RAMAIAH UNIVERSITY
OF APPLIED SCIENCES

ASSIGNMENT - 1

Course Code	19CSC315A
Course Name	Information Security and Protection
Programme	B. Tech
Department	Computer Science and Engineering
Faculty	FET

Name of the Student	K Srikanth
Reg. No	17ETCS002124
Semester/Year	3rd /6th Semester
Course Leader/s	Prof. N. D. Gangadhar

Declaration Sheet			
Student Name	K Srikanth		
Reg. No	17ETSC002124		
Programme	B. Tech	Semester/Year	3rd /6th Semester
Course Code	19CSC315A		
Course Title	Information Security and Protection		
Course Date	18/03/2021	to	04/07/2021
Course Leader	Prof. N. D. Gangadhar		

Declaration

The assignment submitted herewith is a result of my own investigations and that I have conformed to the guidelines against plagiarism as laid out in the Student Handbook. All sections of the text and results, which have been obtained from other sources, are fully referenced. I understand that cheating and plagiarism constitute a breach of University regulations and will be dealt with accordingly.

Signature of the Student	**K Srikanth**	Date	**3/05/2021**
Submission date stamp (by Examination & Assessment Section)			

Signature of the Course Leader and date	Signature of the Reviewer and date

Faculty of Engineering and Technology			
Ramaiah University of Applied Sciences			
Department	Computer Science and Engineering	Programme	B. Tech. in CSE
Semester/Batch	6/2018		
Course Code	19CSC315A	Course Title	Information Security and Protection
Course Leader	Prof. N. D. Gangadhar / Dr. Vaishali R. Kulkarni / Dr. Suvidha K. V.		

Assignment-01			
Reg.No.	**17ETCS002124**	**Name of Student**	**K Srikanth**

Marking Scheme		**Marks**		
			First Examiner Marks	**Moderator**
1	Identification of the assets to be protected and actors involved	**3**		
2	Design of the specific Confidentiality, Integrity and Availability security services required for the assets	**4**		
3	Analysis of the threats to the system based on the determined security requirements	**4**		
4	Recommending specific security policies to counter the threats and attempt a synthesis of them into an overarching policy	**4**		

5	Identify specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks	**4**		
6	Discussion on the assumptions and role of trust in the recommendations	**3**		
7	Discussion of the role of law and University Regulations	**3**		
	Part-A Max Marks	**25**		

Course Marks Tabulation				
Assignment	**First Examiner**	**Remarks**	**Moderator**	**Remarks**
1				
Marks (out of 25)				

Please note:

1. Documental evidence for all the components/parts of the assessment such as the reports, photographs, laboratory exam / tool tests are required to be attached to the assignment report in a proper order.
2. The First Examiner is required to mark the comments in RED ink and the Second Examiner’s comments should be in GREEN ink.
3. The marks for all the questions of the assignment have to be written only in the **Component – CET B: Assignment** table.
4. If the variation between the marks awarded by the first examiner and the second examiner lies within +/- 3 marks, then the marks allotted by the first examiner is considered to be final. If the variation is more than +/- 3 marks, then both the examiners should resolve the issue in consultation with the Chairman BoE.

Name: K Srikanth Registration Number: 17ETCS002124

Assignment 1

Instructions to students:

1. Maximum marks is **25**.
2. The assignment has to be neatly word processed as per the prescribed format.
3. The maximum number of pages should be restricted to 1**0**.
4. The printed assignment must be submitted to the course leader.
5. **Submission Date: 3rd May 2021**
6. **Submission after the due date is not permitted.**
7. **IMPORTANT**: It is essential that all the sources used in preparation of the assignment must be suitably referenced in the text.
8. Marks will be awarded only to the sections and subsections clearly indicated as per the problem statement/exercise/question

Preamble

This course is aimed at preparing the students to understand, design, analyse, implement and integrate security provisions in an IT environment. Students are taught elements of information security, known attacks and counter measures. The module also introduces the students to IT policies, auditing and standards that enable them to understand and provide information security assurance. Scenario based case studies are employed. Students are trained to analyse a given scenario and propose security measures and policies and develop an analytical report documenting their effort.

