**QUESTIONS JUMBLED HAIN WO BHI PASTE KRO**

**6th??**

**1b??**

**2b?**

**2 b I am trying but there should be one more trying wiht me**

**2c guys?????**

Format

Question - 1 a….

Answer - ….Confidentiality principles include: THIS IS CORRECT

1)Need to know: Unless you have the proper authorization or clearance, you cannot see all the information at a particular classification level. To be authorized to receive sensitive or classified information, a prospective recipient must first prove that they need access to that information.

2) Data separation

Some measures employ access control

mechanisms to prevent adversaries from reaching information

or to prevent information from reaching locations where unauthorized disclosure may occur

By doing so, we prevent disclosure of information. There are many ways to protect data from being accessed by unauthorized people. One way is to physically separate the data (for example, by keeping it in separate compartments), or to use a filtering router that screens data by matching character strings or security labels.

3) Compartmentalization : is based on the concept that restricting and isolating access to information will reduce the risk of compromising complete confidentiality of information.

4) Classification

Assign labels to information to identify the

appropriate level of protection, handling and

control of the information.

5) Encryption

A reversible process of transforming plain text

into enciphered text using an encryption

algorithm.

Question 2:

(a) (10 pts) What are the three types of security strategies? Briefly describe each of them.

(b) (5 pts) For an organization, under what conditions, it is necessary to use all three types of security strategies? Why?

(c) (6 pts) Identify which types of security strategy use the following mechanics or tools?

* 1. Fire walls
  2. Intrusion detection mechanisms
  3. Information assurance policies
  4. Smart cards
  5. Cryptography
  6. Digital signatures

Answer 2:

(a) The three types of security strategies are:

(I) Obscurity Strategy

* if the existence of an organization’s IA   
  baseline and critical objects are   
  unknown, the organization might avoid   
  or reduce threats
* Intent to secure the system by hiding  
  the details of security mechanisms

(II) Perimeter Defense Strategy

* Focus on threats from outsiders.
* Intent to control flow of information   
  between organization’s internal trusted   
  network and untrusted external networks.
* Not much IA capabilities is allocated to   
  secure internal system.
* Examples: Firewalls, security access keys,   
  access codes

(iii) Defense in Depth Strategy

* Define a number of inter-operable and   
  complementary technical and nontechnical IA layers of defense
* Separate organization’s network into   
  enclaves
  + An enclave is an environment under   
    control of a single authority with personnel   
    and physical security measures.
* Perimeter defense for each   
  enclave
* Complicated and multiple   
  connections among enclaves and   
  between an enclave and outside
* Need multiple layers and different   
  solutions for each connection

(b)

(c)

1. Fire walls - Perimeter Defense Strategy
2. Intrusion detection mechanisms -
3. Information assurance policies - Defense in Depth Strategy
4. Smart cards
5. Cryptography
6. Digital signatures

5 . Security is a kind of security mechanism used to curb human errors, thefts, frauds or misuse of facilities provided to employees or visitors within an organization.

It needs to taken care of by the HR ( Human Resources ) Team by either implementing certain rules or by referring to existing practices in other organizations.

Below are a few major difficulties related to Personnel that we come across in an organization.

**Background Verifications :**

All the employees, security and all the personnel that are part of the organization have ot be checked for the authenticity of the details provided by them. Things like Credit Report, past police records, insurance Personnelreports, education reports etc.

**Security Clearances :**

This is mostly valid for government and military service employees. if the security clearance is not done, there is chance that the leaving or joining employees might become a threat to the organization by leaking the information from inside.

**Strict Employeement Agreements :**

If there are no strict agreements with the employees mentioning the issues the organization or the personnel would run into given any fraud is committed by the employee, it will become difficult to regulate the actions of the employees. Both Non competitive and non-disclosure agreements have to be signed by the employee.

**Hiring and Termination Practices :**

Hiring Manager must follow a rigid process when selecting an employee and also be vigilant understand the actions of the employee and terminate them when deviating from any given principles. It should be made sure that all the exit formalities like Account Clearance, Asset returns etc are done before an employee leaves the organization.

