

The Internet as a Digital World Application for Secure Data Transfer

Raghav Rao¹, Kavitha Iyer²

Professor¹, Student²

Department of CSE

Coimbatore Institute of Technology

Corresponding Author's E-mail: r.rao321@gmail.com¹

Abstract

Computer security is concerned with the managerial practises and technological measures used to protect computer hardware, software, and data against accidental or deliberate unauthorised access. Computer privacy refers to the moral and legal obligations to safeguard data against unwanted access and publication. Computer privacy concerns are thus political judgments about access to information, whereas security concerns are the methods and protections for implementing the privacy decisions. The desire for military secrecy, industrial security, and information sharing are all incentives for security and privacy. It is feasible to construct some type of operational security based on national and state regulations that enables the management of a computer installation to exert control and accountability over the installation. Guidelines and processes for accountability, control levels, and system configuration may be developed. Through risk analysis, assessment, and insurance research, preventive actions against internal and external dangers can be devised. Psychological security of operational workers is critical to operational security success. It is advised that risk management teams comprised of operations managers, programmers, internal auditors, and physical security employees be developed on a regular basis. Physical security must safeguard against damage caused by natural disasters, tampering, and malicious entrance and destruction. Both hardware and software must be protected by user identification and authentication. There are bibliographies, pictures, and author and subject indexes included.

Keywords: *Digital World Application, Secure Data Transfer, Security Employees*

INTRODUCTION

Computer security, also known as cyber-security or information technology security, is the safeguarding of information systems against theft or damage to their hardware, software, and data, as well as from disruption or misdirection of the services they provide. It entails restricting physical access to hardware and safeguarding against harm caused by network access, data and code injection, and operator misconduct, whether intentional or accidental, or as a result of

being duped into straying from secure processes. The topic is gaining in prominence as most civilizations increasingly rely on computer systems. Computer systems today encompass a diverse range of "smart" devices, including smartphones, televisions, and tiny gadgets connected to the Internet of Things – and networks encompass not only the Internet and private data networks, but also Bluetooth, Wi-Fi, and other wireless networks.

TYPES OF COMPUTER SECURITY

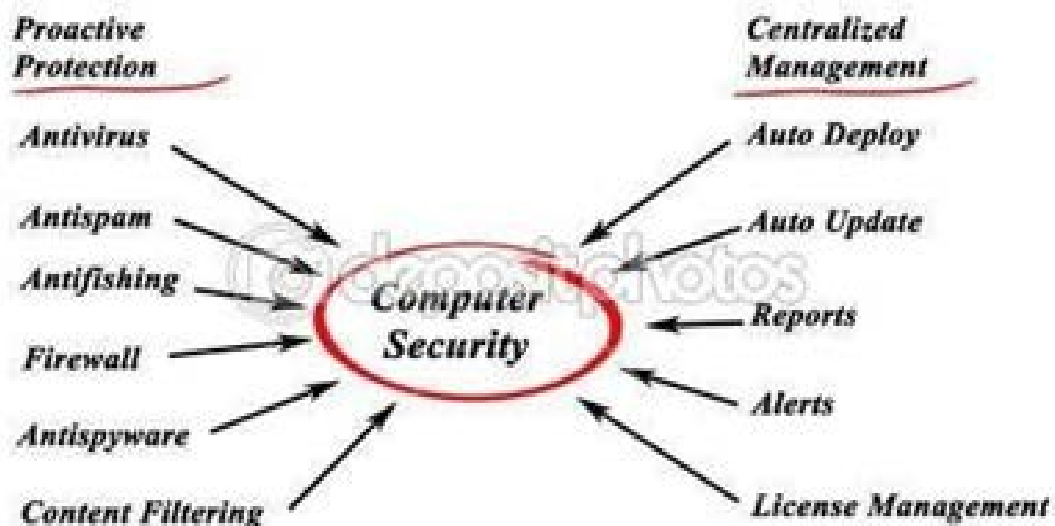


Fig 1 *Types of computer security*

A. Identity management: Each company will have its own identity management system in place to govern access to data and computing resources. Cloud providers can either incorporate the customer's identity management system into their own infrastructure using federation or single sign-on (SSO) technology, or through a biometric-based identification system, or they can provide their own identity management solution. Cloud ID, for example, addresses this issue with privacy-preserving cloud-based and cross-enterprise biometric identification solutions. It securely associates users' personal information with their biometrics and saves it in an encrypted format. Biometric identification is performed in an encrypted domain using a searchable encryption mechanism to ensure that the cloud provider or possible attackers do not obtain access to any sensitive data or even the contents of individual queries.

B. Physical security: Cloud service providers safeguard the IT hardware (servers, routers, cables, etc.) against unauthorised access, interference, theft, fires, and flooding, and guarantee that critical sources (such as electricity) are sufficiently resilient to avoid disruption. This is typically accomplished by providing cloud applications from 'world-

class' data centres (i.e. those that have been professionally specified, developed, constructed, managed, monitored, and maintained).

C. Personal security: Various information security concerns affecting IT and other cloud service professionals are typically addressed through pre-, intra-, and post-employment activities such as security screening potential recruits, security awareness and training programmes, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, and politeness.