Security and Protection of Examination Section on RUAS Portal

RUAS Portal has several overlapping operational sections. One set of functionalities of the portal covers the operation and information flow involving data and information related to the Examinations and Assessment of students. Data and information related to question papers, answer scripts, student reports and presentations, attendance records, time tables, marks sheets and certificates are handled by the section. Owing to the sensitive and confidential nature of the data and information, it is essential that it is well protected with security policies and mechanisms.

The student is required to perform an analysis of the information system along the following lines:

1. Identify the assets to be protected and actors involved

Let’s find out the assets that would help us build this System,

- **Question Papers**
- **Answer Scripts**
- **Student Reports and Presentations**
- **Attendance Records**
- **Time Tables**
- **Marks Sheets**
- **Certificates**

Now let’s look at the Actors who are going to interact with these assets on a daily basis or occasionally as well,

Starting off with,

1. **System Admin**

This Actor would be the one who is going to interact with the system on the daily basis to monitor the system whether its functioning as expected or not as if it fails to satisfy the expected functioning then it would be catastrophic

2. **Faculty**

Faculty would the second actor according to the hierarchy who would also be using it on the daily basis to update the student details (attendance) and conduct examinations and also examining the answer scripts these actor can be divided into 3 Sub-categories

a. **Officers and Organisation**

These are specific group of actors who stand high on the given hierarchy level (such as Chancellor, Vice - Chancellor and followed by Dean and continued. These actors have the supreme access to the entire portal whenever need be.

b. **Teaching Staff**

These actors are the next to the higher hierarchy level as they would continue to monitor the **student progress** and make **question papers and examining the answer scripts and student reports**. This class can be sub divided into two actor categories,

i. Professors

These Actors would be the people who would be mostly monitoring the student progress and make question papers and examining the answer scripts and student reports as well as taking attendance

ii. Tutors

These are the next level of actors in the hierarchy level after professors who manage all the time tables and records of the student

c. **Non-Teaching Staff**

These actors are the last level in hierarchy where they would mostly work on organising everything above such as attendees in examination department.

3. **Students (End Users)**

These actors are the end users who can view and do some certain tasks in the system with its given policies.

2. Determine the specific Confidentiality, Integrity and Availability security services required for the assets

Now let's discuss on the specific Confidentiality, Integrity and Availability security services for our assets discussed from Question 1,

1. **Question Papers**

The one of prime asset from our system is the **Question Papers** as it contains sensitive information until the time when exam is held . When it comes to CIA (Confidentiality, Integrity and Availability) for this asset

<u>**Confidentiality Requirements**:</u> This asset should only be visible to **Officers and Organisation**

(**Actors 2a) and Professors (Actor 2b(i))** as they would be the actors who would be interacting with it but the question paper is only set by actors from **2b(i)** as it should be visible until the exam time. After then time expires then this information can be visible to the **Student (Actor 3)** if they are subscribed to that channel (i.e. That Particular Class) and also if they are registered to that exam then they can also be subscribed.

Integrity Requirements: This Asset can only be able to be modified by the actor **2b(i)** with respect to their course as they have full access to modify this asset.

Availability Requirements: This asset should be available when the exam starts as students who are subscribed to the particular channel can be able to download and start writing the exam.

2. **Answer Scripts**

   The next prime asset from our system is the **Answer Scripts** as it contains sensitive information until the time results or graded. When it comes to CIA (Confidentiality, Integrity and Availability) for this asset,

   Confidentiality Requirements: This asset should only be visible to **Officers and Organisation** (**Actors 2a) and Professors (Actor 2b(i))** as they would be the actors who would be interacting with it but the **Answer Scripts** are only graded by actors from **2b(i)**. After then the graded marks are passed on to the Examination Department who are **Actors (2c)** as they can upload the marks to the Portal later on.

   Integrity Requirements: This Asset can only be able to be graded by the actor **2b(i)** with respect to their course as they cannot be able to tamper the information but other than grade it.

