ability to adapt to the rapidly changing landscape of cyber risks [1]. Additionally, the international scope of digital application deployment mandates adherence to various data protection laws, such as GDPR and CCPA. This complex environment highlights the need for continuous improvement in security strategies to maintain user trust and ensure the integrity of personal data.

Therefore, the intersection of information security and application development is a critical area of study and application. This study aims to bridge the gap between application development and robust cybersecurity practices, ensuring that digital solutions are not only effective in addressing human behavioral issues like procrastination but are also secure against both current and potential future cyber threats.

8th International Scientific and Practical Conference Applied Information Systems and Technologies in the Digital Society AISTDS'2024, 2024, October 1, Kyiv, Ukraine

[*] Corresponding author.

v.pleskach64@gmail.com (V. Pleskach); i.sileikiene@eif.viko.lt (I. Šileikienė); r.tumasonis@eif.viko.lt (R. Tumasonis); y.topolskov@knu.ua (Y. Topolskov)
0000-0003-0552-0972 (V. Pleskach); 0000-0002-1185-0970 (I. Šileikienė); 0000-0002-8921-0674 (R. Tumasonis); 0000-0001-5587-3069 (Y. Topolskov)

The objectives of this work are as follows.

1. Analyze Existing Digital Security Frameworks: To assess their applicability to productivity applications, particularly those designed to combat procrastination.

2. Develop Security Requirements: Formulate specific security strategies designed to protect digital solutions from both current and emerging cyber threats.

3. Implement and Evaluate Security Measures: Apply these security measures in a prototype environment and evaluate their effectiveness through systematic testing, refining the approach based on empirical results and user feedback.

2. Theoretical foundations and security frameworks

2.1. Definition and importance of information security

Technological advancement offered unique solutions to age-old problems, among which procrastination stands out as a complex issue affecting individuals' productivity and well-being. As digital solutions emerge to address this challenge, the significance of embedding robust information security measures cannot be overstated [1]. The development of applications designed to mitigate procrastination through behavior modification underscores the necessity of ensuring these solutions not only fulfill their intended purpose but also safeguard users' data and privacy.

Information Security is the practice of protecting digital assets such as data, networks, systems, and devices from unauthorized access, use, disclosure, disruption, modification, or destruction. It encompasses a range of practices, technologies, and processes designed to safeguard digital information and ensure the confidentiality, integrity, and availability of critical resources [20].

The importance of ISM in today's digital environment is multifaceted, addressing the need to protect against cyber threats, comply with regulatory requirements, mitigate economic and social impacts, enable secure digital transformation, and enhance user trust. As the digital landscape continues to evolve, the role of ISM will only grow in significance, underscoring the need for ongoing investment in information security practices, technologies, and skills.

2.2. The CIA triad

Information security consists of several key principles, each fulfilling a distinct role in addressing the complex threats and vulnerabilities within digital environments. These principles include confidentiality, integrity, and availability [4].

Confidentiality ensures that sensitive information is accessed only by authorized individuals and is protected from those who are not permitted to access it. In digital solutions, particularly those managing personal productivity, confidentiality can be upheld through the use of encryption, secure user authentication methods, and stringent access controls [7]. For instance, a digital application designed to combat procrastination may store user data related to personal goals and daily activities, which should be accessible only by the user and not be exposed to unauthorized access.

Ensuring confidentiality is paramount not only for user trust but also for the application's credibility and long-term viability. Users entrust applications with their data, expecting that their information will be handled with the utmost discretion. Breaches in confidentiality can lead to loss of user trust, legal repercussions, and potential harm to individuals whose data may be exposed. Achieving confidentiality requires a complex approach, incorporating both technical measures and organizational policies. Techniques to ensure confidentiality include encryption, access control mechanisms, and data classification policies that dictate the levels of secrecy and the measures required to protect each classification level.

In procrastination-addressing applications, the integrity of data stands as a pillar of user trust and application efficacy. Integrity refers to the assurance that information is protected against unauthorized alteration or deletion and that it accurately reflects the original intended content as created, transmitted, or stored by the user. This principle ensures that the data presented and acted upon by both users and application algorithms remains true to its source, untainted by corruption or unauthorized manipulation. Integrity protection mechanisms include cryptographic hash functions, digital signatures, and version control systems. These measures help detect unauthorized changes, prevent data tampering, and ensure that data remains consistent, accurate, and valid over its entire lifecycle.

Availability, the third cornerstone of the CIA Triad, is pivotal for the functionality and reliability of digital solutions. Ensuring the availability of productivity applications involves a comprehensive strategy that incorporates redundancy, fault tolerance, regular maintenance, disaster recovery planning, load balancing, and vigilant monitoring. For applications targeting behavioral changes like procrastination, the uninterrupted availability is tightly linked to the application's ability to effectively support users in achieving their goals. Service interruptions not only impede user progress but can also foster frustration and reduce motivation, undermining the application's purpose [9].

3. Security threats and vulnerabilities

3.1. Overview of common security threats

The cybersecurity area is continuously evolving, marked by an array of diverse and sophisticated threats. These threats, ranging from malware to sophisticated denial of service attacks, endanger the confidentiality, integrity, and availability of digital data.

Malware represents a significant threat, encompassing various forms of malicious software such as viruses, worms, and trojans. Viruses, for example, can replicate themselves and spread across networks, corrupting data and disrupting operations. Worms operate similarly but do not require human action to propagate, making them particularly virulent. Trojans disguise themselves as legitimate software, creating backdoors in security to facilitate further illicit activities. Each type of malware can cause extensive damage to digital systems, compromising both personal and corporate data.

Phishing Attacks leverage social engineering to deceive users into divulging sensitive information. These attacks typically occur through email, where attackers impersonate legitimate institutions to lure victims into entering personal data on fraudulent websites. Phishing is especially dangerous because it exploits human vulnerability, bypassing many technical safeguards.

Ransomware is a specific type of malware that encrypts a victim's files, demanding payment to restore access. These attacks directly impact data availability and can halt business operations, leading to significant financial losses and erosion of trust among users.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks disrupt services by overwhelming systems with a flood of traffic. DoS attacks originate from a single source, whereas DDoS attacks are distributed across numerous compromised devices. These attacks aim to render websites and online services inoperative, causing operational disruption and damaging reputational trust.

