K.G.C.E.
Karjat - Raigad

Assignment No-1

Page No. :

Date :

Name:- Bhavesh S Panchal

Roll no- 42.

Branch: I.T

Year - B.E.

	DOA	DOP	Remark	Sign.

K.G.C.E.
Karjat - Raigad

Assignment No 1

Page No. :
Date :

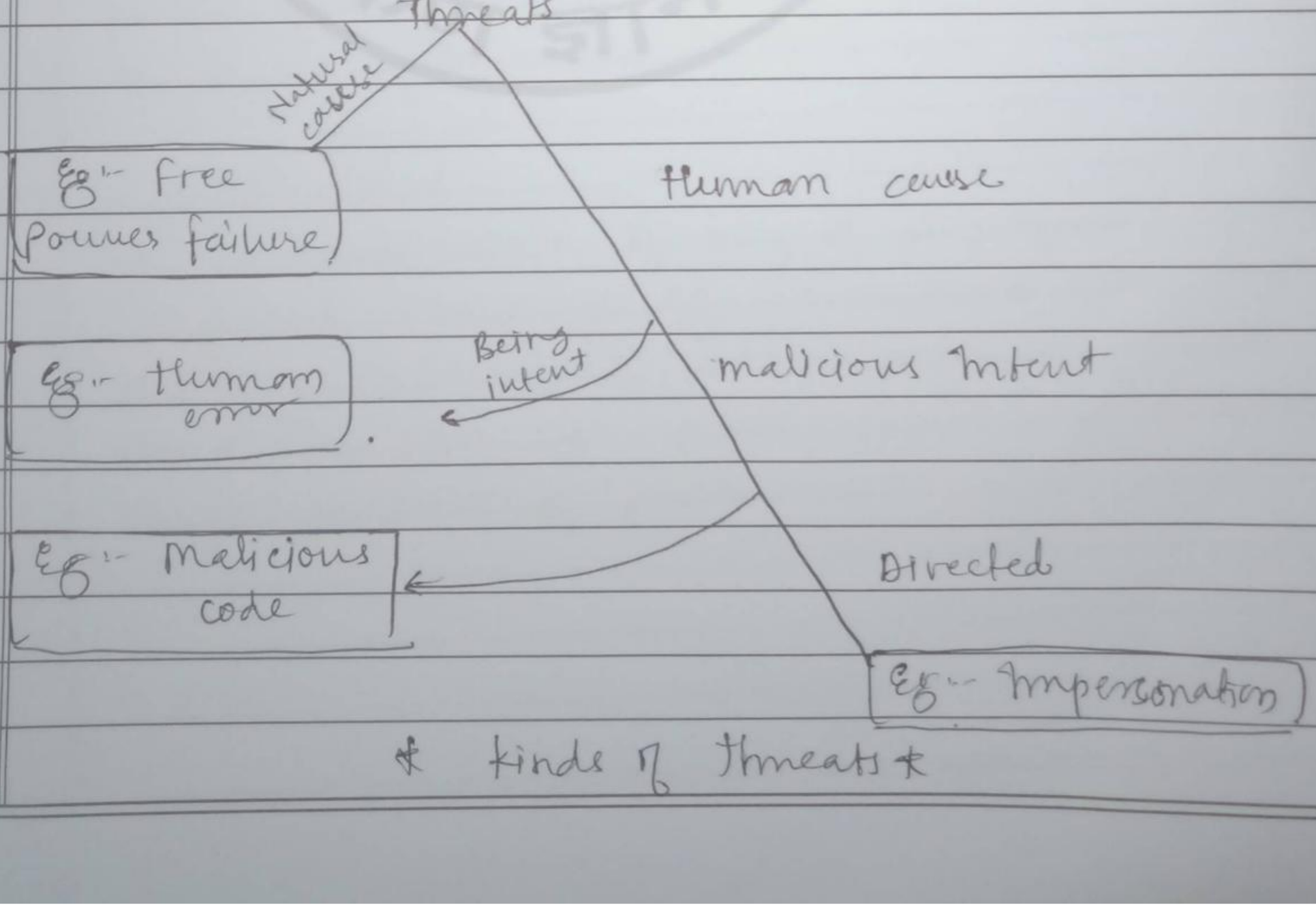
Q1 Explain all cloud security risk threats.