   Availability Requirements: This asset should be available when the actors of **(2b(i)) request** to download the answer scripts from the portal after the exam is held with respect to their course.

3. **Student Reports and Presentations**

   The next prime asset from our system is the **Student Reports and Presentations** as it contains sensitive information until the time they are graded or announced. When it comes to CIA (Confidentiality, Integrity and Availability) for this asset,

   Confidentiality Requirements: This asset should only be visible to **Officers and Organisation** (**Actors 2a) and Professors (Actor 2b(i))** as they would be the actors who would be interacting with it but the **Student Reports and Presentations** are only graded by actors from **2b(i)**. After then the graded marks are passed on to the Examination Department who are **Actors (2c)** as they can upload the marks to the Portal later on.

Integrity Requirements: This Asset can only be able to be graded by the actor **2b(i)** with respect to their course as they cannot be able to tamper the information but other than grade it.

Availability Requirements: This asset should be available when the actors of **(2b(i)) request** to download the **Student Reports and Presentations** from the portal after students submit their **Reports and Presentations** with respect to their course.

4. Attendance Records

The next prime asset from our system is the **Attendance Records** as it contains information that cannot be tampered until the end of the semester. When it comes to CIA (Confidentiality, Integrity and Availability) for this asset,

Confidentiality Requirements: This asset should only be visible to **Officers and Organisation** (**Actors 2a) and Professors (Actor 2b(i))** as they would be the actors who would be interacting with it but the **Attendance** are only marked by actors from **2b(i)**. After then the finalised at the end of the semester they are passed on to the Examination Department who are **Actors (2c)** as they can upload the attendance to the Portal later on.

Integrity Requirements: This Asset can only be able to be marked by the actor **2b(i)** with respect to their course as they cannot be able to tamper the information but other than mark the attendance.

Availability Requirements: This asset should be available when the actors of Students **(3) request** to download the **Attendance Records** from the portal after **Professors (2b(i))** finalised at the end of the semester with respect to their course and are uploaded.

5. **Time Tables**

The next prime asset from our system is the **Time Tables** as it contains information that cannot be tampered without certain access to them until the end of the semester. When it comes to CIA (Confidentiality, Integrity and Availability) for this asset,

Confidentiality Requirements: This asset can be visible to **all the actors** as but can only be modified or created by the **Actors (2c) and 2b(ii)** . After then the finalised **Time Table** is verified by actors **(2b(i))** before publishing it or making it visible to everyone after that they are passed on to the Concerned Department who are **Actors (2c)** as they can upload the **Time Table** to the Portal later on.

Integrity Requirements: This Asset can only be able to be tampered or modified by the **Actors (2c) and 2b(ii)** with respect to their department .

Availability Requirements: This asset should be available to all the actors when they **request** to download the **Time Table** from the portal after **Actors (2c) and 2b(ii)** finalised at the beginning of the semester with respect to their Department and are uploaded.

6. **Marks Sheets**

The next prime asset from our system is the **Marks Sheets** as it contains information that cannot be tampered. When it comes to CIA (Confidentiality, Integrity and Availability) for this asset,

Confidentiality Requirements: This asset should only be visible to **Officers and Organisation** (**Actor 2a), Professors (Actor 2b(i)) and Actors (2c)** as they would be the actors who would be interacting with it but the **Marks** are only marked by actors from **2b(i)**. After then the finalised marks at the end of the semester are passed on to the Examination Department who are **Actors (2c)** as they can upload the attendance to the Portal later on. After they are finalised by them and later can be visible **to Actors (3)** after results are announced**.**

Integrity Requirements: This Asset can only be able to be marked by the **Actor 2b(i)** with respect to their course as they cannot be able to tamper the information but other than grade then student and **Actor (2c)** can put together an mark sheet with all the course marks combined which student has subscribed to.

Availability Requirements: This asset should be available when the actors of Students **(3) request** to download the **Marks Sheet** from the portal after **Professors (2b(i)) and Actor (2c)** upload the sheet when the results are announced with respect to student course.