3.2. Security vulnerabilities and their implications for productivity applications

The evolution of the cybersecurity threat landscape poses significant challenges for productivity applications as well, as essential tools underpinning both individual productivity and organizational efficiency. These applications, encompassing a broad range of communication platforms to project management tools, serve as repositories for vast amounts of sensitive data, rendering them prime targets for cyber threats [2].

When attackers manipulate SQL queries to gain unauthorized access or modify a database, the consequences can be severe. This type of vulnerability not only leads to data breaches but also erodes user trust and can result in substantial legal and financial repercussions under data protection laws such as GDPR.

Furthermore, vulnerabilities that allow attackers to inject malicious scripts into web pages expose users to risks of sensitive information theft, such as session tokens. In environments where applications offer collaborative features, such security breaches can severely undermine the platform’s credibility and reduce user confidence in the safety of their data.

Issues with authentication processes are equally concerning. Inadequate authentication mechanisms provide easy entry points for attackers, leading to unauthorized access and potential data leaks. The repercussions extend beyond data integrity, affecting user access and the overall reliability of the application. These disruptions are particularly detrimental in applications relied upon daily for personal management and productivity, directly impacting user satisfaction and trust.

The exposure of sensitive data due to insecure APIs or poor encryption practices can attract significant regulatory attention, resulting in heavy fines and damage to the organization's reputation. Moreover, operational disruptions from attacks like DDoS not only degrade service quality but can also lead to substantial downtime, frustrating users and compromising the effectiveness of the application.

To address these challenges, adopting a security-by-design approach throughout the application development lifecycle is critical. By implementing rigorous testing, compliance checks, and user education, developers can mitigate risks and reinforce the security framework of their applications. This proactive stance on security not only safeguards against specific vulnerabilities but also enhances user trust and compliance with international standards and regulations.

4. Risk management in ISM

4.1. Risk assessment methodologies

Risk assessment is a fundamental aspect of information security management, providing a systematic process for identifying vulnerabilities and evaluating the risks associated with potential security threats. The methodologies employed in risk assessment can vary widely, each with its approach to quantifying and managing risk [13].

Risk assessments are generally categorized into two types: qualitative and quantitative. Qualitative assessments focus on subjective analysis of the impact and probability of risks based on expert opinion and industry knowledge. This type often results in risk prioritization on a scale such as low, medium, or high. Quantitative assessments, on the other hand, aim to assign numerical values to risks, calculating potential impacts in financial terms or other measurable units. This approach can provide a more objective basis for comparing risks and allocating resources [17].

Common Methodologies.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Developed by Carnegie Mellon University, OCTAVE is a framework that focuses on organizational risk and security practices. It is particularly suited for larger organizations looking to integrate business objectives with risk-based security strategies [5].

FAIR (Factor Analysis of Information Risk): FAIR is a quantitative risk assessment methodology that helps organizations understand, analyze, and quantify information risk in financial terms. It is useful for making informed decisions about security investments and risk management priorities [5].

Risk IT Framework: Designed by ISACA for IT-related risk, the Risk IT framework provides a comprehensive guide for enterprises to identify, govern, and manage IT risk. It helps organizations align IT risk management with overall enterprise risk management.

Adapting these methodologies to digital solutions involves considering the specific characteristics and requirements of the application. For instance, a digital tool designed to combat procrastination might utilize OCTAVE to assess organizational risks involving user data security and system availability. FAIR could be employed to quantify the financial impact of potential breaches or downtime, aiding in decision-making about where to focus security efforts. The Risk IT framework can guide the overall risk governance structure, ensuring that all IT risks are systematically managed in line with the application's strategic goals [22].

4.2. Identifying, prioritizing and mitigating risks

Effective risk management in digital applications requires identifying, prioritizing risks and implementing appropriate mitigation strategies. This integrated approach ensures that the most critical risks are addressed with effective solutions to protect the application and its users.

The first step in risk management is to identify potential risks. This involves a thorough analysis of the entire ecosystem of the digital application, including software components, user interactions, data flows, and external integrations. Techniques such as brainstorming sessions, expert interviews, and the use of automated tools can help uncover potential vulnerabilities. For digital applications aimed at combating procrastination, risks might include unauthorized access to user data, data leakage, or service interruptions that could derail users' productivity improvements [9].

Once identified, risks are prioritized based on their potential impact on the application and the likelihood of their occurrence. Tools such as risk matrices and SWOT analysis help in assessing risks to focus resources and attention on the most significant threats. Prioritization considers factors like the severity of impact, regulatory compliance requirements, and operational criticality.

The next crucial step is to implement strategies to mitigate those risks. Risk avoidance might be applied to eliminate threats, such as opting for more secure alternatives in technology or redesigning vulnerable system components. Where risks cannot be entirely avoided, reduction strategies are crucial and may include deploying advanced security measures like encryption, stringent access controls, and adherence to secure coding practices. In scenarios where risks cannot be internally managed, sharing through insurance or outsourcing to third-party vendors with specialized security expertise can be effective. Risk acceptance is considered for less critical risks, where the cost of mitigation exceeds the potential impact. Integral to these strategies are implementing robust preventative, detective, and corrective controls. Preventative controls are designed to prevent security incidents, detective controls to identify and react to incidents as they occur, and corrective controls to recover from incidents and restore normal operations. Continuous monitoring and regular review of these controls are essential to ensure they remain effective and are adjusted in response to evolving threats and business needs.

5. Security frameworks and standards

5.1. Overview of established frameworks

Established frameworks provide comprehensive guidelines and best practices for establishing, implementing, maintaining, and continually improving information security.

ISO/IEC 27001 is one of the most prevalent international standards for information security management systems (ISMS). It outlines a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process. This standard is particularly useful for organizations that need to demonstrate their commitment to information security to clients or regulatory bodies through formal certification [6].

The NIST Cybersecurity Framework developed by the National Institute of Standards and Technology in the United States. The framework is used globally to improve cybersecurity across industries. It provides a policy framework of computer security guidance for organizations that want to assess and improve their ability to prevent, detect, and respond to cyber incidents. The NIST Framework is flexible and can be tailored to the specific needs of individual organizations, regardless of their size or sector [19].

