

Sampurna Prabhu
22101A0078 - IMFT-A

Page No.	
Date	

Assignment 4 :- Cyber Security

- Q.1 Why are digital Signature considered more secure than handwritten Signatures in legal and financial transaction? Discuss how the use of digital Signatures in India has accelerated the adoption of digital governance.

Soln Digital Signature vs Handwritten Signatures in Legal and Financial Transactions

(i) Security of Digital Signatures:-

Digital signatures are generally considered more secure than handwritten signatures because they utilize cryptographic algorithm such as Public Key Infrastructure to ensure that the signature is uniquely tied to the signer and the document.

(ii) Digital Signature

(i) Authenticate Identity:- They confirm the signers identity through encryption keys which are difficult to forge.

(ii) Provide non-repudiation :- Once a document is digitally signed the signer cannot deny their involvement in signing the document.

(iii) Digital Signatures and Digital Governance in India

India has embraced digital signature to modernize and simplify governance fostering the digital economy and ensuring transparency and accountability.

Online transactions.

(iv) The Aadhar system (a biometric identification program) and e-filing of taxes benefit from digital signature to ensure the security and authenticity of transactions.

Q.2 How does CERT-In collaborate with international cybersecurity agencies? How does CERT-In's role extend beyond incident response to include proactive measures like vulnerability assessment?

Soln CERT-In's collaboration with International Cybersecurity Agencies to combat cyber threats and improve cybersecurity.

(i) Interpol:- CERT-In works with Interpol to share intelligence on emerging cyber threats and improve cybersecurity.

(ii) ITU (International Telecommunication Union):- CERT-In participates in global forums with ITU to establish cybersecurity standards, best practices and responses to large scale cyber incidents.

(iii) CERT-In's Role Beyond Incident Response-

While CERT-In is primarily focused on incident response, it also plays a proactive role in enhancing India's cybersecurity posture.

- Capacity building :- CERT-In works to enhance the cybersecurity knowledge and readiness of both public and private sector entities through training and awareness programs.
- Vulnerability assessments - CERT-In conducts assessments to identify weaknesses in infrastructure and recommends mitigation strategies.

Q.3 With the rise of AI-driven attacks and quantum computing on the horizon, do you think current mechanisms like firewalls and encryption will become obsolete?

Soln

Impact of AI and Quantum Computing on cybersecurity

- As AI-driven attacks and quantum computing evolve, traditional security mechanisms, such as firewalls and encryption, face growing challenges.
- AI driven attacks :- AI can be used to automate and refine attacks making them faster, more targeted and harder to detect.

- Quantum Computing :- Quantum Computers could potentially break existing encryption algos. (eg, RSA) which rely on the difficult of factoring large numbers.

• Three ~~the~~ innovation shaping future cybersecurity defenses:

(i) Quantum-resistant encryption
To counter quantum computing threat to current encryption algorithm the development development of quantum safe cryptography will be critical.

(ii) Zero Trust Architecture:-

This approach assumes no device or user is trustworthy by default, even if they are inside the network. Every access request is verified continuously which limits the damage a cyberattack can cause even if an intruder penetrates the network.

(iii) AI-driven threat detection

AI can be leveraged to identify patterns of behaviour that deviate from the norm, allowing faster detection of new and sophisticated threats.

Q.4 India is moving towards stricter data localization laws. How does this impact cybersecurity and what role should CERT-IN play enforcing these regulations?

Soln Data localization and cybersecurity

- India's movement towards stricter data localization laws mandates that sensitive data be stored and processed within the country.
- This can have several cybersecurity implications:

- Positive Impacts

- Ensures that sensitive data is protected by Indian cybersecurity laws and regulations
- Reduces the risk of cross-border data theft or cyberattacks that might target data stored overseas.
- Facilitates faster response time in case of cyber incidents involving local data.

- Challenges

- could create data silos that complicate data sharing across borders
- may increase the complexity and cost of compliance for international companies, potentially impacting innovation and efficiency.

Role of CERT-In in Enforcing Data Localization:

CERT-In should play a crucial role in ensuring compliance with data localization laws by:

- (i) monitoring and enforcing compliance with localization regulation.
- (ii) Coordinating responses to cyber incidents involving localized data.
- (iii) Providing guidelines for organizations on securing data stored within India.

* Enhancing National Security or Creating Barriers?

- Data localization can enhance national security by ensuring greater control over data and its protection under local laws.
- Balancing security with the free flow of information is essential to ensure the data localization does not inadvertently hinder business innovation or international cooperations.