7. **Certificates**

The next prime asset from our system is the **Certificates** as it contains information that cannot be tampered. When it comes to CIA (Confidentiality, Integrity and Availability) for this asset,

Confidentiality Requirements This asset should only be visible to **Officers and Organisation** (**Actor 2a), Professors (Actor 2b(i)) and Actors (2c)** as they would be the actors who would be interacting with it but the Certificates are only produced by actors from **2b(i) when verified with students achievement** . After then the finalised student achievement are passed on to the Concerned Department who are **Actors (2c)** as they can generate certificate and upload to the Portal.

Integrity Requirements: This Asset can only be able to be verified and certified by the Actor **2b(i)** with respect to students achievement as they cannot be able to tamper the information but other than verify and certify the achievement.

Availability Requirements: This asset should be available when the actors of Students **(3) request** to download the **Certificates** from the portal after being verified by the **actors (2b(i)) and uploaded by actors (2c).**

3. Analyse the threats to the system based on the determined security requirements.

a. Clearance Breaches

These are one of the potential threats that can collapse the main intention of system when it is not structed properly. As we have divided that each actor will have a different role when it comes to interacting with the portal. Let's take a scenario to see how this can be a threat,

Scenario

In this scenario let's assume that **Actor (2b(i)) has Clearance level "2" and Actor (3) has Clearance level "3".** Now, as we discussed that **Actor (2b(i))** can perform certain tasks and **Actor (3)** as well, now **Actor (2b(i))** has made a question paper prior to the exam data and has upload it and will only be visible to **Actor (2b(i)) and Actor (2a)** and no one else and even **Actor(1)** who is administrating the system as well because the question paper should be encrypted and cannot be visible until the exam date. Now, let's say that there was a clearance breach where the person who is not supposed to access the question paper has attempted to access the paper and his **clearance level is "3"** so this is considered to be a breach in the clearance level and if the person who was accessing it was clearly unauthorized and this could be considered as threat to the system's integrity.

b. Malware

This is the most common threat out there when you system is running perfectly fine and all of the sudden you system is attacked by malware if not maintained or structed properly while designing the system's security. Let's take a scenario to see how this can be a threat,

Scenario

In this scenario let's assume that our **system (Portal)** was running perfectly alright and all of the sudden all the **services started to decline** to give service to users and system admin is trying to figure out what is happening but he won't be able to see that there was a malware which was **injected into the system by someone (hacker**) which is making the system integrity declining as

the time ticks, now what happens is that it can be a threat to the data and confidentially of the system as **the malware is spreading throughout the system progressively** and this might even affect the end users system when user is trying to access the portal, and might enter the users system as well if not protected as **this threat can be brutal if the users and system's data** is **compromised or modified.**

c. Data Breaches

This is also the most common threat that the systems are challenged to face every day, this breach happens when someone tries to access the data without proper clearance level who is unauthorized to perform this actions related to data in the system. Let's take a scenario to see how this can be a threat,

<u>Scenario</u>

In this scenario let's assume that **Actor (2b(i)) has Clearance level "2" and Actor (3) has Clearance level "3".** Now, as we discussed that **Actor (2b(i))** can perform certain tasks and **Actor (3)** as well, now **Actor (2b(i))** has updated the marks of the student after the student submitting their answer scripts and let's say that the results are announced and everyone can see their marks according to their course now **Actors with Clearance level "2" have Read and Write access to the data and Actors with Clearance level "3" have only Read Access to their data.** Now, let's assume that there a breach when actor with **Clearance level "3"** has accessed the data to overwrite the data which is been already written then this scenario would be called as a data breach where the **Actor with Clearance level "3" was unauthorized to write the data in to system** and this could be considered as threat to the system's integrity**.**

d. Denial Attacks

This is also the most common threat that the systems are challenged to face every day, this threat happens when someone is denied service from the system when requested. Let's take a scenario to see how this can be a threat,

Scenario

In this scenario there are multiple types of **Denials Attacks** most common of them are