COBIT is a comprehensive framework for IT governance and management developed by ISACA. It is designed to be a supportive tool for managers and allows for bridging the gap between technical issues, business risks, and control requirements. COBIT’s principles and tools aim to provide a holistic approach to IT management, focusing on maximizing the value of information by aligning IT processes with business objectives.

5.2. Application to procrastination-addressing digital solutions

Integrating established ISM frameworks and standards into digital solutions that focus on combating procrastination and enhancing productivity is critical for ensuring robust security while supporting functional and user-centric design. These frameworks provide a structured approach to safeguarding sensitive user data and maintaining application integrity, which are crucial for applications that handle personal productivity data.

Applications designed to manage procrastination often collect detailed data on user habits, preferences, and productivity patterns. Adhering to standards like ISO/IEC 27001 and the NIST Cybersecurity Framework helps ensure that this data is handled securely and responsibly. These frameworks provide guidelines for implementing comprehensive data protection measures that respect user privacy while preventing unauthorized access and data breaches [6].

Trust is a cornerstone of applications focused on personal productivity, as users need to feel confident that their sensitive data is in safe hands. Compliance with recognized security standards demonstrates a commitment to data protection, which can be a significant factor in user adoption and retention. For instance, aligning with GDPR and other privacy regulations not only meets legal requirements but also positions the application as trustworthy and reliable.

Digital solutions for procrastination need to be agile and responsive to changes in user behavior and technological advancements. Frameworks like COBIT can guide developers in managing IT risks that could affect the application's performance and security. These include risks from new software updates, integration with other apps, or evolving cyber threats. A structured risk management process enables developers to identify potential vulnerabilities early and adapt their security strategies accordingly.

Table 1
Frameworks Comparison

Framework	Focus Area	Key Features	Applicability to Procrastination-Combatting Apps
ISO/IEC 27001	Comprehensive ISMS	Systematic approach, risk management, control implementation	High - versatile for all app types
NIST Cybersecurity	Cybersecurity risk management	Core functions (Identify, Protect, Detect, Respond, Recover), tailored to organizational needs	Medium - ideal for critical infrastructure apps
COBIT	IT governance and management	Aligns IT with business goals, ensures compliance, optimizes resources	Low - more suitable for enterprise IT management
PCI DSS	Payment card data security	Secure data processing, strong access control, network infrastructure security	Medium - essential for apps handling payments
GDPR	Data protection and privacy	Data subject rights, data protection principles, regulatory compliance	High - mandatory for apps used by EU residents

Procrastination-management applications benefit from a continuous improvement approach to security. This involves regular security audits, user feedback loops, and updates to security policies as part of the lifecycle management prescribed by frameworks like ISO/IEC 27001. Continuous improvement helps ensure that the application adapts to new security challenges and evolving user expectations, thus maintaining its effectiveness and competitive edge.

Evaluating security frameworks is essential for determining their suitability in addressing the unique requirements and challenges of procrastination-combatting applications. The Table 1. examines the effectiveness and applicability of established frameworks within the context of such applications, considering factors such as comprehensiveness, flexibility, and alignment with regulatory requirements.

6. Privacy and data protection

6.1. Data protection laws

Data protection laws play a crucial role in safeguarding personal information, particularly for applications that collect and process user data to manage behaviors such as procrastination. Understanding these regulations is essential for ensuring legal compliance and safeguarding user privacy.

As one of the most stringent privacy and security laws in the world, the General Data Protection Regulation (GDPR) affects any entity that processes the data of EU citizens, regardless of the entity's location. For procrastination-addressing applications, this means adhering to principles of lawfulness, transparency, and consent. The GDPR mandates that users must explicitly consent to the collection and use of their data, which must be collected for specified, explicit, and legitimate purposes. Furthermore, users have the right to access their data, correct inaccuracies, and request the deletion of their data under certain circumstances [12].

California Consumer Privacy Act (CCPA) gives California residents the right to know what personal data is being collected about them, whether their personal data is sold or disclosed, and to whom. It also grants the right to object to the sale of personal data and the right to access their data. For apps focusing on productivity and procrastination, which might collect detailed user activity data, compliance involves implementing processes to manage user data access requests efficiently and transparently [10].

Depending on the nature of the procrastination management app, other specific laws might also apply. For instance, apps that integrate health tracking or mental well-being aspects might need to comply with the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., which protects sensitive patient health information from being disclosed without the patient's consent or knowledge. Developers must also stay informed about emerging laws in other regions, such as Brazil's LGPD or India's proposed Personal Data Protection Bill, which introduce additional compliance requirements and could impact global operations.

6.2. Relevance to digital solutions

Applications designed to manage procrastination often collect and analyze extensive personal data to provide customized advice and track user progress. The sensitivity of this data and the potential consequences of its misuse make robust data protection practices a fundamental requirement for these digital solutions.

Procrastination management applications typically gather data that users consider private, such as details about personal goals, daily routines, and behavioral patterns. This data can reveal much about a person's lifestyle, health, and psychological state. As such, protecting this information is a legal obligation under laws like GDPR and CCPA and also a critical aspect of maintaining user trust. Any breach that leads to unauthorized access could have severe repercussions, damaging the users' trust and the application's reputation.

Users of digital productivity tools have high expectations regarding the privacy and security of their data. They trust these applications to not only help them manage their time more effectively but also to protect the personal information they share. Failing to meet these expectations can lead to loss of trust, user attrition, and severe reputational damage.

The specific nature of data collected by procrastination-management apps increases their risk exposure, making them potential targets for cyber threats such as data breaches or unauthorized access. These risks are not only technical but also legal and ethical, as mishandling personal data can lead to significant legal repercussions under laws like GDPR or CCPA.

Non-compliance with data protection laws can result in hefty fines and legal actions. Beyond the financial implications, non-compliance can erode user confidence, impacting the application's marketability and long-term viability. For instance, a breach in user data privacy can trigger a decline in user engagement, negatively affecting the overall effectiveness of the app in managing procrastination.

6.3. Compliance strategies

Ensuring compliance with data protection laws is critical for applications that help users manage procrastination. These laws not only protect users but also build trust and enhance the credibility of digital solutions.

Procrastination-combatting digital solutions should adopt a data minimization approach, collecting only the necessary information required for their functionality. By limiting data collection to essential elements, such as user preferences or task schedules, these applications can minimize the potential impact of data breaches and unauthorized access.

