KSAi AN APP FOR ALL SERVICES

2110252-2110278

Computing Ethics , CCIY-112, Ms. Reem Al-Ghamdi

Rama Maqbool,Riham Al-Nashri

CASE STUDY	PLANNING
required to identify and judge such issues for your application	All questions are mutually analysed, we both had a background for this topic so we gathered the information and helped each other in this matter we started to search in google scholar for verified scientific articles that help us, we changed the font to 12 Times new roman and sent the margin between lines to 1.0. Also we used Ethics book to gather information and and visited CITC and NCA to understand the policies forced by the government

1. Communication channel is secure for secure communication of the data

There are three most crucial component of security that organization use to guide policies for information security called CIA triad

A. Confidentiality stands for a set of rules that limits access to specific information; it's equivalent to privacy. Ensuring confidentiality means only appropriate people can access sensitive data.

B. Integrity stands for assurance that the information is trustworthy, accurate and unauthorized people can not change data.

C. Availability stands for the grantee of reliable access to data. It is crucial that access channels, authentication mechanisms, and systems all work properly for the information they protect and ensure its availability when needed

there are some methods we used to provide a good CIA in our app :

- **Data encryption :**

Encryption is a way to protect data that is sent from user to the server and from one server to another. It helped us meet company regulations. organisations that handle data countain customers accounts information, cardholder data and transactions should have strict regulations and compliance guidelines.

- **Transport layer security (TLS) :**

It is a protocol that uses encryption to ensure integrity and privacy for data communication through dependable end-to-end secure connection between any two sources within the network.

- **firewall :**

Is designed to filter, prevent unauthorized access and protect data against any attacks that aim to steal our users' information such as bank accounts and credit cards. it lies between a private internal network and the public internet as a whole to detect and combat attacks on the network seamlessly and quickly.

- **Proxy server:**

Is a system we used that serves as a bridge between user and internet to protect user devices from malware and other threats. it is a layer between end user and any browser the user visits online, and help user to keep the digital address hidden from hackers

we use proxy server to :

- Increase security. without proxy hackers can easily obtain the IP address and use it to penetrate the network.
- Protect user’s data from being spied on

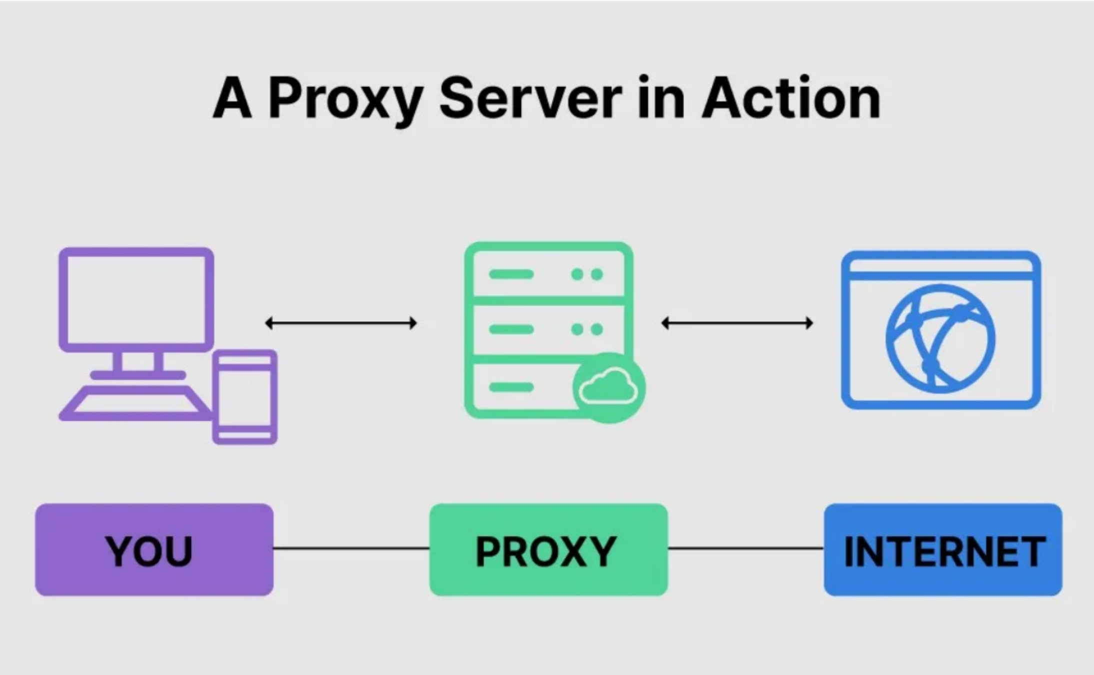
- Balance internet traffic to avoid problems