1. Denial of Service

2. Denials of Receipt

3. Distributed Denial of Service

Let's take all the types of **Denials Attacks** as the part of the scenarios, Let's take **Denial of Service** Where the system doesn't respond to what the user has requested and it denies to give the response for example the **user has requested to view his results** when they are announced and then the **system responds** with **saying that you cannot see the results yet** as this would be a denial attack made but the **system**. The other type of **Denials Attacks is "Denials of Receipt"** this happens when they user has received the data they requested by them and deny that they haven't got the response yet even though they have received it as this would be a denial attack made but the **user.** The Third type of **Denials Attack is "Distributed Denial of Service Attack"** where the user keeps on requesting the server in a large scale to a particular resource or an service which system provides and this would cause the system to not respond and also might crash as it doesn't have that potential to handle large number of requests if it exceeds it threshold. All of the above types of this **Denials Attacks** could be considered as threat to the system's integrity

e. Phishing

This is also the most common threat that the systems are challenged to face every day, this breach happens when someone tries to access the system pretending to be you with your credentials as they were leaked or maybe be taken from you. Let's take a scenario to see how this can be a threat,

Scenario

In this scenario let's assume that you have a **Clearance level "2"** who can perform all the tasks that require confidently of the takes that you perform. Now let's say that you received some kind of **an e-mail or a message** asking to you **to login in to your account** to perform some task which **was fake-ly assigned to you by a hacker** and now you login into the fake website that you have received along with your **e-mail and now that you have logged in to the fake website** that looks similar to the one that you use daily **except the point that it was made by the hacker** which looks similar. Now, the **Hacker has your credentials and can login** to the actual portal and pretend to be you and **can perform all actions** that the actor with **Clearance level "2" can do.** This is the Major threat to the system as it can as threat to **the system's and data's integrity.**

4. Recommend specific security policies to counter the threats and attempt a synthesis of them into an overarching policy.

Let's look the security policies to counter the threats with respect to our assets,

1. Question Paper

a. Clearance Breaches

Accessing the questions paper before actually being visible to student on the exam data is a clearance threat to the system only some have the clearance level to access the question paper before the exam and no one else. So to counter this threat we can setup an token access and verify if the user is valid or not via a gateway if the user is unauthorized then they can't access the data.

b. Malware

We can keep our system malware free by updating the system time to time using an external software to look out for any threat that would compromise the system.

c. Data Breaches

Accessing the Question Paper without the proper clearance level is a threat to the system only some have the clearance level to access the some types of data like modify the data and no one else. So to counter this threat we can setup an encryption technique where we would verify the private key right after the user is cleared through the gateway. (Only if the user is certified to access to the data) else we kick the user out.

d. Denial Attacks

i) Denial of Service

Accessing the Question Paper download service cannot be overridden by anyone except the System Administrator.

ii) Denials of Receipt

We can a keep a download log whenever a student downloads the question paper and add it to logs database so that the user cannot say that he didn't receive the data

iii) Distributed Denial of Service

We can make a custom DDoS Attack Service which can take care of this threat. If the Attack happened then it would notify the concerned team.

e. Phishing

We can setup an token access and verify if the user is valid or not via a gateway if the user is unauthorized then they can't access the data.

2. Answer Scripts

a. Clearance Breaches

Accessing the Answer Scripts and performing actions on them is possible by only some of the actors if accessed by anyone else that would be a breach, So to counter this threat we can setup an token access and verify if the user is valid or not via a gate if the user is unauthorized then they can't access the data via their clearance level.

b. Malware

We can keep our system malware free by updating the system time to time using an external software to look out for any threat that would compromise the system.

c. Data Breaches

Accessing the Answer Scripts without the proper clearance level is a threat to the system only some have the clearance level to access the some types of data like modify the data and no one else. So to counter this threat we can setup an encryption technique where we would verify the private key right after the user is cleared through the gateway. (Only if the user is certified to access to the data) else we kick the user out.

d. Denial Attacks

i) Denial of Service

Only the actor who is responsible for that course is supposed to download the answer scripts and this functionality cannot be over written unless until system administrator does it.

ii) Denials of Receipt

We can a keep a download log whenever a faculty downloads the answer script and add it to logs database so that the user cannot say that he didn't receive the data.

iii) Distributed Denial of Service

We can make a custom DDoS Attack Service which can take care of this threat. If the Attack happened then it would notify the concerned team.

e. **Phishing**

We can setup an token access and verify if the user is valid or not via a gateway if the user is unauthorized then they can't access the data.

