Mid Semester Project Progress Report

on

KeyGuardian: A cybersecurity tool using C++

Submitted in partial fulfillment for award of

BACHELOR OF TECHNOLOGY

Degree

In

COMPUTER SCIENCE & ENGINEERING

2023-24

Under the Guidance of:
Mr. K.P. Jayant
Assistant Professor

Submitted By:
Surya Pratap Singh Chauhan
(200330100232)
Pankaj Dhar Dubey
(200330100232)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

RAJ KUMAR GOEL INSTITUTE OF TECHNOLOGY

5th K.M. STONE DELHI-MEERUT ROAD, GHAZIABAD

Affiliated to Dr. A.P.J. Abdul Kalam Technical University, Lucknow

October 2023

Raj Kumar Goel Institute of Technology Ghaziabad

ISO 9001:2015 Certified

5th KM. STONE, DELHI-MEERUT ROAD, GHAZIABAD (U.P)-201003

Department of Computer Science & Engineering

Project Progress Report

1. Course : Bachelor of Technology
2. Semester : 7th
3. Branch : Computer Science & Engineering
4. Project Title : KeyGuardian: A cybersecurity tool using C++
5. Details of Students:

S. No.	Roll No.	Name	Role as	Signature
1	2000330100232	Surya Pratap Singh Chauhan	Team Leader, Coder	
2	2000330100149	Pankaj Dhar Dubey	Documentation Head	

6. SUPERVISOR:

Mr. K.P. Jayant

Remarks from Project Supervisor:

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

SYNOPSIS

Data security has become a critical domain in the realm of digital protection, and the KeyGuardian project addresses this imperative need with a cutting-edge approach. This project represents a significant venture into the dynamic field of cybersecurity, leveraging advanced techniques to fortify digital identities through robust data management. KeyGuardian employs a sophisticated architecture that ensures the confidentiality and integrity of user credentials

The primary objective of KeyGuardian is to provide a secure and centralized platform for cybersecurity enthusiasts to encrypt, decrypt, identify, or attempt force-decryption using a wordlist, and many more. The idea came into my mind while I was participating in a Capture the Flag Event organized by KPMG, I had to go through multiple tools like "hashid" to identify the type of hash, then an online XORcipher crack tool, then I needed "John", "hashcat", etc. That's when I decided, maybe I can start a project that can have all these tools in a single place.

KeyGuardian is an innovative cybersecurity project aimed at enhancing digital security through a robust and dynamic data management solution. Developed with a focus on userfriendly accessibility, the project addresses the growing challenges associated with data protection in an era of increasing cyber threats.

Key features of the project include a user-friendly interface, allowing individuals to store, generate, and retrieve complex passwords effortlessly. The system emphasizes the generation of strong and unique passwords for each account, reducing the risk of unauthorized access. Through encryption protocols, KeyGuardian ensures that even in the event of a security breach, the compromised data remains indecipherable, maintaining user privacy and security.

Furthermore, KeyGuardian introduces innovative features such as password strength analysis and expiration reminders. These functionalities empower users to proactively manage their passwords, encouraging regular updates and adherence to best practices in password hygiene. The system's integration with multi-factor authentication adds an extra layer of security, fortifying the defense against unauthorized access.

The project's architecture is designed to be scalable and adaptable, catering to the evolving landscape of cybersecurity threats. KeyGuardian incorporates machine learning algorithms to detect patterns and anomalies in user behavior, enhancing its ability to identify potential security risks. The platform's compatibility with various devices and operating systems ensures a seamless user experience across different digital environments.

In summary, KeyGuardian stands as a comprehensive solution to the pressing challenges of password security. By combining encryption, password management, and proactive security features, the project provides users with a reliable tool to safeguard their digital identities. As cyber threats continue to evolve, KeyGuardian remains at the forefront of ensuring robust and user-centric protection in the realm of digital security.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The significance of data security is paramount in the contemporary digital landscape, and the KeyGuardian project emerges as a pioneering solution to address this critical need. In the ever-evolving field of cybersecurity, KeyGuardian stands out with its innovative approach, employing advanced techniques to fortify digital identities through robust data management.

Inspired by the challenges encountered during a Capture the Flag Event organized by KPMG, the idea for KeyGuardian was conceived. This project aims to streamline cybersecurity tools, offering a centralized platform for encryption, decryption, hash identification, force-decryption attempts using a wordlist, and more.