→ We call potential cause of harm threat. can be either benign or malicious Non malicious kinds of harms include someone's accidentally spilling a soft drink on laptop, unintentionally deleting text, inadvertly sending message to wrong person.'

- most computer security activity relate to malicious human-caused harm. A malicious human-caused harm actually to cause harm
- Indirected attack, attackers intends harm to specific computer perhaps at one organisation or belongs to specific individual trying to drain bank account

* Advance persistent threats:-

Security experts are becoming increasingly concern about type of threat called advance persistent threat. Alone attacks might create random attack that individuals, but resulting impact is limited



* kinds of threats *

Q2. Explain in detail various types of cloud security mechanism

→ Types of clouds:-

1) Public cloud:
In this type of cloud model, consumers can access service over internet resource are publically available to uses cloud infrastructure & management are not

2) Private cloud:-
It is managed by either 3rd party cloud service provider or organization itself. This type of cloud is built in firewall of organization. Its advantages are secured, etc.

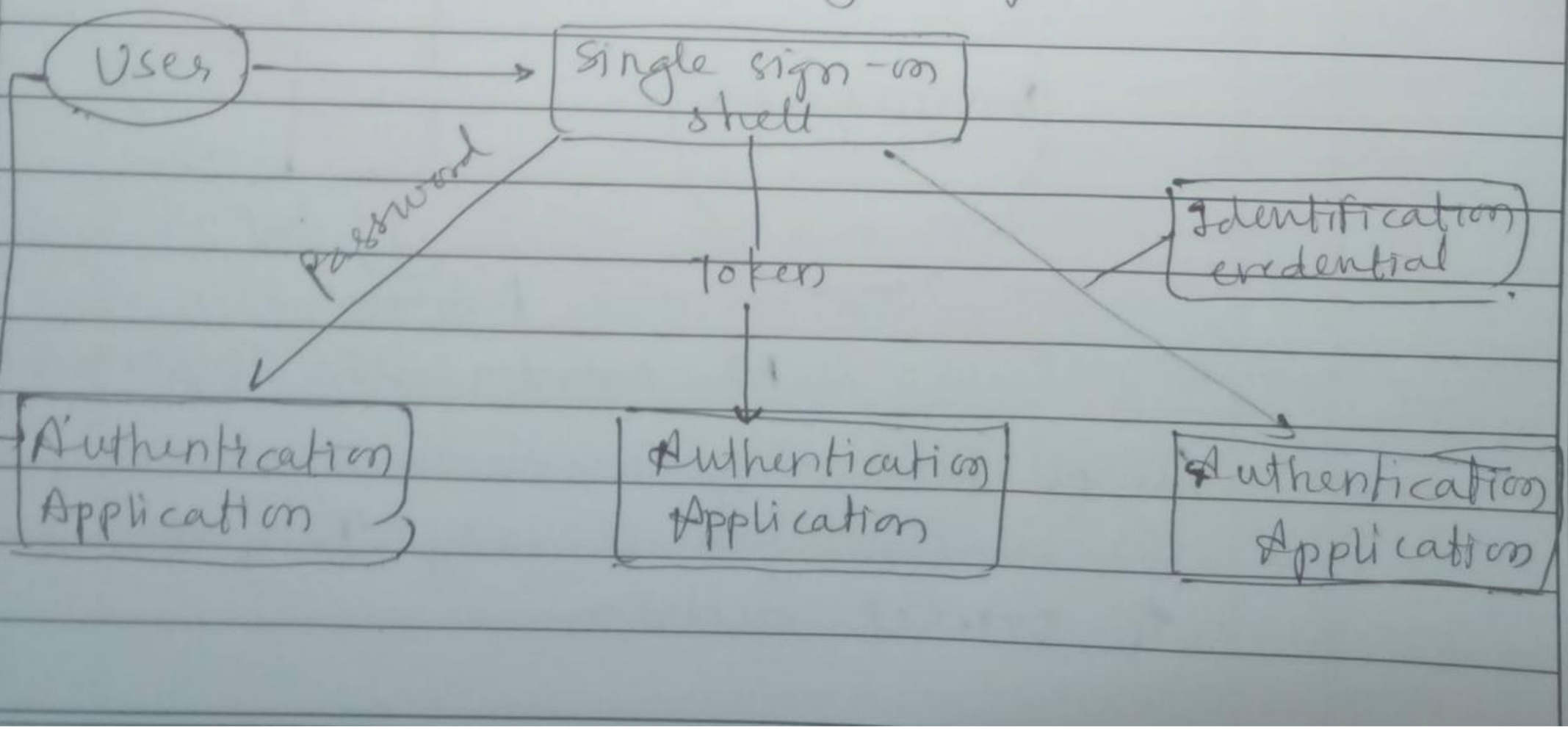
3) Community cloud:-
This type of cloud model allow uses from some community to share computing infrastructure community cloud can be created using salesforce platform prices of such cloud depend type of uses, whether employee organization