2. User authentication is secure enough to stop unauthorized login attempts

Authentication is ensuring that users are who they claim to be. When a person seeks to access a network or an application, they provide their identity via a username, then the system checks and compares the username to a list of authorized users to confirm that they have permission to enter.

There is many approaches for authentication (password, two factors authentications, tokens, biometrics, transaction authentications, computer recognition, CAPATCHAs, and sign-on)
we use authentication in three layers :
1 - Network level
2 - Application level
3 - End user level
and here is some methods we implemented to guarantee a strong authentication system :

1) **Password Authentication :**
The simplest type of authentication, when a user enters the username they must enter a secret code to obtain access to the network.



2) **Two-Factor Authentication :**
This relies on passwords to provide a far more powerful security solution. To obtain access to a network, a user must have both a password and a specific physical item (something you know and something you have). In order to login after entering the password and username, the user must first overcome an extra barrier : the user must enter a one time code from a specific device.
Codes may be provided via text messages, or phone calls. When a hacker guesses the password, it is impossible to proceed without the user's cell phone. so we implemented this method because our app contains sensitive data such as banking, health records and education history. we improved the security by this method.
3) **Biometric Authentication :**

Identification relies on a user's physical characteristics. This system commonly uses fingerprints, retinal or iris scans, voice recognition, and face recognition. Biometric authentication is particularly safe since no two users have the same physical characteristics. so we prefer using biometric because :

- You can get access rapidly.
- Stealing a biometric identification like a fingerprint or an iris scan is extremely tough.
- They are permanent because they do not change throughout time.

4) CAPTCHAs :

This authentication focuses on determining whether or not a user is human. CAPTCHA stands for “completely automated public Turing test to tell computers and humans apart.” we made sure that we apply and use CAPTCHA in our app because :

- Increases network security by adding another layer of defense against automated hacking systems.
- Stops bots from creating bogus accounts by flooding the registration system.
- Stop spamming blogs and news content pages with questionable comments and links to other websites.

Our Password Policies :

- A minimum of sixteen **16** characters.
- Not based on something that someone else may readily assume or figure out based on personal information **e.g.**, phone number and names.
- Passwords must never be shared with another individual for any reason or in any manner not consistent with this policy.
- Passwords must be different from those used for other personal services and must be unique.
- Passwords need to be updated on a frequent basis

3. Privacy of users is not compromised

a) **Educational records**

In our app we provided **Family Educational Rights and Privacy Act** , due to including all educational information of the children in a family and linking these information to their parents it includes:

- Access all grades for previous years
- Madrasati access to monitor
- Children’s educational status
- Teachers direct communication with student’s parents

Moreover, we provided **Information Privacy** as well due to the communication between teachers and parents so we secured it and protected the data so no one is accessing nor monitoring the conversation.

b) **Financial data**

Here we adapted **Right to Financial Privacy Act** because there is a section in our app for all financial features like transfers,SADAD,investments and requesting a loan.