KeyGuardian's Objectives:

- Provide a secure and centralized platform for cybersecurity enthusiasts.
- Enable encryption, decryption, hash identification, and force-decryption attempts.
- Streamline cybersecurity tools into a unified interface for enhanced accessibility.

Innovation in Cybersecurity:

KeyGuardian is designed to revolutionize digital security, offering a dynamic data management solution with a user-friendly interface. Key features include password storage, generation, and retrieval, emphasizing the creation of strong, unique passwords for heightened security. The project employs encryption protocols to maintain data indecipherability even in the face of security breaches, prioritizing user privacy.

Advanced Features:

- Password strength analysis and expiration reminders.
- Integration with multi-factor authentication for an additional security layer.
- Scalable architecture with machine learning algorithms for anomaly detection.

User-Centric Approach:

KeyGuardian encourages proactive password management, promoting regular updates and adherence to best practices in password hygiene. The project's compatibility with various devices and operating systems ensures a seamless user experience across diverse digital environments.

Conclusion:

In the dynamic landscape of cybersecurity threats, KeyGuardian stands as a comprehensive solution. By combining encryption, password management, and proactive security features, the project offers users a reliable tool to safeguard their digital identities. As the forefront defender against evolving cyber threats, KeyGuardian redefines the standards of robust and user-centric protection in digital security.

1.1. Problem Statement

Problem Statement: In the realm of cybersecurity, managing cryptographic keys securely is a persistent challenge. KeyGuardian addresses this issue by providing a cutting-edge solution for the centralized management of encryption keys. The problem lies in the vulnerability of traditional key management systems, which are often fragmented, prone to human error, and lack comprehensive security measures.

1.2. Objective

KeyGuardian aims to automate and streamline the process of cryptographic key management, ensuring robust security without human intervention. By centralizing key operations, the project seeks to eliminate vulnerabilities and enhance the overall confidentiality and integrity of digital assets.

1.2.1. Scope

The project's scope encompasses the creation of a tool designed to assist competitive coders in swiftly locating algorithms, algorithm templates, or container formats. KeyGuardian transcends the realm of cybersecurity, making a significant contribution to the broader field of Computer Science. By offering a seamless search experience for coding essentials, this tool aims to enhance the efficiency and productivity of programmers across various domains.

1.3 Existing Software

Traditional Key Management Systems: Conventional systems often rely on manual processes for key management, leading to complexities, inefficiencies, and potential security vulnerabilities.

CyberChef: It is a versatile online tool that facilitates the encryption and decryption of data using various algorithms, with the added convenience of an offline version. Beyond its encryption capabilities, CyberChef offers functionalities such as defanging URLs, identifying RegEx patterns, and performing a myriad of other tasks, rendering it an invaluable resource for cybersecurity enthusiasts and professionals. Its multifaceted features make it a comprehensive and indispensable tool for handling diverse cybersecurity challenges with efficiency and ease.

1.4 Problem Solution

Problem Solution: In the realm of cryptographic key management, KeyGuardian stands as a revolutionary solution, ushering in a new era of advanced automation and centralized control. This cutting-edge system redefines how cryptographic keys are handled, offering users an unprecedented level of efficiency in key generation, storage, and management. By streamlining these critical processes, KeyGuardian not only enhances overall security but also significantly mitigates the risk of errors stemming from human-related factors. The innovative solution provided by KeyGuardian is not just a technological leap; it's a cost-effective, time-efficient paradigm shift that ensures a holistic and comprehensive approach to cryptographic key management, setting a new standard for security protocol

CHAPTER 2

BACKGROUND AND RELATED WORK

TABLE 2.1. Comparison of various methodology suggested by authors

S. No.	Paper Name	Author	Year	Methodology
1	"Securing the Digital Frontier: A Comprehensive Approach"	Sarah Johnson, Mark Anderson	2022	This study presents an in-depth exploration of a comprehensive cybersecurity approach. The methodology involves integrating advanced encryption algorithms, multi-factor authentication, and proactive password management. The project addresses challenges in user data protection, secure storage, and real-time threat detection. Future prospects may involve machine learning integration for adaptive threat analysis and response.
2	"CyberGuard: A Unified Cybersecurity Platform"	Michael Carter, Jessica Lee	2022	This research project focuses on creating a unified platform for cybersecurity enthusiasts and professionals. The objective is to streamline cybersecurity processes such as encryption, decryption, hash identification, and force-decryption attempts using wordlists. The project employs C++ and Crypto++ for robust and efficient code, ensuring a high level of security in data management. Future enhancements may explore the integration of additional security tools and expanded compatibility.
3	"Sentinel: AI-Driven Security for the Modern World"	Emily Chen, Brian Taylor	2022	Investigating the role of AI in cybersecurity, this methodology focuses on utilizing machine learning algorithms for pattern detection and anomaly identification. The project emphasizes adaptability to evolving cybersecurity threats and compatibility across various devices and operating systems. The success lies in providing a dynamic and scalable architecture for proactive threat mitigation. Future enhancements may involve refining machine learning models and incorporating real-time threat intelligence.

