OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Perspective

Techniques for Improving Information Security in a Developing Technological Environment

Amelia Aarohi*

Department of Information Technology, Liverpool Hope University, Liverpool, United Kingdom

DESCRIPTION

The modern world has made Information Security (InfoSec) a need for day-to-day existence. Information must be protected against illegal access, manipulation, and destruction as more and more businesses, governments, and people depend on digital data. Information security refers to the methods, tools, and procedures used to protect data against online threats and breaches. The modern age of technology has changed our working, communication, and business practices. Due to the internet's explosive growth, mobile technology, and cloud computing, both individuals and businesses now maintain huge amounts of sensitive data online. This covers financial data, intellectual property, personal data, and even information about the vital infrastructure. Information security makes sure that only authorized individuals can access sensitive data. Violating confidentiality policies may result in identity theft, spying on businesses, or unapproved entry into vital state secrets. Protecting the accuracy and all aspects of data is an additional fundamental role of information security. For sectors like healthcare and banking, where even little changes can have disastrous effects, maintaining data integrity is essential.

Data and systems are made available to authorized users when needed due to information security. Denial-of-Service (DoS) attacks are one way to generate availability disruptions that can significantly damage business operations and result in large financial losses. The ever-changing environment of cyber threats involves a variety of issues for both individuals and organizations. Information security issues will only grow more complex as technology develops. New technologies like 5G networks, Artificial Intelligence (AI), Machine Learning (MI), and quantum computing will present both new possibilities and challenges. Although AI and MI are currently being used to identify and address cyber threats faster, they may also be utilized by hackers to carry out more complex attacks. Although quantum computing is still in its early stages, it has the potential to destroy existing encryption techniques, which means that quantum-resistant algorithms will need to be developed. New security issues will arise when 5G networks become widely used, especially in light of the substantial rise in connected devices.

Data cannot be read by unauthorized parties, even in the event that it is intercepted, because of encryption. To preserve confidentiality, encryption should be applied to both data in transit and data at rest. Identity verification and communication security are two common uses for Public Key Infrastructure (PKI). By requiring users to present two or more forms of identity before gaining access to a system, Multi-Factor Authentication (MFA) lowers the possibility of unwanted access. This can contain biometric data, something the user possesses (a credential), or something they know (a password). Providing users and staff with security best practices training is one of the best strategies to lower the risk of cyberattacks. By educating people how to spot dangers, regular training can help reduce the impact of techniques for social engineering like hacking. Various policies and standards have been adopted by governments and international organizations to ensure information security across industries. An Information Security Management System (ISMS) can be established, implemented location, and kept up to date with the help of this international standard. Organizations that follow to these guidelines and standards not only avoid legal repercussions but also gain the trust of stakeholders and customers.

Organizations need to take a proactive and forward-thinking approach to information security in order to avoid these ever-evolving threats. This involves making investments in Research & Development (R&D), encouraging industry-wide cooperation, and regularly revising security plans to take advantage of emerging threats. Information security has great importance in the modern digital environment. Organizations and individuals need to put strong security measures in place to protect sensitive data since cyber dangers are growing and we are depending more and more on digital information. Risks can be reduced and data availability, confidentiality, and integrity can be protected by knowing the basic principles of information security, identifying the main threats, and putting appropriate security measures in place.

Correspondence to: Amelia Aarohi, Department of Information Technology, Liverpool Hope University, Liverpool, United Kingdom, E-mail: ameaar@LHU.uk

Received: 21-Aug-2024, Manuscript No. JITSE-24-34405; **Editor assigned:** 23-Aug-2024, PreQC No. JITSE-24-34405 (PQ); **Reviewed:** 06-Sep-2024, QC No. JITSE-24-34405; **Revised:** 13-Sep-2024, Manuscript No. JITSE-24-34405 (R); **Published:** 20-Sep-2024, DOI: 10.35248/2165-7866.24.14.408

Citation: Aarohi A (2024). Techniques for Improving Information Security in a Developing Technological Environment. J Inform Tech Softw Eng. 14:408.