

**EVALUATION OF INTERNSHIP REPORT**

## B.Tech: III Year

**Department of Computer Science & Information Technology**

**Name of the Student – Jitendra Aakde**

**Branch & section - CSIT-2**

**Roll No - 0827CI201088**

**Year-2022-23**

## Department of Computer Science & Information Technology

**AITR, Indore,**

**ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**Certificate**

Certified that training work entitled “*Cyber Security*” is a bonafied work carried out after sixth semester by “Jitendra Aakde” in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from “*Prof. Nidhi Nigam (CEH certified)*” Acropolis Institute of Technology and Research during the academic year 2022-23.

*Name and Sign of Training Coordinator Name & Sign of Internship Coordinator*

**ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**ACKNOWLEDGEMENT**

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training coordinator, *Prof. Nidhi Nigam (CEH certified)* , CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him/her. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

*Name – Jitendra Aakde*

*Enrollment No. – 0827CI201088*

### ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

### INDEX

S.no CONTENTS Page no

1. Introduction to technology Undertaken…….... 1

2. Objectives ………..……………………………….... 3

3. Project undertaken ……………………….. 4

4. Screenshots of Project and Certificates……………………….. 11

5. Github Links (Project/certificate/video/copy of report.… ……. 12

7. Conclusion……….. ……………………………………. 16

8. References/ Bibilography………………………………..…………… 17

**Introduction to technology Undertaken**

**( Cyber Security)**

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

Some other definitions of cybersecurity are:

"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

Types of Cyber Security

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

Network Security: It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.

Application Security: It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.

Information or Data Security: It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.

Identity management: It deals with the procedure for determining the level of access that each individual has within an organization.

Operational Security: It involves processing and making decisions on handling and securing data assets.

Mobile Security: It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.

Cloud Security: It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.

Disaster Recovery and Business Continuity Planning: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

User Education: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event

**Objectives**

Cyber Security's main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

We can break the CIA model into three parts: Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.

1. Confidentiality

Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. Data encryption is an excellent example of ensuring confidentiality.

1. Integrity

This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

1. Availability

This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

**Project undertaken**

**(Encryption / Decryption of Images)**

Encryption cannot only be used on text, but also on images. There are numerous algorithms that you can use to encrypt the image. Some examples include AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest-Shamir-Adleman) which can be used to encrypt the image to protect it from a hacker. Even if the hacker gets access to the image over the internet, to decrypt it, the hacker first needs access to keys and then convert the image into the required format. In any case, the project gives a solid understanding and exhibits that you have a knack for cryptography. Also, the project is not too advanced and can be made if you’re beginning to dive into cybersecurity.

**Encryption**

It is nothing but a simple process in which we convert our data or information into secret code to prevent it from unauthorized access and keep it private and secure.

First, we will select an image, and then we will convert that image into a byte array due to which the image data will be totally converted into numeric form, and then we can easily apply the XOR operation to it. Now, whenever we will apply the XOR function on each value of the byte array then the data will be changed due to which we will be unable to access it. But we should remember one thing here our encryption key plays a very important role without that key we can not decrypt our image. It acts as a password to decrypt it.

**Decryption**

It is nothing but a process of converting our encrypted data into a readable form. Here we will again apply the same XOR operation on an encrypted image to decrypt it. But always remember that our encryption key and decryption key must be the same.

Step-1:- Whatever image we want to encrypt, we should know the name of that image as well as in which folder it is.

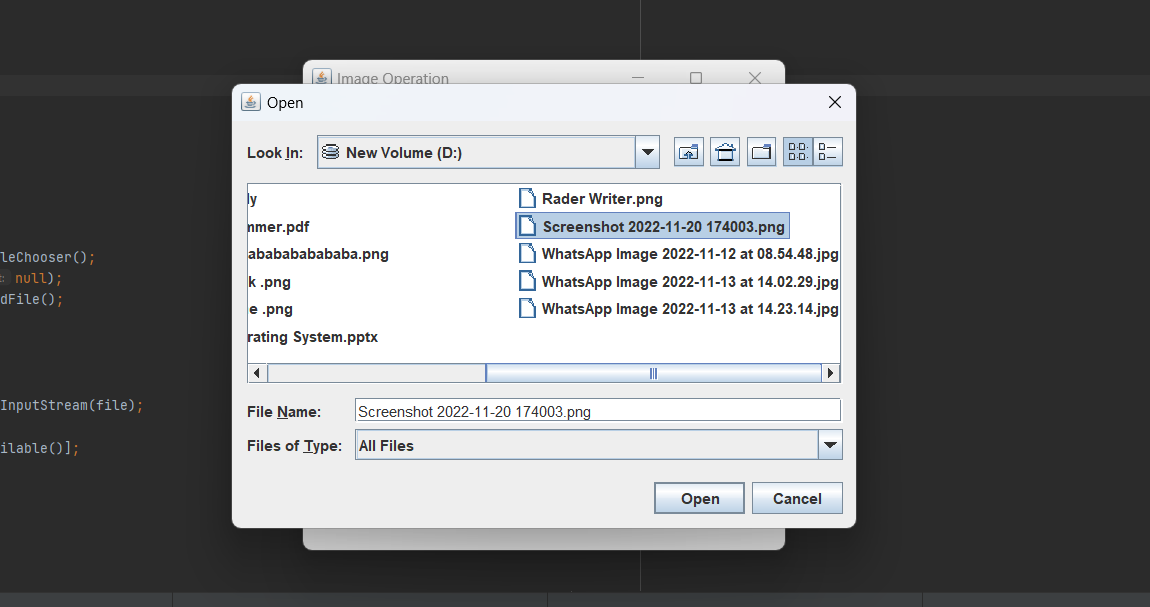
Step -2:- After which we have to run our code and first of all we have to enter a code through which the image will be encrypted, after entering the code we have to select that image as shown in the screenshot below, in this way any image will be encrypted.

