**Internship Report**

**Task:** Secure Authentication System using Python (Tkinter)  
**Intern:** Ammad Aziz  
**Organization:** Internee.pk  
**Internship Duration:** July-September

**1. Introduction**

During my internship at **Internee.pk**, I was assigned the task of building a **Secure Authentication System**. The primary aim was to design a desktop application that enables secure user registration and login, while following best practices of **encryption and authentication**.

The system is built using **Python Tkinter** for GUI, **SQLite** for data storage, and integrates modern cryptographic techniques to ensure sensitive information remains protected. This project also serves as a foundation for **future enhancements** like **Two-Factor Authentication (2FA)** and **OAuth 2.0** integration.

**2. Objectives**

* To design a **user-friendly authentication interface** using Tkinter.
* To implement **secure password storage** with bcrypt hashing.
* To encrypt sensitive data (like email) with **AES-256-GCM encryption**.
* To integrate persistent storage using an **SQLite database**.
* To prepare the system for **advanced authentication mechanisms** in the future.

**3. Tools & Technologies**

* **Programming Language:** Python 3.x
* **Libraries Used:**
  + tkinter → Graphical User Interface (GUI)
  + bcrypt → Secure password hashing
  + cryptography → AES-256 encryption
  + sqlite3 → Database management
* **Environment:** Windows Virtual Machine
* **Version Control:** GitHub (for code submission)

**4. Implementation Details**

**🔹 User Registration**

* Users can create accounts by providing **username, password, and email**.
* Passwords are hashed with **bcrypt** before storage.
* Emails are encrypted using **AES-256-GCM** and stored securely.

**🔹 User Login**

* On login, the entered password is checked against the **bcrypt hash**.
* If authentication succeeds, the system decrypts and displays the user’s email.

**🔹 Account Management**

* Users can:
  + **Change Password** (re-hashed with bcrypt).
  + **Delete Account** (data removed from SQLite database).
  + **Logout** securely.

**🔹 GUI Design**

* Built with Tkinter for a **simple and intuitive interface**.
* Includes separate windows for **Register, Login, and Dashboard**.

**5. Results**

* Successfully developed a **desktop authentication system** with strong security practices.
* Demonstrated use of **hashing + encryption** for layered protection.
* Provided a **working GUI prototype** for future enterprise-level improvements.

**6. Future Enhancements**

The current system is secure but designed as a **base model**. In the future, the following features can be added:

1. **Two-Factor Authentication (2FA)**
   * Integrate **Google Authenticator (TOTP)** for an extra security layer.
   * Users will scan a QR code during setup and provide a 6-digit OTP during login.
2. **OAuth 2.0 Integration**
   * Enable **Google / GitHub / Microsoft login** for seamless sign-ins.
   * Reduces password fatigue and leverages trusted identity providers.
3. **Improved Key Management**
   * Store encryption keys in a **secure Key Management System (KMS)** instead of local files.
   * Environment variables or hardware tokens can be used.
4. **Logging & Monitoring**
   * Add **activity logs** for login attempts, password resets, and suspicious behavior.
   * Could integrate with **SIEM tools** for real-time monitoring.
5. **UI/UX Enhancements**
   * Modernize Tkinter UI with themes (ttk.Style or external libraries).
   * Add animations and responsive layouts.

**7. Conclusion**

This internship project gave me practical experience in combining **security principles with application development**. I learned how to:

* Apply **password hashing and encryption** in real-world applications.
* Build structured GUI applications with **Tkinter**.
* Design a system with **future scalability and enhancements in mind**.

The Secure Authentication System is a **successful prototype** that ensures user data confidentiality and integrity. With the planned enhancements, it can evolve into a robust authentication platform suitable for enterprise use.