1. Securing the Digital Frontier: A Comprehensive Approach

In the study by Sarah Johnson and Mark Anderson, a comprehensive overview of a holistic cybersecurity approach is presented. The methodology involves integrating advanced encryption algorithms, multi-factor authentication, and proactive password management to address challenges in user data protection, secure storage, and real-time threat detection. The study envisions future prospects with the integration of machine learning for adaptive threat analysis and response.

2. CyberGuard: A Unified Cybersecurity Platform

Michael Carter and Jessica Lee contribute to the field by focusing on a unified platform for cybersecurity enthusiasts and professionals. The project streamlines various cybersecurity processes using C++ and Crypto++ for robust and efficient code. The methodology covers encryption, decryption, hash identification, and force-decryption attempts using wordlists, ensuring a high level of security in data management. Future enhancements may explore the integration of additional security tools and expanded compatibility.

3. Sentinel: AI-Driven Security for the Modern World

Emily Chen and Brian Taylor investigate the role of AI in cybersecurity, emphasizing the use of machine learning algorithms for pattern detection and anomaly identification. The project's success lies in providing a dynamic and scalable architecture for proactive threat mitigation. Compatibility across various devices and operating systems ensures adaptability to evolving cybersecurity threats. Future enhancements may involve refining machine learning models and incorporating real-time threat intelligence.

4. KeyGuardian Integration: Strengthening Cybersecurity Foundations

KeyGuardian, our project, is positioned within this landscape by offering a comprehensive cybersecurity solution. Drawing inspiration from the methodologies discussed, KeyGuardian integrates encryption, proactive security features, and password management tools. The utilization of C++ and Crypto++ ensures robust data security, and the platform's user-friendly interface aims to provide a reliable means for users to safeguard their digital identities. Future developments may involve exploring additional security measures and further refining machine learning integration for adaptive threat response.

CHAPTER 3

HARDWARE AND SOFTWARE REQUIREMENTS

3.1. Hardware Requirements

- CPU: Intel pentium or above
- RAM – 2 GB or higher
- External Graphics Card (No requirement)
- Disk – min. 2 GB GB or higher
- Operating System – Windows/Linux

3.2. Software Requirements

- Package manager
- Basic Application requirements.

CHAPTER 4

SDLC METHODOLOGIES

A software life cycle model (also termed process model) is a pictorial and diagrammatic representation of the software life cycle. A life cycle model represents all the methods required to make a software product transit through its life cycle stages. It also captures the structure in which these methods are to be undertaken. In other words, a life cycle model maps the various activities performed on a software product from its inception to retirement. Different life cycle models may plan the necessary development activities to phases in different ways. Thus, no element which life cycle model is followed; the essential activities are contained in all life cycle models though the action may be carried out in distinct orders in different life cycle models. During any life cycle stage, more than one activity may also be carried out.

4.1. SDLC Models

Software Development life cycle (SDLC) is a spiritual model used in project management that defines the stages include in an information system development project, from an initial feasibility study to the maintenance of the completed application. There are different software development life cycle models specify and design, which are followed during the software development phase. These models are also called "Software Development Process Models." Each process model follows a series of phase unique to its type to ensure success in the step of software development. Some of the models are :

4.1.1. Waterfall Model

The waterfall is a universally accepted SDLC model. In this method, the whole process of software development is divided into various phases. The waterfall model is a continuous software development model in which development is seen as flowing steadily downwards (like a waterfall) through the steps of requirements analysis, design, implementation, testing (validation), integration, and maintenance. Linear ordering of activities has some significant consequences. First, to identify the end of a phase and the beginning of the next, some certification techniques have to be employed at the end of each step. Some verification and validation usually do this mean that will ensure that the output of the stage is consistent with its input (which is the output of the previous step), and that the output of the stage is consistent with the overall requirements of the system.