4) Hybrid cloud.
It is combination of any of deployment models mentioned above for eg:- consumers can store their individual to create data in private cloud or can use public cloud for processing large amount of data

Q3 Explain digital signature as cloud security mechanism

- Digital signature mechanism is means of providing data acts enticity integrity through authentication and non-repudation.
- A message is assigners a digital signature prior to transmission which is then reduced invalid if message experience any selbsequent, unauthorized modificating
- A digital signature provides evidence that message received is came as one created by its rightful sender.
- Data hashing and assymetrical encryption are invalid in creation of digital signature which especialy exists as message digest that was encrypt by private key to originate.
- Recipent verifies signature validity by using corresponding public key to decrypt digital signature encrypted hash which produce message digest.

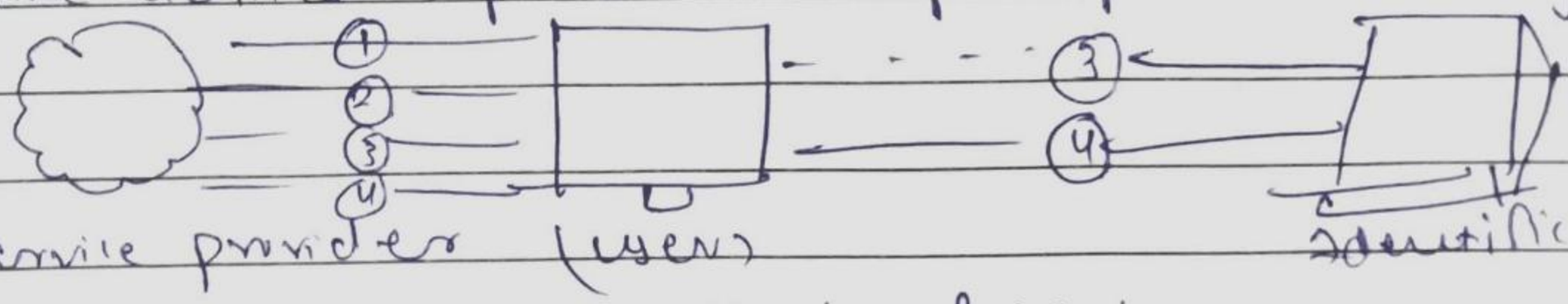
Q4. Write short note on single sign on



- Think of an umbrella procedure to which you login once per session for example once a day per session you identity and authentication codes for all that different processes when you want to access email for eg. instead of your simple used ID and password screen single sign-on process.
- Difference between these 2 approaches is that federated identity managment involves a single identity managment modules

Qs) write note on SAML (Security Assertion Markup Language)

- Two prerequisites make work. Trust and standardization.
- System that request identity information must trust data it recieves system provide identity information must trust rec
- The 2 system must have std. way to communicate
- Security assertion Markup language makes such exchange possible, standards specifies xml messages that parties can use to exchange identity as well as protocols.
- HTTP offers benefit of compatibility with TLS use of which we highly recommed for protection of SAML communication
- SAML defines 3 parties where participate in identity exchanges



1) subject navigates to SP site of login.
2) SP sends subject browser an authentication
3) Browser relays authentication request to IDd.
4) Idp attempts to authenticate subject then returns authentication response to browser and reads authentica login user in with previleges idp specified.

Q6) Explain cloud security as service with its advantages

- A cloud can be configured in many way but there basic modes with which clouds provide service
- cloud provider gives customer access to applications dumming in cloud.
- Here customer has no control over infrastructure or even most of aspect and user application
- community cloud shared by several organization and is usually intended to accomplish a share goal.
- Public cloud available by an organization and sells cloud service
- A hybrid cloud is composed of two or more types of clouds connected by technology.
- Advantages

1) Automatic Backup
2) Hardware failure independence
3) Security of clients virtual environment.
4) Responsibility of provider before clients company.