Moreover, implementing robust user consent mechanisms is paramount to ensuring compliance with privacy regulations. Procrastination-combatting apps should obtain explicit consent from users before collecting, processing, or sharing their data. Transparent disclosure of data practices and clear opt-in/opt-out options empower users to make informed decisions about their data usage, fostering trust and accountability.

Incorporating privacy by design principles into the development process is integral to building privacy-centric procrastination-combatting solutions. By embedding privacy considerations into every stage of product design and development, from concept ideation to deployment, developers can proactively address privacy risks and vulnerabilities. Privacy-enhancing features, such as end-to-end encryption and anonymization techniques, should be prioritized to safeguard user data against unauthorized access and misuse.

Ongoing compliance monitoring and auditing are essential components of an effective privacy and data protection strategy. Procrastination-combatting app developers should establish internal processes for regularly assessing compliance with relevant regulations, conducting privacy impact assessments, and maintaining comprehensive audit trails. External audits by independent third-party assessors can provide additional validation of compliance efforts, demonstrating a commitment to transparency and accountability.

6.4. Designing security requirements for a procrastination-addressing digital solution

This document outlines the security requirements for a prototype of a mobile application designed to combat procrastination issue through gamification and task management (Fig.1).

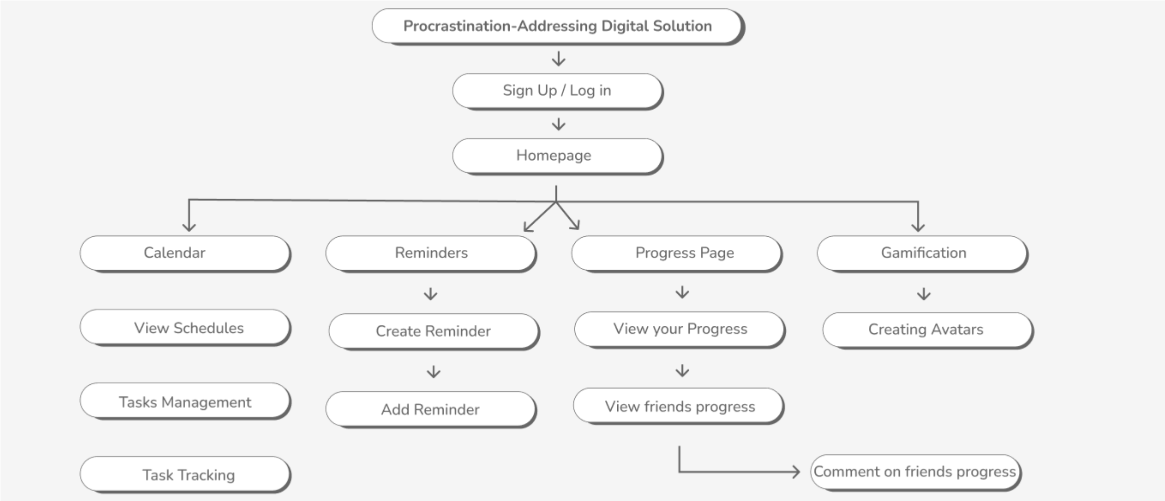


Figure 1: Information Architecture.

The objective is to develop a security framework that not only protects user data but also aligns with global security standards, ensuring the application’s integrity and trustworthiness.

The security requirements specified in this document are structured to provide a comprehensive approach to safeguard the application from inception through deployment and operation. Inspired by the OWASP Mobile Application Security Verification Standard (MASVS), this work aligns with globally recognized best practices tailored specifically to the mobile environment [15].

7. Architecture, design, and threat modeling

7.1. Architecture and design

The prototype is conceptualized to engage users with a dynamic interface that helps manage tasks effectively while encouraging progress through gamified elements. As a prototype aimed at demonstrating potential functionalities and security strategies, it incorporates best practices in software architecture and mobile application security.

The architecture of the digital solution encompasses multiple layers, each serving distinct functions while contributing to the overall security and usability of the application.

At the presentation layer, the use of frameworks like React Native or Flutter ensures a responsive and engaging user interface across different mobile platforms. This layer is meticulously designed to handle user inputs, display task-related information, and manage interactive elements with a focus on usability and accessibility.

Beneath the presentation layer lies the business logic layer, where the core functionalities of the application reside. This layer processes user requests, manages task data, and orchestrates gamification features to incentivize user engagement and productivity. Hosted on a secure cloud platform, the business logic layer leverages cloud-native services and best practices to ensure scalability, reliability, and resilience against potential security threats.

The data storage layer, situated at the foundation of the architecture, is responsible for persistently storing user data, task-related information, and application settings. Utilizing encrypted database solutions, this layer employs industry-standard encryption algorithms and access control mechanisms to safeguard sensitive data from unauthorized access and malicious tampering. Additionally, data integrity checks and redundancy measures are implemented to mitigate the risk of data corruption or loss.

7.2. Threat modeling

Threat modeling is a crucial step in identifying and assessing potential security risks to our procrastination-addressing digital solution. Each category of threat identified by STRIDE is analyzed to determine its potential impact on the system and the likelihood of its occurrence. This detailed analysis informs the prioritization and resource allocation for security measures [8].

In the digital solution, spoofing identity refers to the risk where unauthorized individuals may attempt to gain access to the system by impersonating legitimate users. This could occur through phishing attacks where attackers deceive users into providing their login credentials. The likelihood of such incidents is considered medium given the common nature of these tactics despite robust authentication mechanisms. The impact, however, is high as successful spoofing attacks could lead to unauthorized access to sensitive user data and personal information, severely undermining user trust and data integrity. To mitigate this risk, implementing multi-factor authentication and conducting regular security awareness training for users are essential steps. Prioritizing these measures is critical due to the high potential impact on the system’s integrity and user privacy.

Tampering involves unauthorized alterations to data or system configurations. Within the productivity-combatting application, this might manifest as unauthorized changes to user-set tasks or personal goals, potentially through cross-site scripting (XSS) or SQL injection attacks where attackers inject malicious code into the system. The likelihood of tampering is low due to stringent input validation and access controls. However, the impact of such an event is high as it could corrupt the accuracy of user data and disrupt the application's functionality. Ensuring data integrity is therefore a medium priority, with continuous implementation of secure coding practices, regular code reviews, and comprehensive access control mechanisms as our primary defences [2].