3. Student Reports and Presentations

a. **Clearance Breaches**

Accessing the Student Reports and Presentations and performing actions on them is possible by only some of the actors if accessed by anyone else that would be a breach, So to counter this threat we can setup an token access and verify if the user is valid or not via a gate if the user is unauthorized then they can't access the data via their clearance level.

b. **Malware**

We can keep our system malware free by updating the system time to time using an external software to look out for any threat that would compromise the system.

c. **Data Breaches**

Accessing the Student Reports and Presentations without the proper clearance level is a threat to the system only some have the clearance level to access the some types of data like modify the data and no one else. So to counter this threat we can setup an encryption technique where we would verify the private key right after the user is cleared through the gateway. (Only if the user is certified to access to the data) else we kick the user out.

d. **Denial Attacks**

i) Denial of Service

Only the actor who is responsible for that course is supposed to download the Student Reports and Presentations and this functionality cannot be over written unless until system administrator does it.

ii) Denials of Receipt

We can a keep a download log whenever a faculty downloads the Student Reports and Presentations and add it to logs database so that the user cannot say that he didn't receive the data.

iii) Distributed Denial of Service

We can make a custom DDoS Attack Service which can take care of this threat. If the Attack happened then it would notify the concerned team.

e. Phishing

We can setup an token access and verify if the user is valid or not via a gateway if the user is unauthorized then they can't access the data.

4. Attendance Records

a. Clearance Breaches

Accessing the Attendance Records and performing actions on them is possible by only some of the actors if accessed by anyone else that would be a breach, So to counter this threat we can setup an token access and verify if the user is valid or not via a gate if the user is unauthorized then they can't access the data via their clearance level.

b. Malware

We can keep our system malware free by updating the system time to time using an external software to look out for any threat that would compromise the system.

c. Data Breaches

Accessing the Attendance Records without the proper clearance level is a threat to the system only some have the clearance level to access the some types of data like modify the data and no one else. So to counter this threat we can setup an encryption technique where we would verify the private key right after the user is cleared through the gateway. (Only if the user is certified to access to the data) else we kick the user out.

d. Denial Attacks

i) Denial of Service

Only the actor who is responsible for that course is supposed to upload the attendance and Student should be able to view it cannot write as this functionality cannot be over written unless until system administrator does it.

ii) Denials of Receipt

We can a keep a download log whenever a faculty has seen the attendance can be added it to logs database so that the user cannot say that he didn't receive the data.

iii) Distributed Denial of Service

We can make a custom DDoS Attack Service which can take care of this threat. If the Attack happened then it would notify the concerned team.

e. Phishing

We can setup an token access and verify if the user is valid or not via a gateway if the user is unauthorized then they can't access the data.

5. Time Tables

a. Clearance Breaches

Accessing the Time Tables and performing actions on them is possible by only some of the actors if accessed by anyone else that would be a breach, So to counter this threat we can setup an token access and verify if the user is valid or not via a gate if the user is unauthorized then they can't access the data via their clearance level.

b. Malware

We can keep our system malware free by updating the system time to time using an external software to look out for any threat that would compromise the system.

c. Data Breaches

Accessing the Time Tables without the proper clearance level is a threat to the system only some have the clearance level to access the some types of data like modify the data and no one else. So to counter this threat we can setup an encryption technique where we would verify the private key right after the user is cleared through the gateway. (Only if the user is certified to access to the data) else we kick the user out.

d. Denial Attacks

i) Denial of Service

Only the actor who is responsible for that course is supposed to upload the Time Table and Student should be able to view it cannot write as this functionality cannot be over written unless until system administrator does it.

ii) Denials of Receipt

We can a keep a download log whenever a faculty has seen the Time Table can be added it to logs database so that the user cannot say that he didn't receive the data.

iii) Distributed Denial of Service

We can make a custom DDoS Attack Service which can take care of this threat. If the Attack happened then it would notify the concerned team.

e. Phishing

We can setup an token access and verify if the user is valid or not via a gateway if the user is unauthorized then they can't access the data.