**Job Description :**

If it's not clearly mentioned in the Job description about the criticality and sensitivity of hte project the employee is working on, there is a chance of human error happening.

**Job Rotation :**

Its important to rotate the jobs to possibly discourage fraud, waste and abuse. We must promote cross training so as to keep the employee excited about their work and also to keep them away from any kind of malicious attempts.

**Sepration of Duties and Repsonsibilities :**

Its important assign responsibilities to each employee separately such that one can monitor hte actions of other that will make sure one adhere to the rules.

Q. (10 pts) Identify as many major difficulties as you can to improve personnel security for an organization and provide justifications for each of the major difficulties you identify.

Ans -

Personnel security are the mechanisms to reduce risks of human error, thefts , frauds and misuse of facilities.

The major difficulties that can be improved in personnel security are -

Protecting the data itself and not the perimeter

Many firms appear to be focusing on securing the walls around their data, with firewall technology accounting for nearly 90% of security budgets. There are hundreds of ways to get through a firewall, including through customers, suppliers, and workers. All of these individuals have the potential to circumvent external cyber-security and misappropriate critical information. As a result, you must guarantee that your security efforts are centered on the data rather than the perimeter.

Pay attention to insider threats

It's always easy to imagine threats coming from outside the organizations because they're frequently highlighted by the media sources however it is the insiders who can hurt us the most. Insider assaults are generally difficult to avoid due top its stealthy nature. It can be as simple as an innocent employee clicking on an email link which results in the spread of ransomware across company servers. These types of hazards are the most common and costly ones to organizations like what happened with uber recently.

Encrypt all devices

Nowadays many people prefer to work on their devices like mobile phones and tabs. How can these devices be trusted as reliable? It is integral they be encrypted properly so the data remains secure during migrations.

Testing your security

Think again if you think putting antivirus can safeguard you from cyber threats. It is therefore integral to hire a competent agency to undertake a security audit that will help find security vulnerabilities you weren't expecting. Even walking around the office can show how many coworkers have passwords written down on sticky notes that could overall cause the whole company to be vulnerable.

Deleting redundant data

Many businesses like those in healthcare,banking,government and education deal with sensitive data necessary for the organization. having information disposal measures in place helps to avoid stale data from being lost and stolen later by bad actors. Having a mechanism in place for shredding or deleting redundant data can overall improve security.

Establish Strong passwords

Numerous associations are as yet utilizing loosened up secret word arrangements, prompting straightforward, conventional and simple to hack passwords for basic records, which approach the delicate and significant information. Executing solid passwords is the initial step you can take to fortify your security around here. Utilize sensibly complex passwords and change them like clockwork. Never use passwords like "12345" or "Admin1". Absolutely never record your passwords and pass on them on your workstation for others to discover.

Backing up data regularly

This should as of now be a urgent piece of your IT security system. With secure reinforcements set up, you can endure everything from unplanned record erasure to a total ransomware lockdown. As a security best practice, reinforcement information ought to be put away in a solid, far off area away from your essential business environment.

Updating programs regularly

Ensure your PC is appropriately fixed and refreshed. This is regularly the most ideal approach to guarantee its sufficiently ensured. Your security applications are just on par with their latest update. Since programmers and ransomware strains are continually adjusting to take advantage of shortcomings in prior programming adaptations, it is prudent to refresh these applications consistently.

Spending more resources on cyberSecurity

Many CIO's have conceded that investing more cash and more energy in information security is an absolute necessity, as its absence keeps on being the main danger to your IT foundation. Many large organizations with delicate business information to ensure are designating boss security officials, regularly to board level situations, with an affirmation that network safety must be a vital piece of all business measures.

Create a company wide security mindset

Each and every individual who has a security key and username is answerable for keeping information secure. IT directors should occasionally remind their chiefs and workers that they should not impart logon data to any external party. Data security is everybody's work and isn't simply restricted to simply a modest bunch of representatives in the IT group.

Better background checks

It is important to have a thorough background check performed before letting employees join an organization. This helps the new employee understand the importance of the overall organization security and also lets the company have an understanding of the employee. prevents malicious people from joining an organization also.

