Sultan Qaboos University

College of Economics and Political Sciences

INFS4425 - Information System Security

LOCKER ACCESS

Done By:

Oday Al-Muharbi 132006

Ayham Al-Juma 131313

Hussain Al-Mahdi 135201

Hassan Al-Balushi 130674

Ali Al-Mania 134370

Submitted to:

Dr. Waqas Aman

Date : 11/05/2025

Contents

1. Introduction and Problem Statement

Variety of essential services are offered to Sultan Qaboos University (SQU) students to boost their academic performance and campus life. To ensure and maintain the student's academic integrity , these services provide student attendance tracking as well as it includes safe network connectivity , computer lab access for educational and experimental learning. One of the disregarded services which is offered to the students is locker access which could be found in the campus library and some of the colleges buildings. These lockers are used to store student's personal items such as laptop , iPad , textbooks or any valuable belongings to the student. Students are no longer required to carry materials between long classes.

Frequently, compared to other services , locker access is handled with less technical security regardless of its importance. Usually, small physical keys are used to control access to lockers, something that can be a threat because it can be lost or stolen. Ensuring that locker access is limited only to authorized users is important. Countless things could happen like Theft , improper use of locker space or careless storage of unallowed things could be stored in it due to insecure access to lockers. The goal of the project is to redesign locker access by implementing a safe and secure multi-factor authentication (MFA) system which is suitable for SQU environment.

1.2 Significance of Locker Access Management

Firstly, majority of the students require a private and secure location to keep their personal belongings such as notebooks and laptops etc.. , Secondly those lockers help in reducing the physical strain from carrying those belongings all day round from place to another . Moreover, using a secure locker will protect the students from theft and unauthorized messing with their stuff. Therefore, developing an efficient and trustworthy locker would benefit the SQU learning environment, SQU can guarantee better protection of personal data, property safety, and institutional control over its physical resources by strengthening the security of this service.

1.3 Problem Statement

At present, in SQU the lockers' access is outdated, which is a simple small physical key which is not secure. For example, a student can share the key with his friends or lose it somewhere he won't be able to find or track it ,sometimes he may forget the locker open. So, there is no way we can track who opened the locker and who left it open. And for the safety of the student, we won't be able to know who hides items in the locker plus we won't be able to know who is responsible for that in case something happens . The existing lock security methods are weak and easy to manipulate by the students. Therefore, the system needs to be updated with the latest tech and faster response so everything will be logged and monitored easily.

1.4 Scenario

Sarah, a CEPS student in her final year uses her locker to store academic material and personal belongings regularly. The locker system is very old and uses traditional keys given to students so they can operate the locker. One day Sarah's friend, Maryam, needed a place to store some of her belongings for a short period of time so Sarah lent her the key to her locker. During a random inspection a few days later, the university staff have found unauthorized exam related material in Sarah's locker. Sarah denies having stored those items in her locker but since the locker system is outdated there is no way for the staff to track user activity, they decide to hold her accountable.

1.5 The Need for Secure Locker Access

Students must have access to lockers at SQU to securely store their personal belongings and academic materials. However, existing physical key systems are easily shared or misused which creates security issues and a lack of responsibility. To prevent unwanted use and improve campus safety, a multi-factor authentication system is required to guarantee that only the appropriate student can access the locker.

2. Solution Architecture

2.1 Multi-Factor Authentication Scheme Description

The proposed system is a three-factor authentication system customized for securing student lockers in SQU. The authentication is done in serial stages with the aim of allowing only the authorized users. The process starts with the students scanning their SQU smart ID on the locker's in-built RFID reader. This is for establishing physical possession. The student then enters the preconfigured password through the student portal. This is to confirm knowledge. The system then generates a TOTP-based (time-based one-time-password) that is an algorithm-determined temporary passcode that uses time of day as one of its authentication components (steele, n.d.), which is transmitted to the student's email or mobile number. The locker is opened once the TOTP is entered correctly on the locker interface within the working time frame (normally 30 seconds).

This three-step process guarantees that even in the event of compromise of a single credential (i.e., password), unauthorized individuals will not be able to access the locker unless they have the smart card as well as the real-time OTP. This approach strictly adheres to global standards such as NIST SP 800-63B standards for digital identity authentication.

2.2 Hardware and Software Components

Hardware:

- **Smart Locker Unit:** with secure housing and locks
- **RFID Smart Card Reader:** to detect and verify SQU ID cards
- **Touchscreen Interface or Keypad:** for password and OTP input
- **Microcontroller:** the central processing unit
- **GSM Module or Wi-Fi Adapter:** for OTP transmission
- **LED and Speakers:** for interface feedback

Software:

- **Locker Access Management System (LAMS):** Main application that governs access logic
- **Authentication API:** Connects to SQU's central student database
- **TOTP Generator:** For secure OTP creation
- **Encrypted Communication Protocols:** Ensures all data transmission (passwords, OTPs) is encrypted
- **Database Logging System**: Logs every access attempt with metadata

2.3 Component Communication and Functionality

Our three-factor authentication system is highly dependent upon software and hardware component functionality such that the lockers' access is secured. Below is the component detail of the five components utilized by us, their functionality, and data communication among them:

RFID Smart Card Reader:
The functionality of smart card is to read the unique identifier (UID) which is stored inside the student's SQU smart card on contact. While communicating data, the student's smart card UID gets encrypted and forwarded to the Authentication API to verify with SQU's student database. In case the UID is missing or invalid then the whole process is aborted immediately.