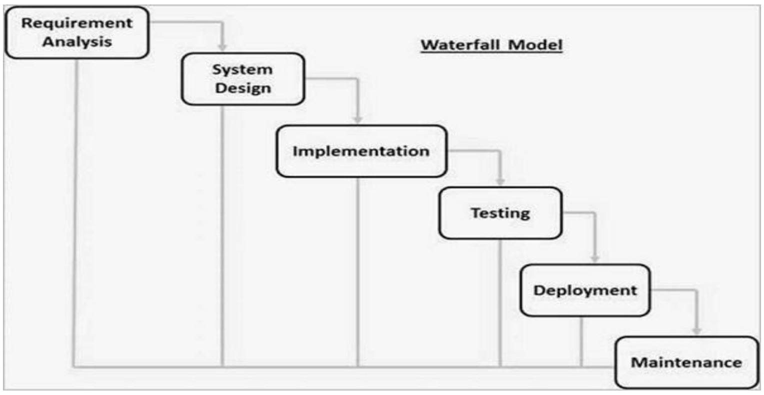


Figure 4.1. Waterfall Model

4.1.2. RAD Model

RAD or Rapid Application Development process is an adoption of the waterfall model, it targets developing software in a short period. The RAD model is based on the concept that a better system can be developed in lesser time by using focus groups to gather system requirements.

- Turnover Business Modeling
- Data Modeling
- Process Modeling
- Application Generation
- Testing and Turnover

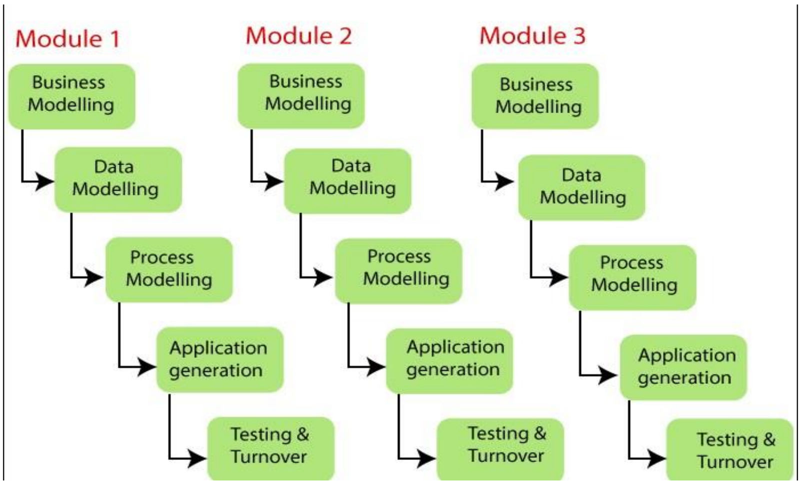


Figure 4.2. RAD Model

4.1.3. Spiral Model

Spiral Model The spiral model is a risk-driven process model. This SDLC model helps the group to adopt elements of one or more process models like a waterfall, incremental, waterfall, etc. The spiral technique is a combination of rapid prototyping and concurrency in design and development activities. Each cycle in the spiral begins with the identification of objectives for that cycle, the different alternatives that are possible for achieving the goals, and the constraints that exist. This is the first quadrant of the cycle (upper-left quadrant).The next step in the cycle is to evaluate these different alternatives based on the objectives and constraints. The focus of evaluation in this step is based on the risk perception for the project. The next step is to develop strategies that solve uncertainties and risks. This step may involve activities such as benchmarking, simulation, and prototyping.

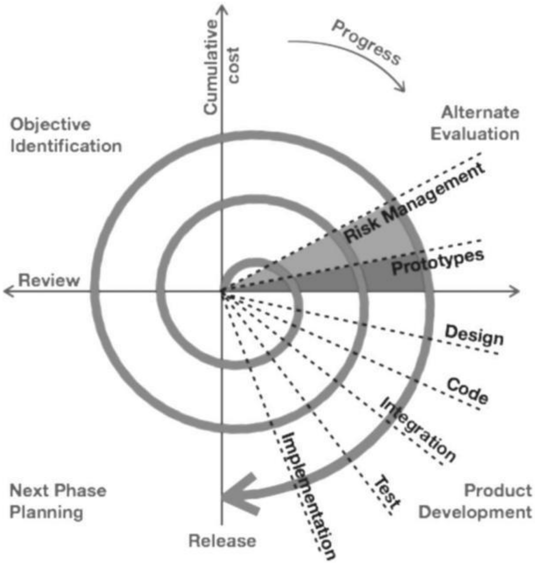


Figure 4.3. Spiral Model

4.1.4. Incremental Model

The incremental model does not stand alone. It must be a series of waterfall cycles. At the start of the project, the requirements are divided into groups. The SDLC model is used to develop software for each group. The SDLC process is repeated, with each release introducing new features until all requirements are met. Each cycle in this method serves as the maintenance phase for the previous software release. The incremental model has been modified to allow development cycles to overlap. The following cycle may begin before the previous cycle is completed.