Information disclosure poses a significant threat to this application, especially concerning the unauthorized access to or exposure of personal user data through breaches or leaks. The likelihood of this threat is high, as data breaches continue to be prevalent in the digital landscape, often through compromised security systems or insider threats. The impact is deemed very high due to the potential for severe privacy violations and subsequent legal and reputational damage. Consequently, this threat is a very high priority, and robust measures, including advanced encryption, comprehensive data access policies, etc.

A Denial of Service (DoS) attack aims to make the digital solution unavailable to legitimate users, typically by overwhelming the system with excessive requests. The likelihood of such attacks is medium, reflecting the general risk across digital platforms. The impact is also medium, as service disruptions can degrade user experience but usually do not result in permanent damage. Mitigating DoS attacks is a medium priority, with strategies such as deploying anti-DDoS protections and ensuring scalability and redundancy in our hosting infrastructure.

Elevation of privilege involves attackers gaining higher-level permissions than intended, allowing them to execute actions that should be restricted. While the likelihood of this occurring is low due to stringent access controls, the potential impact is very high as it could lead to extensive unauthorized access and system damage. Preventing such escalation is a high priority, necessitating rigorous enforcement of the principle of least privilege, regular audits of user permissions, and the deployment of anomaly detection systems to quickly identify unauthorized attempts to elevate privileges. Table 2 below presents a summary of key threats identified along with their potential impact, likelihood, priority, and corresponding mitigation strategies.

Table 2
Threat Analysis

Threat	Impact	Likelihood	Priority	Mitigation Strategy
Spoofing Identity	High	Medium	High	Multi-factor authentication, security awareness training
Tampering with Data	High	Low	Medium	Input validation and parameterized queries, least privilege access controls
Repudiation	Medium	Medium	Medium	Content security policies, sanitize user input to prevent script injection
Information Disclosure	Very High	High	Very High	Advanced encryption, enforce data access policies, conduct continuous monitoring
Denial of Service	Medium	Medium	Medium	Anti-DDoS protections, ensure scalability and redundancy
Elevation of Privilege	Very High	Low	High	Principle of least privilege, regular audits, anomaly detection systems

8. Data storage and privacy

8.1. Data management

Effective data management is fundamental to the development of the prototype mobile application. Given the diverse range of user-generated content and operational data involved, adopting a systematic approach to data collection, storage, and processing is crucial. This approach must align with global data protection standards, particularly the General Data Protection Regulation [12], to ensure the privacy and security of user data, especially for potential users within the European Union [18].

In the context of data collection and classification, the application will only collect essential data required for delivering its services. This includes personal information for account setup, task details for functionality, and interaction data for enhancing user experience. Personal information, such as names and email addresses, will be gathered with explicit user consent, accompanied by clear explanations regarding the purposes and benefits of data submission. Task details, including deadlines and notes, will be treated with utmost confidentiality due to their personal nature. Additionally, data on user interactions with the application's features will be handled judiciously to maintain user privacy while leveraging insights to refine functionality.

To ensure the security of data storage and access, the application will leverage encrypted cloud services, employing robust encryption protocols such as Advanced Encryption Standard (AES-256) for data at rest and Transport Layer Security (TLS) for data in transit. Role-Based Access Control (RBAC) will be implemented to regulate data access within the application, with strict user permission policies based on predefined roles to prevent unauthorized data access.

Data retention and compliance are also critical considerations. The application will adhere to a concise data retention policy, limiting the duration of stored data to what is strictly necessary for its intended purposes. Users will have control over their data management, including the ability to update or delete their information, empowering them to maintain control over their data. Furthermore, the application will be designed to comply with relevant privacy laws, incorporating mechanisms to address user rights under GDPR, such as data portability and the right to erasure [14].

8.2. Privacy enhancements

Data anonymization serves as a critical method in protecting user privacy, especially when handling data that could reveal personal user behaviors or preferences. In the prototype, anonymization is applied to user interaction data, which includes general metrics on app usage patterns and feature engagement. This data is processed to remove or obscure any personally identifiable information (PII), employing techniques such as pseudonymization and aggregation [21].

Pseudonymization replaces identifiers with pseudonyms, severing the direct link between data sets and user identities, while aggregation combines data points from multiple users to create a non-identifiable dataset that prevents the reverse engineering of individual profiles. These measures significantly reduce the risk of privacy breaches and ensure that the data used for improving app functionalities and conducting analytics cannot be traced back to any individual user.

9. Cryptography requirements

The implementation of robust cryptographic measures is paramount, as it helps securing user data and ensuring that communications between the application and its servers are shielded against interception and tampering. The application will incorporate advanced encryption protocols to safeguard data at every stage of its lifecycle:

Data Encryption at Rest: Given the sensitive nature of personal and task-related information, the application will employ the Advanced Encryption Standard (AES) with a 256-bit key for encrypting data stored within its databases and on user devices. AES-256 is renowned for its robustness, and a meticulous key management system, including hardware security modules (HSMs) and key rotation procedures, will be implemented to securely manage encryption keys [16].

Data Encryption in Transit: Transport Layer Security (TLS) version 1.3 will be utilized for encrypting all data transmitted between the mobile application and the server. TLS 1.3 offers improved security and efficiency, ensuring that data in transit remains confidential and unaltered. The application will enforce HTTPS across all API endpoints to guarantee encrypted communication channels.

The prototype will leverage cryptographic hash functions, incorporating salted hashes to enhance the security of stored credentials. Salted hashes prevent attackers from efficiently using precomputed tables (e.g., rainbow tables) to crack passwords, significantly bolstering the application's security posture [11].

For sensitive operations like financial transactions, the application will employ challenge-response authentication mechanisms. This approach safeguards against man-in-the-middle attacks by ensuring that intercepted communications do not expose reusable credentials.

9.1. Authentication and session management

Effective authentication and session management are fundamental to securing user interactions within mobile applications. These mechanisms not only verify user identities but also ensure that users are authorized to perform actions within their sessions without compromising security. For the mobile application prototype focused on reducing procrastination and gamification, implementing robust authentication and reliable session management is imperative to protect against unauthorized access and session hijacking.