5. Determine specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks.

Now all the methods we discussed in the above question. Now let's look at how we can implement them into our system,

1. Clearance Mechanism

This is the one prime mechanism that is needed to verify if the user is valid or not as if this not verified then the user cannot perform any tasks with his/her account. So the Authentication and Authorization technique we will be using to provide this service is **OAuth** which helps the actors to grant access to their service with a token and it is verified every time the User is logged in. if the produced token is not valid then the user is kicked out of the system. Prompting Unauthorized access

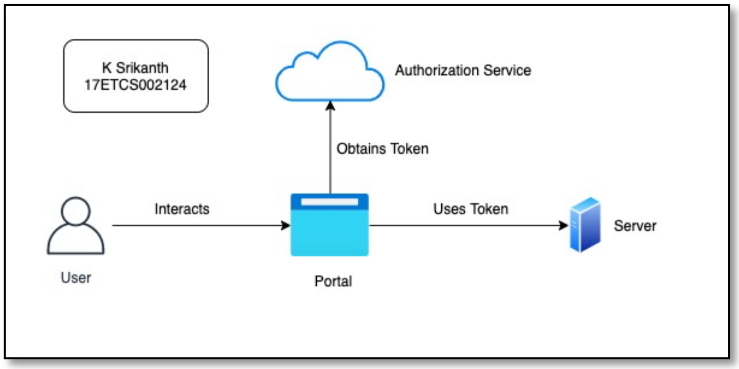

Figure 1 Authorization Service Flowchart

2. Malware Protection Mechanism

This is the next Mechanism that we have to take care of, what can be done to prevent this from happening is we can,

1. Restrict administrative rights

Limit the ability of actors to have access to the data to which they do not have access to reducing theses privileges will help to reduce the attacks significantly.

2. Keep your systems up to date

Having the latest security software, operating systems and web browsers are your best defence against viruses, malware and other online threats. It is best to turn on automatic updates, so you install the latest fixes as soon as they become available.

3. Back up

The best defence against ransomware is to not be vulnerable to their threats in the first place. This means that our portals need to back up their critical data daily. In the event your computers or servers get locked, you would not be forced to pay for access to your data.

3. Data Encryption Mechanism

To Protect our data we can use this use an encryption mechanism where we can protect our data which includes all the assets and let only certain actors perform operations on them. The encryption technique we can use is, **AES (Advanced Encryption Standard)** which uses **symmetric encryption algorithm** which can resist a **brute-force attack.** So, AES includes three block ciphers **AES-128, AES-192 and AES-256 AES-128 uses a 128-bit key length** to encrypt and decrypt a block of messages, whereas AES-192 uses a **192-bit key length** and **AES-256 uses a 256-bit key length** to encrypt and decrypt messages. There are **10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys**. A round consists of several processing steps that include **substitution, transposition and mixing of the input plaintext to transform it into the final output of ciphertext.**