QUESTION 4

**Part A:**

The major advantages of usinchain to protect information systems handling confidential informations are listed as follow:

* **Decentralization:** This is one key characteristic of blockchain technology, and its advantage is that it eliminates the need for a third party to serve as a middleman in order to validate transactions or activities, speeding up transaction validation.
* **Network distribution:** This point offers a number of advantages since, by keeping the network spread, nobody owns the networks in the initial place and various users can always access several copies of the same information. Additionally, this feature makes it robust and durable to any sort of failure as the loss of a single nodes doesn't really imply widespread network issues.
* **Availability:** Even when some nodes are down, a huge number of servers guarantees blockchain resiliency. Additionally, even in the event of a hacked node, other peers may still access the proper blockchain since every node in the network has a copy of the distributed ledger.
* **Data integrity:** Blockchains are intended to serve as ledger accounts, where each block is connected to the blocks around it by use of a cryptographic hash function. A transaction cannot be changed or removed after it has been added to the blockchain. Any modifications made to the information that has already been stored are handled as transactions.

**Part B:**

The serious concerns in using blockchain to improve the information assurance of information systems with high security requirements are as follow:

* **Scalability:** Every active node must keep a complete version of the blockchain, which requires a lot of storage.
* **High computational resource requirements:** Block hashes generated by Proof of Work consensus techniques demand a substantial amount of processing power.
* **51% attack:** The main characteristics of blockchain will be compromised if a small number of miners can control more than 50% of the network's processing power.
* **Data is Immutable:** One of the major drawbacks of the blockchain has been data immutability. You should see that this immutability could only exist if the network nodes are distributed equitably if you comprehend how networks operate.

Part C:

For this type of system we will use Private Permissioned typ pf blockchain system. The development of a stable agreement between all of the participants in the inventory network using blockchain technology might provide more simplicity. By using a clever agreement, the store network organization may reduce the number of mediators. These clever arrangements can save exchange costs, improve competitiveness, and increase proficiency, allowing the rancher or producer to keep a larger portion of the revenue.

The food industry may benefit greatly from blockchain when combined with cutting-edge information technology. By combining the power of blockchain with the Internet of Things, we can transform the food industry (IoT). IoT systems connect the physical and digital worlds by monitoring variables like temperature and humidity while an object is being transported or stored. Each component in the production network may store and retrieve this data on the blockchain, a stable and immutable platform.

Costs for the stores will decrease if the production network is streamlined. It focuses on administrative consistency and will help to expedite and improve the food approval process.

Q- 4

A) A blockchain is a decentralized ledger that contains data about all transactions performed across a peer-to-peer network.

**Major Advantages and Reasons**

**Secure data storage and processing** — Blockchain records are immutable and any change recorded on the blockchain is transparent and non-removable. Therefore, data stored on a blockchain is protected better than traditional digital or paper-based records.

**Safe data transfers** — The blockchain enables fast and secure transactions of data and finances. Features like smart contracts allow for automatic execution of agreements between several parties.

**No single point of failure** — Permissionless blockchain systems are decentralized and, therefore, more resilient than traditional systems. The compromise of a single node won’t affect the operation or security of the whole blockchain. This means that even in the case of DDoS attacks, the system will operate as normal thanks to multiple copies of the ledger. Private blockchains, however, can’t offer you this advantage.

**Data transparency and traceability** — All transactions on blockchains are digitally signed and time-stamped, so network users can easily trace the history of transactions and track accounts at any historical moment. This feature also allows a company to have valid information about assets or product distribution.

**User confidentiality** — The confidentiality of blockchain network participants is high due to the public key cryptography that authenticates users. However, some blockchain-based startups go a step further and improve this technology. For instance, Guardtime developed a Keyless Signature Infrastructure (KSI) that allows users to verify their signature validity without disclosing keys.

**Increased customer trust** — A blockchain offers data privacy and transparency that can help businesses gain customers’ trust. Furthermore, in many of today’s blockchain networks, data owners can be granted full control over their personal data and decide who can access it and when.

B) **Serious Concerns and Reasons**

**Scalability**: All the actively participating nodes are required to have entire copy of blockchain which is a huge storage requirement

**High computational resource requirements**: Proof of Work consensus algorithms require a significant amount of computation power to calculate hash of block.