To strengthen the authentication process, the prototype will require users to provide multiple forms of verification. This includes SMS-based verification, the use of authentication apps and backup codes. MFA significantly reduces the risk of unauthorized access even if one credential component is compromised.

Depending on the sensitivity of the actions being performed or the user's login behavior, the system may invoke additional security checks. For instance, if a login attempt is made from a new device or location, the system will prompt for additional verification steps or send an alert to the user’s primary email. The prototype will enforce strong password policies requiring users to create passwords with a mix of characters, numbers, and symbols. Passwords will be stored using salted hash functions to ensure that stored credentials are not in plain text. Additionally, the prototype will integrate features for password recovery and reset that are secure and user-friendly.

Maintaining the integrity and security of user sessions is crucial to preventing session-related attacks such as session hijacking and fixation:

- Sessions will have an automatic timeout limit to reduce the risk of unauthorized access when devices are left unattended. For sessions requiring extended duration, periodic re-authentication will be necessary, especially before accessing sensitive features or data.
- Session tokens will be generated using cryptographic methods to ensure they are unique and cannot be guessed or reused. These tokens will be securely stored on the device and validated on the server for each session-related request.
- Proper session termination practices will be implemented to ensure that sessions are securely ended when users log out or after periods of inactivity. This includes invalidating session tokens both client-side and on the server.

To ensure that the authentication and session management systems remain secure against emerging threats, the prototype will undergo regular security reviews and updates. This includes updating authentication protocols and session management strategies to incorporate new security practices and respond to new vulnerabilities discovered in the technology landscape.

9.2. Platform interaction

In the design of digital solutions aimed at combating procrastination, understanding the user and system interactions is paramount to identifying potential security risks. The prototype involves complex interactions where users manage tasks, engage socially, and earn rewards based on their activities. Table 3 below categorizes the different types of user interactions within the application, identifying potential security risks and proposing mitigation strategies for each interaction type.

The core functionalities where user interaction is most prevalent include account creation and management, task management, social interactions, and the reward system. Each interaction point involves specific data points such as emails, usernames, passwords, task descriptions, and personal details, which are susceptible to various security threats. For instance, account creation and management are critical areas vulnerable to account takeovers and data breaches. This necessitates robust security measures such as CAPTCHA, two-factor authentication (2FA), and rate limiting to prevent unauthorized access and safeguard user information.

Table 3
User and System Interaction Analysis

Interaction Type	Description	Data Points	Security Concerns	Mitigation Strategies
Account Creation and Management	Users create accounts and manage profiles	Email, username, password, personal details	Vulnerable to account takeover, and data breaches	Implement CAPTCHA, two-factor authentication (2FA), and rate limiting
Task Management	Users input and manage tasks	Task descriptions, categories, deadlines	Unauthorized access, and data manipulation risks	Use data validation and user authentication to secure access
Social Interaction	Users participate in groups, chat, and challenges	Messages, group memberships, interactions	Harassment, spreading of malware, privacy breaches	Content filtering, user reporting, and blocking mechanisms
Reward System	Users earn and spend points on virtual goods	Points, item purchases, reward history	Exploitation of reward mechanisms, unfair manipulation	Monitor for unusual activity, and validate transactions server-side

9.3. Implementing and evaluating security measures for a prototype in Figma

The primary objective of our work is to implement and evaluate the security measures designed within a digital solution prototype to combat procrastination. This work bridges theoretical security planning and practical application, showcasing how advanced security protocols can seamlessly integrate into a user-centric digital environment. The focus is on enhancing the prototype's security while maintaining ease of use and ensuring compliance with relevant data protection laws.

The prototype, designed using Figma, simulates a mobile application that provides task management tools enhanced with social features to engage users in a productive and secure environment. The prototype includes detailed user interaction flows for registration, authentication, account management, and privacy settings, emphasizing robust security measures such as multi-factor authentication (MFA), data encryption, and compliance with the General Data Protection Regulation (GDPR).

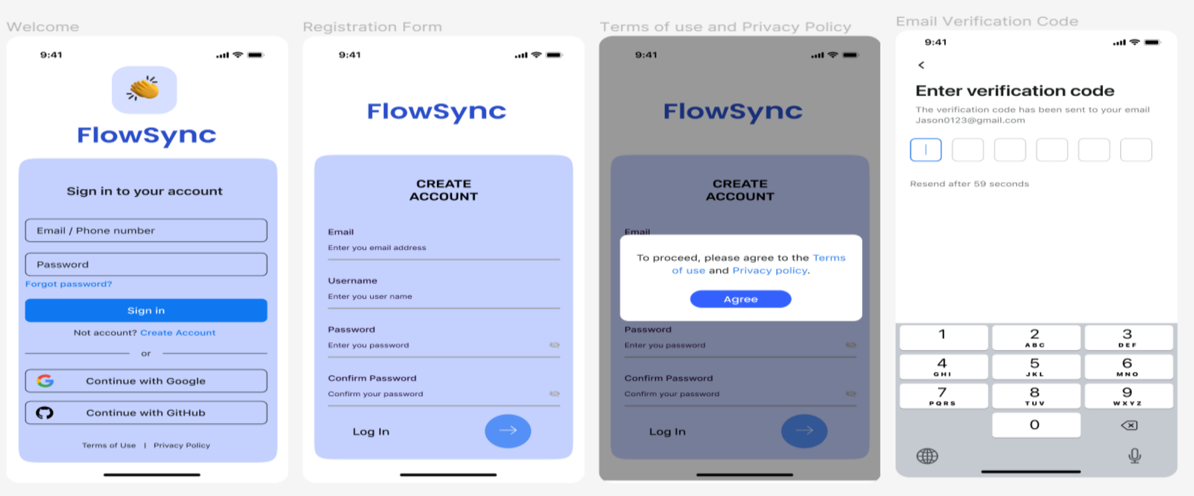
9.4. Registration and authentication flow

The registration and login processes are designed to ensure user identity verification while maintaining a balance between security and user convenience. These processes are critical for preventing unauthorized access and protecting user data from potential security breaches.

The application supports various authentication methods to cater to user preferences and security needs. This includes traditional email/password combinations and more seamless integrations with third-party authentication providers like Google and GitHub. Figure 2. below provides a more detailed visual presentation of this process.