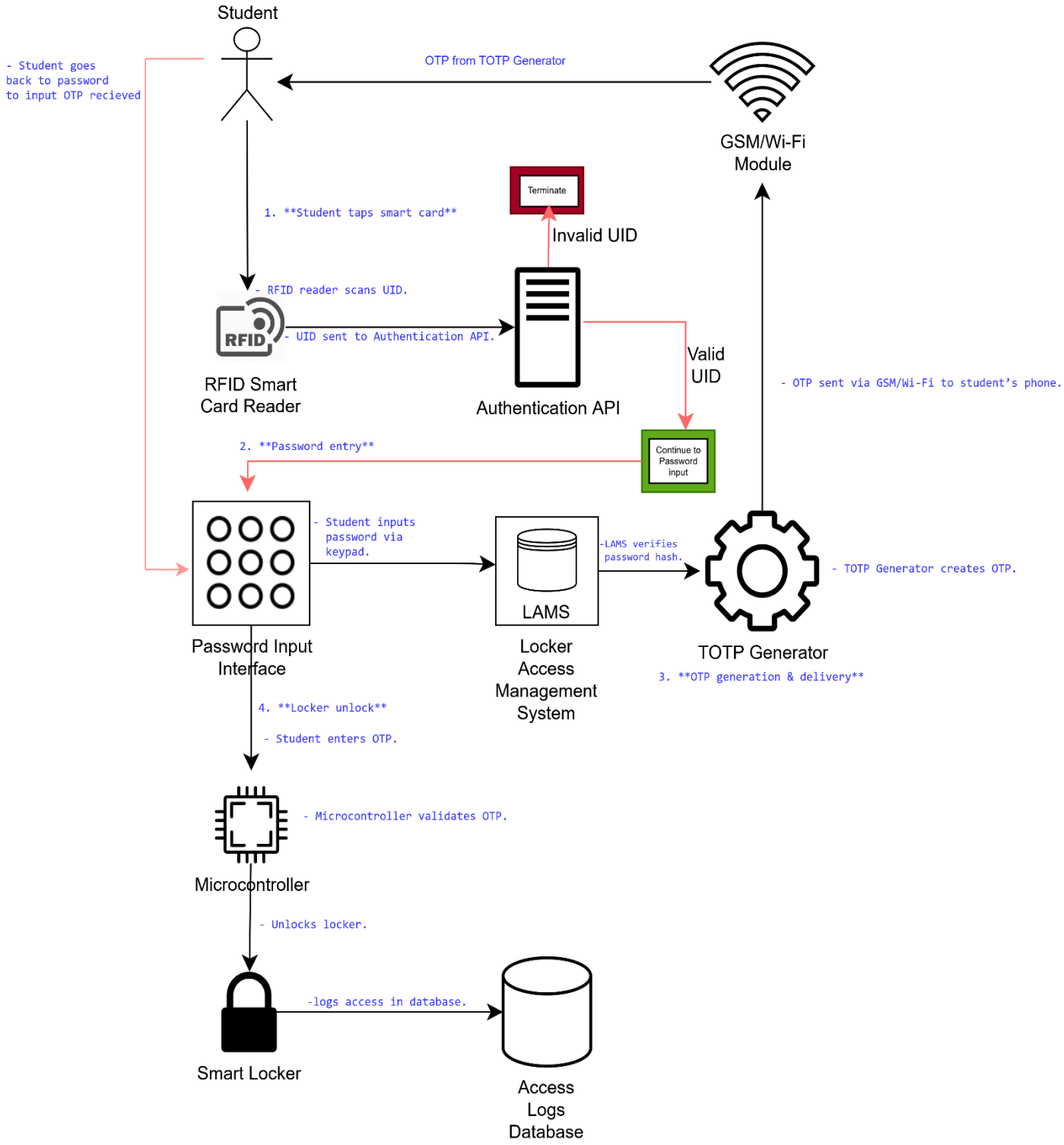
Keypad/Touchscreen Interface:
The function of this interface is to accept the password and TOTP of the student. Data in this interface is transmitted by hashing the password using SHA-256 and transmitting it to Locker Access Management System (LAMS) using TLS 1.3. Once authenticated, LAMS invokes the TOTP Generator to send a time-sensitive OTP.

Wi-Fi/GSM Module:
This module enables OTP to be sent to the email or mobile of the student in real time. The OTP is generated server side, sent by SMS or email, and has an expiry of 30 seconds. For preventing replay attacks the microcontroller of the locker stores the timestamp of the OTP.

Microcontroller (Arduino/RaspberryPi):
The microcontroller controls the locking devices and handles authentication steps. When the microcontroller receives the "access granted" signal from LAMS after successfully authenticating the OTP, it will activate the locking motor to open the door. Events will also be logged (timestamps, locker number, student ID) into the encrypted Database Logging System.