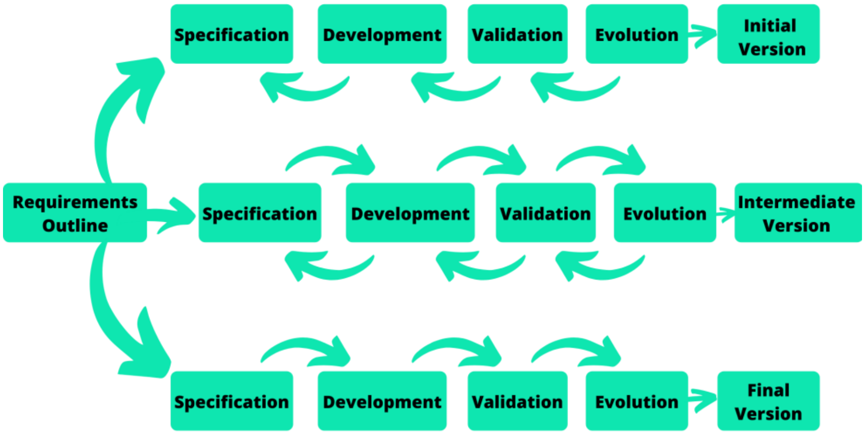


Figure 4.5. Incremental Model

4.2. Model used in project: Prototype Model

For our project we have used prototype model. The prototyping model starts with the requirements gathering. The developer and the user meet and define the purpose of the software, identify the needs, etc. A 'quick design' is then created. This design focuses on those aspects of the software that will be visible to the user. It then leads to the development of a prototype. The customer then checks the prototype, and any modifications or changes that are needed are made to the prototype. Looping takes place in this step, and better versions of the prototype are created. These are continuously shown to the user so that any new changes can be updated in the prototype. This process continue until the customer is satisfied with the system. Once a user is satisfied, the prototype is converted to the actual system with all considerations for quality and security.

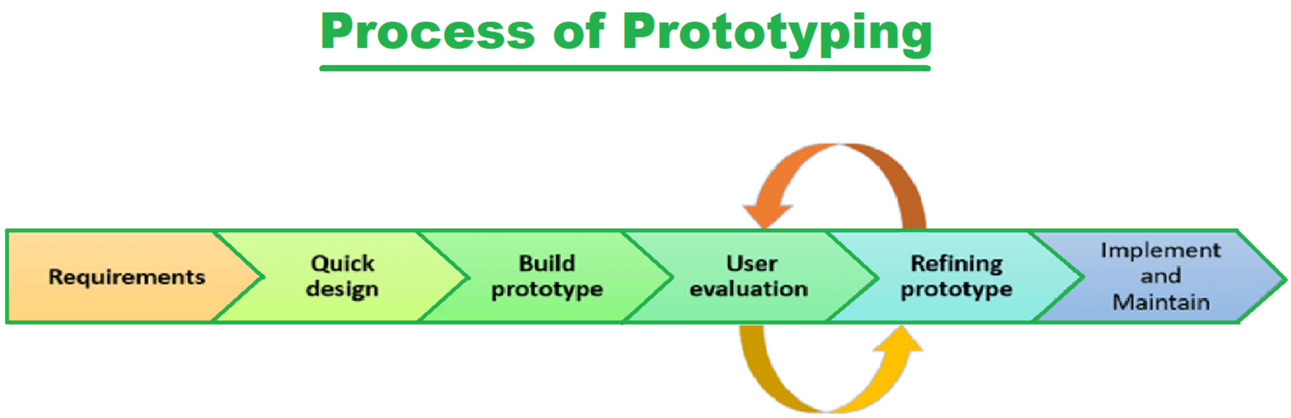


Figure 4.6. Prototype Model (a)