Also Gramm-Leach-Bliley Act which consists of

- Financial privacy rule to protect personal financial data
- Citizens can refuse to give banks the right to share their financial data
- Safeguards rule is to document a plan for protecting personal data

However, we allowed the citizens to obtain a free credit report from their own bank to check if there is anything unusual by **Fair and Accurate Credit Transactions Act**.

c) **Medical history**

This section in the app is the most important and developed section since COVID-19.Actually, our app idea came up after the pandemic so in order to insure the safety of our citizens we released KSAi and TABAUD. KSAi have **Health Insurance Portability and Accountability Act** due to :

- Communicating with a doctor for consultations
- Checking health insurance coverage
- Booking appointments
- Ordering medications
- Calling an ambulance in emergencies

d) **Driving record**

For citizens safety we have speed detection for vehicles known as SAHER which takes a photo and then asks for the owner (of the car) to record the speed violation with **Traffic Device Vehicle Tracking System** and **Traffic Recognition System** for the citizens database from the Ministry of Interior and Ministry of Transportation. In order to protect vehicles in accidents we provided a **Vehicle Event Data Recorder** to use the photage during the accident in court of law our app includes :

- Car rental for those who wish to rent
- Payment of traffic fines
- Requesting a new car warranty
- Checking Car insurance
- List of traffic violations
- A digital copy of the Diving License.

4. All-in-one-app follows the relevant CITC and Saudi NCA policies

- **Cloud Services**

Before we include a cloud computing system we must have a license based on factors like the handling of sensitive data,the size of commercial presence in KSA and the nature of the services offered. We also must include a guidelines :

1. Guidance on what to benefit from this service and the appropriate license
2. Description of the requirements for obtaining one
3. An overview of practical implications

Therefore, we requested these service providers to obtain CSL, identify a good cloud service and be in contact with CITC to ensure that these service providers are committed to work.

- **Information Security**

Developing an app means that you hold a lot of personal data so we must protect and secure it so no third party can access citizens information due to the fact that our app holds level 4 in classification of user content and it is meant to be for highly sensitive user content belonging for governmental use.

However, it is our obligation to ensure that every personal data,cloud users' data is restricted and used for legal issues only.

- **Strategy Document**

We must contain a good defined strategy, it should be approved , maintained ,perfectly executed and aligned with our whole organization.

Also, regularly checked in compliance.

Moreover, it must address the importance of cyber security,anticipated future state and when cyber initiatives should be executed to achieve future state.

- **Implementing Framework**

Nowadays digital society has high expectations of continuous availability of services,protection of sensitive data and a flawless customer experience. These services are becoming important to all industries.

However, the need to safeguard sensitive data is a must especially in health,education and finance so we have to establish a Cyber Security Framework held by SAMA to enable Financial Institutions to identify risks related to cyber and help citizens in reducing fraud and theft
Framework objectives are :

1. Create a common approach for addressing cyber security
2. Achieve an appropriate maturity level of cyber security controls
3. Ensure cyber security risks are properly managed throughout the organization

These objectives will be used to periodically assess the maturity level and evaluate the cyber security controls at one's organization and compare it with other organizations. Framework is based on SAMA standards such as PCL,BASEL,ISO,ISF and NIST.

5. Relevant intellectual property rights are not violated

1. **Trade secret**

Most companies decide to have **Non-Disclosure clause** to prohibit the employees from revealing company's secret, without further due we also had to include it to make sure none of our employees is going to share nor expose citizens data or incidents inside the company

2. **Copyright**

3. **Patent**

Committing to granting a property right permits us to be excluded from copying our invention. A lot of countries don't have an app for their citizens that has all the services in one. So, for the app we applied to grant a patent. Moreover, to make sure your app idea isn't going to be stole and created you must apply for one.Mostly it encourages business owners to keep their ideas under protection by a Software Patent.

4. **Trademarks**

We applied to have our own logo so citizens can tell the difference between government app and other company's and for that we obtained a trademark from USPTO for a fair use.

REFERENCES

References

- Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security, 10*(3)

- Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. *Vol, 5*, 246-249.