For third-party authentication providers, the application uses OAuth, a widely accepted open standard for access delegation. It allows users to grant websites or applications access to their information on other websites but without giving them the passwords. This is particularly useful for enhancing user experience by simplifying the login process and reducing password fatigue.

All data transmitted during the registration and login processes is encrypted using SSL/TLS, ensuring that user credentials and other sensitive information are securely transmitted over the internet.

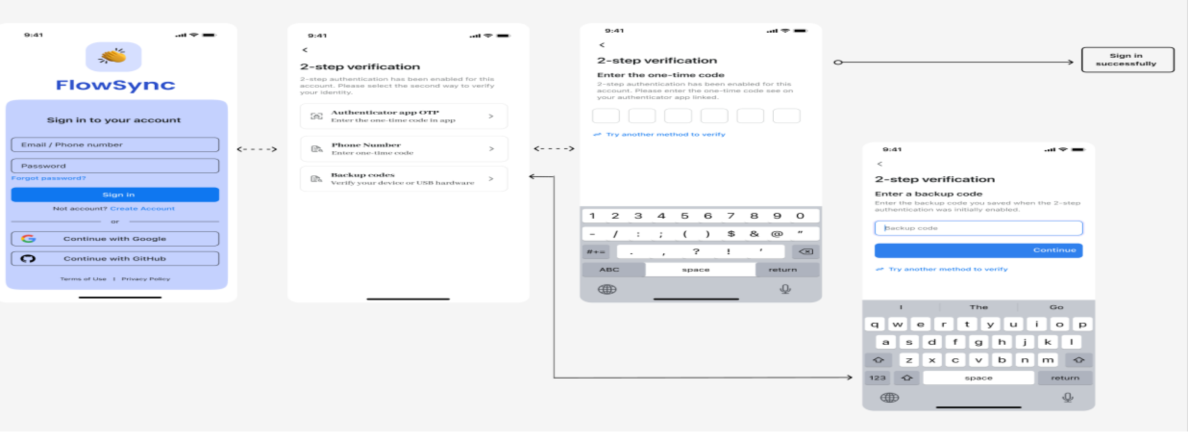


To proceed, please agree to the Terms of use and Privacy policy.

The verification code has been sent to your email Jason0123@gmail.com

Figure 2: Registration process flow.

MFA adds an additional layer of security by requiring two or more verification factors, which significantly decreases the risk of unauthorized access. The application provides several options for MFA, each designed to meet different user needs and security levels. The visual process is presented in the Figure 3.



2-step authentication has been enabled for this account. Please select the second way to verify your identity.

2-step authentication has been enabled for this account. Please enter the one-time code see on your authenticator app linked.

Enter the backup code you saved when the 2-step authentication was initially enabled.

Figure 3: Two-factor authentication.

SMS-based Verification. Users receive a one-time password (OTP) via SMS, which they must enter in addition to their regular password. This method is widely used due to its simplicity and relatively strong security profile. The system utilizes a reliable SMS gateway provider to ensure timely delivery of OTPs. This method leverages the user's access to a mobile device as a form of something they have, adding a physical layer of security. SMS-based OTP is popular and widely understood by users, making it a practical choice for initial MFA implementation.

Authentication App (e.g., Google Authenticator). Recommended for users seeking higher security, this method involves generating a time-based OTP through an app installed on the user's smartphone. The application uses a Time-Based One-Time Password (TOTP) algorithm, which creates a new password at fixed intervals, ensuring that each password is only valid for a short period. Unlike SMS, which can be intercepted, TOTP requires physical access to the user's smartphone, providing a higher level of security.

Backup Codes. As a fallback mechanism, users can generate a set of backup codes during MFA setup. These codes can be used to access the account if the primary MFA method is unavailable. Backup codes are designed to be used sparingly and securely stored by the user. They are generated in the app and can be printed or saved offline for emergency use.

Two-factor authentication can be enabled and setup in the security settings, where users can choose their preferred MFA method. The interface guides them through the setup process for each option. Each time the user logs in, after entering their password, the system prompts them to complete the second factor of authentication based on their chosen method.

9.5. Password and security management

Password and security management are essential components of maintaining robust account security. This section of the application allows users to control and secure their account credentials and settings, providing tools for password changes, recovery options, and managing other security-related preferences.

Password Change allows users to update their password regularly, which is a fundamental practice in maintaining account security. The system employs a password strength validator to ensure that users create strong, hard-to-guess passwords. This tool checks for minimum length, the inclusion of special characters, numbers, and mixed-case letters. Passwords are never stored as plain text. They are hashed using a secure hash algorithm, enhancing the security of stored credentials even in the event of a data breach.

In case users forget their passwords, the application provides a secure method to regain access to their accounts. Users can request a password reset link sent to their registered email or SMS, depending on their security preferences. This process includes verification steps to ensure that only the rightful account owner can reset the password. To prevent abuse, the password reset feature is equipped with rate limiting, reducing the risk of brute force attacks aiming to guess or reset passwords maliciously.

Users can review and adjust their MFA settings, enabling or disabling MFA methods according to their security needs. A dedicated section within the security settings allows users to toggle on or off different MFA options, view their current configurations, and set up new methods if necessary.

Session Management provides a control panel for users to see all active sessions across different devices, offering the ability to end sessions that they do not recognize or no longer need. Each session is uniquely identified and displayed with information such as device type, location (if available), and last active time. This helps users manage their sessions effectively. Users can instantly log out from any device remotely, enhancing security in case a device is lost or stolen. The implementation of security measures as password resetting involves creating intuitive and secure interfaces where users can easily manage their password and security settings.

9.6. Data privacy management

Data privacy management is a critical component that empowers users to control their personal information within the application. This area focuses on ensuring users can exercise their rights over their data, in compliance with data protection laws such as GDPR. It includes managing data sharing preferences, handling data access requests, and ensuring transparent communication regarding data usage.

Privacy Settings Dashboard centralizes all privacy-related settings, making it easy for users to understand and manage their data privacy preferences. The dashboard is designed to offer a clear overview of privacy settings, including data sharing options and access rights, with easy-to-navigate sections and descriptive icons. Information displayed is dynamically adjusted based on user settings and preferences, ensuring users receive relevant and personalized information.