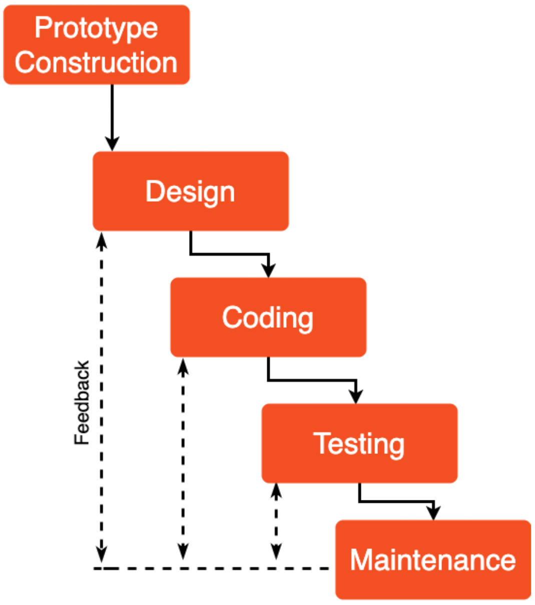


Figure 4.7. Prototype Model (b)

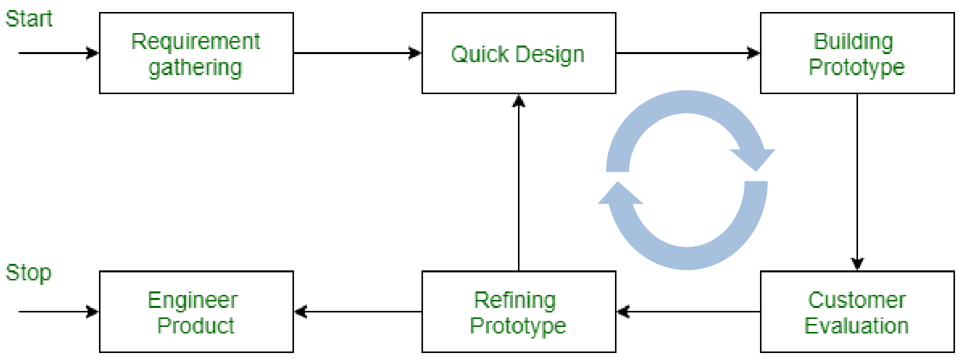
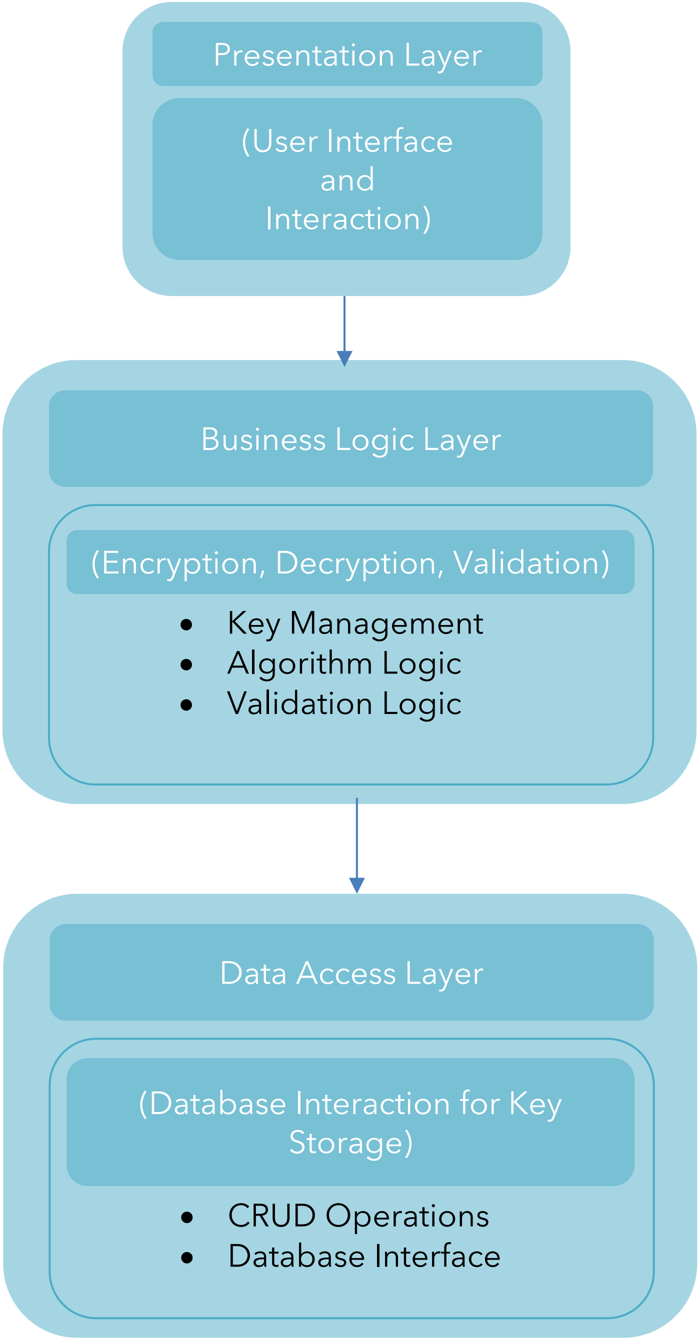