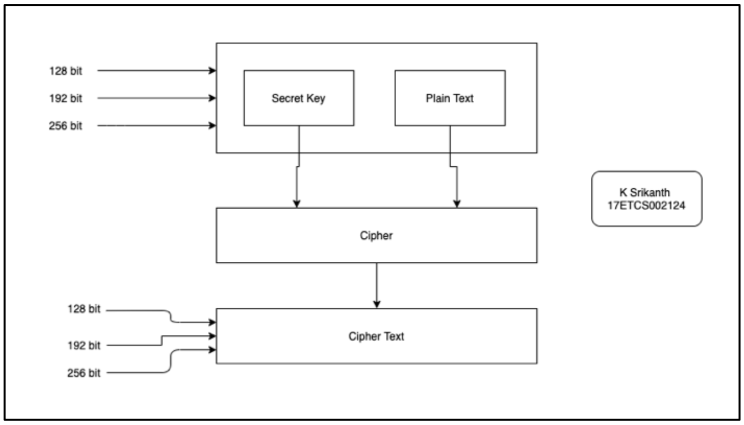

Figure 2 Flowchart of AES Algorithm for Encryption

4. Denial of Service Mechanism

In order to develop a DDoS prevention mechanism based on our college portal requirement we need to take the best steps to prevent this from happening as when DDoS hits, there is no time to think about anything. In order to develop such mechanism, we need some key elements to keep in mind while developing it,

a. **Systems Checklist :** Develop a full list of assets you should implement to ensure advanced threat identification, assessment, and filtering tools, as well as security-enhanced hardware and software-level protection, is in place.

b. **Response Team** : Define responsibilities for key team members to ensure organized reaction to the attack as it happens (which would be system administrator)

By considering some of these factors we can prevent DDoS from happening and our data would be safe as well

5. Phishing Prevention Mechanism

The last Mechanism is “Phishing Prevention Mechanism” were the hacker sends a mail or a link like a bait and then get your credentials and later they perform the same actions that you can perform with your account to avoid this we can add create a spam filter where the user can let these types of bait mails to a spam folder so that Phishing doesn’t happen.

6. Discuss the assumptions and role of trust in the recommendations.

The following assumptions are made to enforce policies by using mechanisms like authentication and authorization.

Assumptions:

All the communication between the user and system happens over secure http connection to make sure the data is encrypted throughout the process. This is important to make sure the data is not understood even if somebody intercepts the connection.

The authentication system must be smart enough to warn the user about updating his credentials if it suspects something wrong. This could be too many failed attempts, abnormal login activities.

The system is capable of identifying Denial attacks in advance to ensure that there is no wastage in system resources. It is able to distinguish between load of Denial attacks and set of fast growing and valid incoming requests, so that it scales only on occurrence of latter situation.

The User did not publish his login credentials anywhere and the user who successfully logs in is trusted. User is smart enough to deal with spoofing.

The User can preserve confidentiality of the data by not sharing downloaded files to people who is not authorized to access them. It is assumed that assets are not modified by unauthorized personnel.

It is assumed that confidential assets like question paper will be made available to the students only after the scheduled time without any delay. If by chance there is any delay this should be properly logged to provide student with lost time in waiting for the paper.

It is assumed that assets like question paper reaches everyone at same time. So, there is no chance for intentional data leak.

It is assumed that printer personnel don’t share the assets when given to them for printing their hardcopies.

Trust:

Trust is evaluated according to the assumptions made.

Although https is more secure compared to http, it is still not entirely foolproof. Data can still be intercepted. It is hard to decrypt, but there are chances of that happening.

The users of the application are trusted thoroughly in this process as we assume that users well behave and strictly bound to their duties, at the same time maintain confidentiality of sensitive data. But we cannot promise that there will be no abuse of trust.

7. Discuss the role of law and University Regulations.

Every organization urges its associates to keep the sensitive information provided to them confidential and to follow their rules strictly.

All of the associates are bound to behave according to these rules, otherwise they are liable to face the consequences as decided by the council and if it is permitted by law. One of the common consequences could be termination from institution.

The University follows the absolute marking system and grades are awarded based on the marks. This evaluation follows the same pattern across the institution that is in accords with the legal bodies.

If any user found to be involved in misconduct or unfair means of practices followed. Legal actions are taken against them. Could be modification of academic records or our assets discussed earlier by unauthorized means.

In case, there are any mistakes found in any assets, the candidate can refer concerned authorities to make corrections.

All concerned are strongly urged to ensure their understanding of the Academic Regulations and time to time amendments. Consequences resulting out of failure to read and understand the Academic Regulations shall rest only with the individual concerned.