Authentication API and LAMS:
The purpose of the LAMS and Authentication API is to enforce access policies and validate credentials like UID, passwords, and UID. They work on the basis of cross verification of inputs from TOTP server and SQU's database. The whole communication is end to end encrypted, while failed attempts trigger alerts for likely violations in security.

2.4 Solution Architecture Diagram



3. Threats Prevention:

3.1 Preventing Internal Misuse

By requiring physical access to the smart card, a personal password, and access to the OTP, the system discourages casual sharing of credentials by the students. Even if a password is divulged, the OTP and the smart card will also be needed. The multi-stage barrier reduces the temptation to "lend access" to another individual and engenders a sense of ownership and accountability.

3.2 Preventing Unauthorized External Access

Three-factor requirement is solely aimed at neutralizing external aggressors. A smart card and an enrolled phone/email without SQU credentials precludes outsiders from using any locker effectively. Spawning attempts with credentials or compelling OTPs will be monitored and reported to trigger security response.

3.3 Encouraging Accountability

Every access event is recorded into a secure timestamped database with student ID, locker number, result (success/failure), and timestamp. In case of complaints, the logs can generate verifiable audit trails establishing responsibility, and thus the complaints are removed in case of theft or tampering with lockers.

3.4 Protection of Sensitive Data (Disclosure Protection)

All data transmissions, passwords, and OTPs are encrypted with TLS 1.3 encryption. OTPs are never reused and are sensitive for one minute. Card UIDs is hashed upon storage or comparison so that they cannot be reverse engineered to sensitive identifiers. The server-side database is also encrypted with AES-256 encryption.

3.5 Replay Attack Defense

TOTP makes OTPs transient. They cannot be reused and anticipated. If an attacker intercepts an OTP, it can be used for only seconds. Additionally, the system checks redundant or late OTP inputs and filters them out.

4.Related Risks and Countermeasures

4.1 Physical Device Malfunction or Hardware Failure

Malfunction of hardware units like RFID readers and GSM/Wi-Fi modules which are main parts of the locker system that are vulnerable to physical and environmental damage like humidity and dust as well as power outage. A vulnerability in these physical components could prevent students from accessing their lockers, which could lead to academic disruption and inconvenience. To prevent this from happening, lockers need to be fitted with a tamper-proof manual override device that is accessible only by authorized users (*Multi-Factor Authentication in Cyber Physical System: A State of Art Survey*, 2019). This access can only be logged by administrator ID, timestamp, and justification to ensure transparency and accountability. Further, the use of predictive maintenance approaches via embedded diagnostics can also proactively detect failing parts as well as reducing downtime (Yang, H., Han, Q. L., Ge, X., Ding, L., Xu, Y., Jiang, B., & Zhou, D, 2019). This proactive approach is supportive of fault-tolerant design principles, and the system becomes available even when hardware is operating under high stress.

4.2 Network or Server Downtime

The real-time aspect of MFA, most notably for password authentication, OTP generation, and logging, renders the system reliant on constant connectivity and availability of the authentication server. Network failure or authentication server failure could deny students access to their lockers, especially during exam time (Ahmad et al., 2012). To counter this, there should be backup authentication server functionality with automated failovers. Pursuant to NIST SP 800-63B guidelines, edge processing methodologies may enable microcontrollers in lockers to authenticate cached OTPs intermittently when central servers are unavailable (Theofanos, 2020). Additionally, load balancing will ensure that overloads are averted when access is highest to make authentication both reliable and fast.

4.3 Credential Loss or Theft

Students might lose their SQU smart card or mobile phone. Both are critical to the three-factor authentication process. If lost or stolen, these credentials might be exploited by attackers if the phone is not secure with biometric or PIN-based authentication. The integrity of the locker system is compromised in this situation, since unauthorized access can be provided through compromised credentials. A strong credential recovery process should be available. After validation through formal documents and security questions, temporary digital access tokens should be given to be used only for one-time access to a locker for permanent credentials to be recreated (Baloch, 2017). Students must also be encouraged to activate multi-layer security (such as a screen lock and biometric authentication) on their devices, and future software updates can include optional biometric login (such as fingerprint or face recognition) for extra security measures (Alotaibi & Elleithy, 2020).

Reference

Multi-factor authentication in cyber physical system: A state of art survey. (2019, February 1). In 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS) (pp. 1-6). IEEE.

Ahmad, A., Maynard, S. B., & Park, S. (2012). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370. https://doi.org/10.1007/s10845-012-0683-0

Baloch, R. (2017). *Ethical hacking and penetration testing guide*. CRC Press.

Grassi, P. A., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). U.S. Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Yang, H., Han, Q. L., Ge, X., Ding, L., Xu, Y., Jiang, B., & Zhou, D. (2019). Fault-tolerant cooperative control of multiagent systems: A survey of trends and methodologies. *IEEE Transactions on Industrial Informatics, 16*(1), 4-17.

Steele, C. (n.d.). *What is a time-based one-time password?* TechTarget. Retrieved May 2, 2025, from https://www.techtarget.com/searchsecurity/definition/time-based-one-time-password-TOTP