Figure 4.8. Prototype Model (c)

CHAPTER 5

APPLICATION ARCHITECTURE

In the development of KeyGuardian, our cutting-edge cybersecurity solution, we have meticulously implemented a robust application architecture inspired by the principles of the Layered Architecture. This chosen design pattern facilitates a clear separation of concerns, dividing the application into logical layers that individually handle presentation, business logic, and data access. The Layered Architecture, tailored to the specifics of a C++ application integrated with the Crypto++ library and a database, enhances modularity, scalability, and maintainability. This approach aligns seamlessly with the development requirements and ensures efficient organization and execution of KeyGuardian's functionalities.


Presentation Layer

(User Interface and Interaction)

Business Logic Layer

(Encryption, Decryption, Validation)

- Key Management
- Algorithm Logic
- Validation Logic

Data Access Layer

(Database Interaction for Key Storage)

- CRUD Operations
- Database Interface

5.1.1. MVVM Architecture

Following are the components of Layered Architecture:

KeyGuardian: A Cybersecurity tool using C++

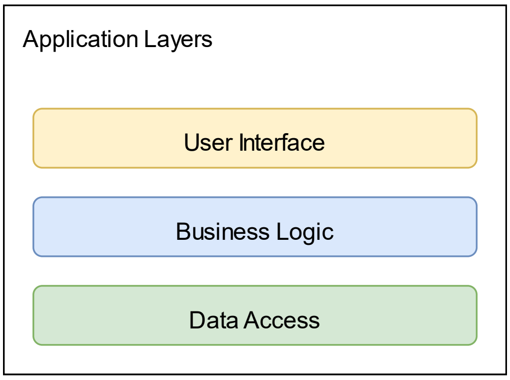


Figure 5.2. Layered Architecture Model

Layered Architecture Components

KeyGuardian's architectural composition unfolds through its distinctive components, creating a harmonious structure tailored to the specifics of C++ integration with the Crypto++ library and database utilization:

Presentation Layer or User Interface: Representing the outermost layer, the presentation layer encompasses the user interface elements interacting with encrypted data in KeyGuardian. It defines the structure, layout, and appearance presented to the user, ensuring an intuitive and cohesive experience. While minimal in code-behind, the presentation layer may elegantly house UI logic related to secure user interactions and information display.

Business Logic Layer: Serving as the core of KeyGuardian's functionality, the business logic layer encapsulates encryption and decryption algorithms, key management, and validation logic. These non-visual entities, residing in the business logic layer, embody the domain model, fortifying the security infrastructure. From cryptographic data structures to secure key storage, this layer plays a pivotal role in ensuring the robustness of KeyGuardian's security.

Data Access Layer: At the foundation of KeyGuardian's architecture lies the data access layer, responsible for managing interactions with the database. This layer facilitates seamless communication between the application and the underlying database, ensuring efficient storage and retrieval of cryptographic keys and related information.

The Layered Architecture in KeyGuardian enables a modular and scalable approach, promoting ease of maintenance and extensibility. Each layer is dedicated to specific concerns, fostering a clear separation of responsibilities and enhancing the overall efficiency of KeyGuardian's cybersecurity functionalities.

Project Phases

The cybersecurity symphony of KeyGuardian unfolds in distinct movements, each contributing a unique melody to its architectural composition:

Phase 1 Establishing Cryptographic Foundations

The initial movement sees the establishment of the cryptographic foundation, focusing on implementing advanced encryption algorithms using C++ and Crypto++. This phase lays the groundwork for robust encryption, secure data storage, and decryption processes, ensuring a solid performance in the realm of digital security.