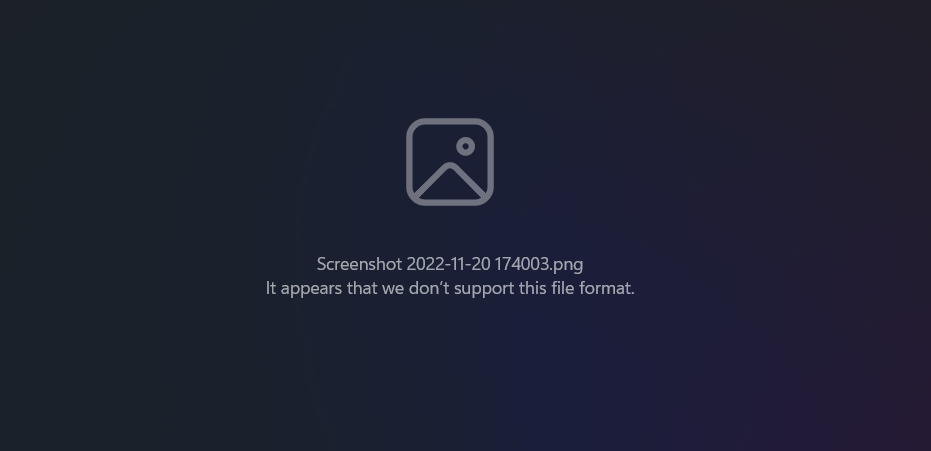
Step-3:- After which the image will be encrypted and no one can see it.

Step-4:- Now if we want to decrypt, we will have to repeat this process and enter the same decrypt code which was entered to encrypt.

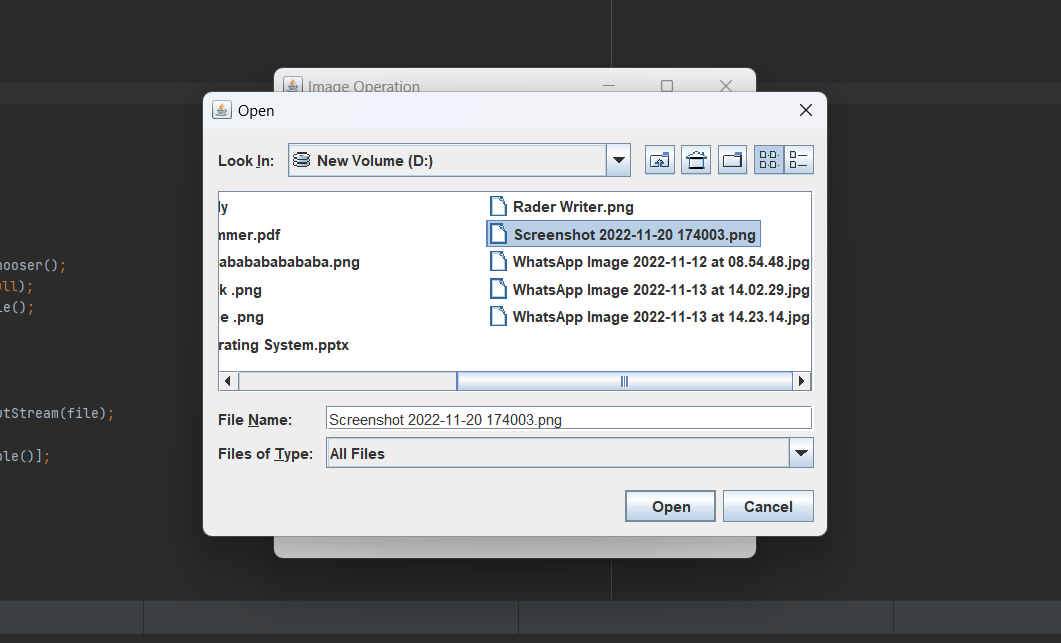
**Screenshots of Project and Certificates**

**Incryption:-**

****

****

**Decryption:-**

****

**Screenshot of certificate :-**

****

**Github Links (Project/certificate/video/copy of report)**

* **Project –** <https://github.com/jitendraaakde/EOI->
* **Certificate-** https://github.com/jitendraaakde/EOI-/blob/main/Jitendra%20Aakde%20(2).pdf
* **video-**
* **copy of report-**

**Conclusion**

As threats and protection measures continue to become more complex and sophisticated, it’s important for employers to find candidates with in-depth knowledge into cyber security and other highly relevant areas. In this way, while a bachelor’s degree may suffice for some types of cyber security careers, the most attractive candidates are those who hold master’s degrees.

Those interested in these or other types of cyber security careers can put themselves on the path to employment by obtaining a high-level degree. The Online Cybersecurity, Master of Science program at the University of Nevada at Reno provides students with the skills, experience and expertise they need to pursue an array of exciting and high-compensating cyber security careers.

**References**

[**https://google.com/**](https://google.com/)

[**www.youtube.com**](http://www.youtube.com)