Privacy Policy allows users to view the data the application has collected about them and to request a copy in a portable format for transparency and control over their information. It is extremely important to ensure that all data handling processes are secure, minimizing the risk of unauthorized access during the data retrieval process. Users are able to to request the deletion of their account and associated data, aligning with the "right to be forgotten".

Another security feature implemented is Login Alerts, with which users can preferences for how they receive notifications about unrecognized logins—either through in-app notifications, emails, or both. Alerts are integrated with the user's account settings, allowing for easy adjustments anytime.

Moreover, Automated Checkup offers automated recommendations for users to enhance their account security, such as updating passwords, verifying email addresses, and confirming phone numbers are correct. It provides interactive tips and direct links to update security settings, making it easy for users to follow through on recommendations.

Device Permissions Features is a dedicated section within the app settings that allows users to see at a glance all the permissions the app has requested and to toggle these permissions on or off. The dashboard is structured to provide a clear and concise overview of all device permissions, such as camera, microphone, location, and contacts. Each permission is accompanied by an explanation of why it is needed, enhancing user trust and compliance with privacy practices. The app uses system APIs to request permissions only when necessary, following the principle of least privilege. Permissions can be toggled on or off depending on user preference, with the app responding accordingly by enabling or disabling specific features.

Users can manage permissions individually, providing them with the ability to tailor the app’s access to only those functionalities they are comfortable with. Permissions are requested in context, meaning the app asks for permission at the point when access to a device feature is necessary, which can help reduce user concerns about privacy.

10. Conclusions

1. This initial phase successfully laid the foundational groundwork for understanding the complex landscape of information security within digital solutions aimed at combating procrastination. By exploring various security frameworks, threat modeling, and risk management techniques, the assignment provided a thorough theoretical backdrop against which practical security measures can be developed and implemented. It emphasized the importance of robust information security management to safeguard sensitive user data and maintain trust in digital applications. The insights gained serve as the basis for the subsequent practical applications, ensuring a well-informed approach to designing secure digital solutions.

2. Building on the theoretical knowledge, this phase applied these concepts to design detailed security requirements for the prototype of a digital solution focused on enhancing productivity through procrastination management. Covering critical aspects of security such as authentication, data privacy, session management, and compliance with legal standards like GDPR, the work not only addressed potential vulnerabilities identified through threat modeling but also set a solid framework for implementing these security features practically. This comprehensive approach ensures that the prototype is not only functional but also secure from various cybersecurity threats.

3. The final phase brought the theoretical designs and security requirements to life through practical implementation within a digital solution prototype. Detailing the integration of security measures into the prototype demonstrated the feasibility and effectiveness of the security strategies in a simulated real-world environment. This work provided insights into the challenges of implementing security features and solutions to enhance user experience without compromising security. Moreover, it showcased how security and functionality can be balanced effectively, paving the way for potential future development and real-world application of the prototype.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Rajasekharaiah, K.M., et al. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering, 981*, 022062.

[2] Rouland, Q., Hamid, B., & Jaskolka, J. (2021). Specification, detection, and treatment of STRIDE threats for software components: Modeling, formal methods, and tool support. *Journal of Systems Architecture, 117,* 102073.

[3] Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE), 04(01),* 1-20.

[4] Van der Ham, J. (2021). Toward a Better Understanding of “Cybersecurity”. *Digital Threats: Research and Practice, 2(3),* Article 18.

[5] Cisco. (2017, October 3). *Securing Cisco IP Telephony Networks*. Cisco Press. Retrieved from https://www.ciscopress.com/articles/article.asp?p=2803867&seqNum=4

[6] International Organization for Standardization. (2022). Information technology — Security techniques — Information security management systems – Requirements (ISO/IEC 27001:2022). Retrieved from https://www.iso.org/standard/27001

[7] Al-Janabi, S., & Al-Shourbaji, I. (2021). Information Security Requirement: The Relationship Between Confidentiality, Integrity and Availability in Digital Social Media. In *Information Security Theory* and Practice (pp. 289-305). Springer.

[8] Hajrić, A., Smaka, T., Baraković, S., & Baraković Husić, J. (2020). Methods, methodologies, and tools for threat modeling with case study. Telfor Journal, 12(1).

[9] Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity and Availability in Digital Social Media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)* (pp. 229-237). Springer, Singapore.

[10] California Legislative Information. (n.d.). Civil Code - CIV. Retrieved from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode =CIV&title=1.81.5

[11] Daisie Team. (2023, August 7). Cryptography for Mobile App Security: 5 Ways. Daisie. Retrieved from https://blog.daisie.com/cryptography-for-mobile-app-security-5-ways/

[12] EU General Data Protection Regulation (GDPR). (2018). Retrieved from http://www.privacy-regulation.eu/en/

[13] Hussain, O. K. (2022). The process of risk management needs to evolve with the changing technology in the digital world. *Published online: 12 August 2022*. Springer Nature.

[14] Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: tracking in mobile apps. *Internet Policy Review*, 10(4).

[15] OWASP. (2024). Mobile Application Security Verification Standard (MASVS) (Version 2.1.0) [OWASP MASVS]. https://mas.owasp.org/MASVS

[16] OWASP. (n.d.). Mobile App Cryptography. In OWASP Mobile Application Security Testing Guide (MASTG). Retrieved from https://mas.owasp.org/MASTG/General/0x04g-Testing-Cryptography/

[17] Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. Encyclopedia, 1, 602–617. https://doi.org/10.3390/encyclopedia1030050

[18] Lambert, T. (2023). Personal Data Protection in Mobile Apps: Best Practices and Guidelines. Retrieved from https://pdtn.org/personal-data-protection-in-mobile-apps/

[19] National Institute of Standards and Technology. (2024, April 3). NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

[20] NIST. (2012). Guide for conducting risk assessments (NIST SP 800-30 R1). NIST Special Publication, 800-30 Revision 1.

[21] Personal Data Protection Commission Singapore (PDPC). (2018, January 25). Guide to Basic Data Anonymization Techniques. Retrieved from https://iapp.org/resources/article/guide-to-basic-data-anonymization-techniques/

[22] Tucker, B. (2018, June 21). OCTAVE® FORTE and FAIR Connect Cyber Risk Practitioners with the Boardroom. Retrieved from https://insights.sei.cmu.edu/blog/octave-forte-and-fair-connect-cyber-risk-practitioners-with-the-boardroom/