**51% attack**: If a miner or a group of miners can control more than half of a blockchain network’s computational resources, this will undermine the major features of blockchain.

**Reliance on private keys:** Blockchains rely on the use of private keys: long sequences of random numbers automatically generated by a wallet. Private keys are used for interacting with the blockchain and, in contrast to user passwords, can’t be restored. If a user loses their private key, all data encrypted with it will most likely be impossible to recover.

**Adaptability challenges** — Though blockchain technology can be applied to almost any business, companies may face difficulties integrating it. It’s quite challenging to employ this technology in supply chain systems, for instance, as it may take much time to re-implement the supply chain logic using a blockchain.

**High operation and customization costs** — A blockchain requires substantial computing power and storage capacity. This may lead to higher marginal costs in comparison with existing non-blockchain systems.

C) To secure and transparent to connect all stakeholders directly throughout the process and to address fraud transaction the best type of blockchain will be either vertically coordinated private blockchain or consortium-type blockchain.

**Consortium** blockchain technology is a combination of several blockchains. E.g like Hyperledger technology.

**Private blockchain** is under administrative control of an entity/organization, or a closed group and does not require expensive mining process. E.g. Corda.

The consortium blockchain technology is used to set permission and authentication for different roles in food transaction, which meet the challenge of the privacy protection of multi-stakeholders. A **smart-contract** life-cycle management method could be introduced to improve the transaction security and privacy protection.

**Advantages**

**Validation:** The number of participants in the consortium blockchain is known and verified. Authentication conducted by them reduces the risk of data threats. The nodes violating the set protocols are immediately identified and suffer the consequences of violation. The other threats like SQL injection, DDoS, “man in the middle” are insignificant in consortium blockchain.

**Control:** Instead of a sole entity, a particular group of authentic participants controls the blockchain. This control helps to set rules, amend balances, edit or cancel an incorrect transaction, and encourage full cooperation for companies with common goals upon confirmation from each participant.

**Security:** The information on the authentic blocks is not permissible for access to the public. But the consortium participants can access the information quickly, ensuring high-end security. It builds high levels of confidence and trust for the platform clients.

**Economic:** As compared to other blockchains, consortium blockchain charges no service or transaction fee in the consortium setting.

**Agreement:** According to the governance scheme, a contract is often made by a relatively fewer number of nodes. This type of consensus is easier to reach as it is less demanding. These aspects directly affect the transactional outputs leading to speedy operations and improved scalability.

**Flexibility:** The involvement of several validators in other blockchains leads to mutual consensus and synchronization issues. However, such issues are avoidable in consortium blockchain due to the limited number of participants.

**Energy requirement:** Nonessential data mining directs the exclusive use of energy for routine operations only. Also, the Proof-of-vote type agreement doesn’t employ much energy.

Ans 3

a. The advantages for using formal methods to address information assurance of information systems are as follows-

1. Clarify requirements and analysis: With the formal methods it becomes possible to state the requirements beforehand which is important while handling confidential information. They aim to remove the uncertainty from the system specifications.

2. Express the implicit assumptions: By stating everything before hand, it allows for people to state their assumptions so that no ambiguity or misunderstanding is there.

3. Identify undocumented or unexpected assumptions: When doing formal methods, as it improves the robustness of the software, all requirements are known and documented.

4. Expose defects: As the formal methods improve the quality of the software, it allows for early defects identification, software errors and failures.

5. Identify exceptions: Using the formal methods, the software becomes more reliable and robust. The edge cases to the to the system can then be found easily and hence it allows for a better tracking of resolutions.

6. Evaluate test coverage: The formal methods are quite important in improving the quality , reliabily and effectiveness of software. Hence by the formal methods the testing coverage improves greatly.

7. They also allow to expose the flows in system requirements and due to this it allows for better understanding of the problem

b. The major challenge of using formal methods to address information assurance problems are as:

1. It requires that the developer has a good knowledge of mathematics.

2. It could be that the various aspects of a design are represented by different formal specifications methods

3. The use of formal methods does not guarantee that the specifications would be completed