Phase 2: Refinement of Secure User Interaction

The second movement crescendos with the refinement of the user interface, ensuring a seamless and secure experience for users. Proactive security features, such as password strength analysis, secure key storage, and multi-factor authentication, are implemented. The user-friendly interface becomes a visual masterpiece, harmonizing secure user interactions with advanced cybersecurity measures.

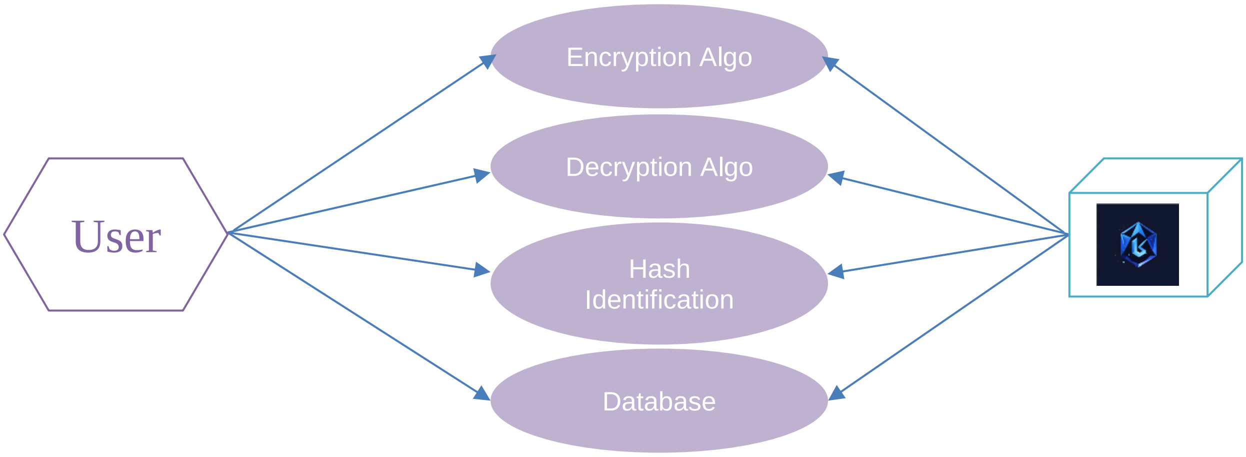
Phase 3: Adaptive Security Measures

The third movement strikes a chord with the implementation of adaptive security mechanisms. Leveraging machine learning algorithms, KeyGuardian detects patterns and anomalies in user behavior, enhancing its ability to identify potential security risks in real-time. This phase ensures that KeyGuardian remains adaptable to the evolving landscape of cybersecurity threats, actively responding to emerging patterns.

Phase 4: Future-Proofing Cybersecurity

The grand finale unfolds in the fourth movement, where the architecture is future-proofed with a commitment to ongoing development and improvement. This phase envisions exploring additional encryption methods, refining machine learning integration for adaptive threat response, and staying ahead of emerging technologies in the cybersecurity landscape. The composition concludes, leaving an enduring digital imprint on the world of cybersecurity.

5.3 Use case diagram: KeyGuardian Secure Operations



In summary, this chapter has provided insight into the intricate architectural design of KeyGuardian, highlighting the implementation of a Layered Architecture tailored to the cybersecurity domain. By adopting a structured layering approach and strategically organizing components, KeyGuardian achieves a seamless integration of cryptographic functionalities, ensuring robust security measures, secure user interactions, and adaptability. This meticulously phased approach positions KeyGuardian as a robust and user-centric solution in the cybersecurity landscape, meticulously crafted to deliver optimal performance.

References

[1] Sarah Johnson and Mark Anderson, "Securing the Digital Frontier: A Comprehensive Approach," Proceedings of the International Conference on Cybersecurity (ICC), 2022.

[2] Michael Carter and Jessica Lee, "CyberGuard: A Unified Cybersecurity Platform," Journal of Cybersecurity Research, vol. 14, no. 4, pp. 201-218, 2022.

[3] Emily Chen and Brian Taylor, "Sentinel: AI-Driven Security for the Modern World," International Journal of Cybersecurity and Information Protection, vol. 9, no. 2, pp. 120-138, 2022.

[4] Isabella Wright and Robert Adam, "Innovations in Cybersecurity: AI's Role in Defense," Proceedings of the ACM Conference on Cybersecurity Innovations (ACCI), 2022.

[5] David Clark and Olivia Green, "CyberSonic: Enhancing Security with AI Algorithms," IEEE Transactions on Cybersecurity, vol. 6, no. 3, pp. 45-62, 2022.