D. Identity management: Cloud computing enables consumers to rely on access to their data and apps; at the very least in part (failures at any point- not just within the cloud service providers domains- may disrupt the communication chains between users and applications).

E. Application security: By specifying, creating, implementing, testing, and maintaining suitable application security mechanisms in the production environment, cloud providers ensure that applications provided as a service via the

cloud are secure. Notably, as with any commercial product, the controls they install may not entirely mitigate all of the risks they identify, nor may they have recognised all of the hazards that worry consumers. As a result, users may also need to ensure that cloud applications are sufficiently secure for their intended use, including regulatory requirements.

F. Browser security: Browser security is the extension of internet security to web browsers in order to safeguard networked data and computer systems from privacy breaches or viruses. Browser security audits frequently make use of JavaScript—and perhaps cross-site scripting (XSS)

G. Network Security: Network security policies are used to prevent and monitor illegal access to, abuse of, modification of, or denial of service attacks against a computer network and network-accessible resources.

PRIVACY

Providers guarantee that any sensitive data (credit card details, for example) is disguised or encrypted, and that only authorised users have complete access to the data. Additionally, digital identities and credentials, as well as any data the

provider collects or creates about client activities in the cloud, must be safeguarded.

A. Internet privacy:

Internet privacy refers to the right or obligation to protect one's personal information while it is stored, repurposed, provided to other parties, and shown over the Internet. The term "internet privacy" refers to a subset of the term "data privacy." Since the inception of large-scale computer sharing, privacy problems have been raised. Privacy can refer to either personally identifiable information (PII) or non-personally identifiable information (non-PII), such as a website visitor's conduct on the site. Personal identifiable information (PII) is any information that may be used to identify an individual. For instance, age and physical address alone may often identify an individual without providing their name directly, as these two criteria are sufficiently distinctive to identify a specific person.

B. Levels of Privacy:

- Individuals with a passing interest in Internet privacy do not need to attain complete anonymity. Internet users can safeguard their privacy by disclosing personal information in a regulated manner.

- Some people demand a considerably higher level of privacy. In that situation, individuals may attempt to establish Internet anonymity in order to protect privacy — the capacity to use the Internet without allowing third parties to link Internet actions to the Internet user's personally identifying information. Additionally, numerous governmental institutions defend individuals' privacy and anonymity online to a certain extent.
- Posting anything online can be detrimental or put you at risk of a hostile assault.

The most popular and straightforward method of safeguarding a network resource is to give it a unique name and password.

C. Search Engine:

- Search engines are capable of tracking a user's search activity. Personal information can be disclosed through searches when the user's computer, account, or IP address is associated with the search words used.
- Search engines have asserted the need to preserve such information in order to provide better services, guard against security threats, and combat fraud. Those in possession of the database frequently keep track of where each user has travelled on the Internet to access AOL's system.
- AOL maintains a database of 21 million subscribers, each with their own unique ID number;
- Search engines can also record user information for up to ninety days, such as location and time spent using the search engine.

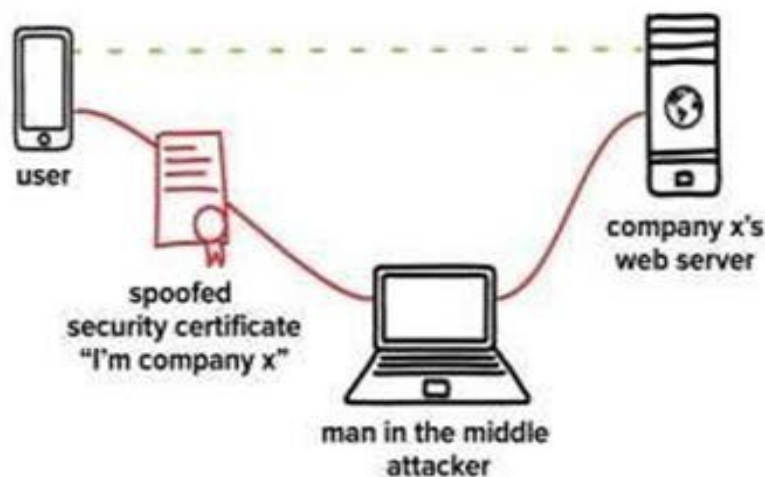


Fig 2. Computer privacy and servers

The data is used by the majority of search engine owners to determine which demands must be satisfied in certain sections of their sector. Individuals in the legal profession are also permitted to utilise information gathered from these search engine websites.

DISASTER RECOVERY

Disaster recovery (DR) is a collection of policies and processes that enables the recovery or continuation of critical

technological infrastructure and systems in the aftermath of a natural or human-caused disaster. Disaster recovery is concerned with the information technology or technology systems that support important business processes, as opposed to business continuity, which is concerned with the continued operation of all critical components of an organisation in the face of substantial disruptions. As a result, disaster recovery is a subset of business continuity.



Fig 3 Disaster recovery cycle diagram

A. Classification:-

The critical nature of disaster recovery planning: Recent research demonstrates that a more comprehensive approach to pre-disaster planning is more cost-effective in the long term. Each dollar invested on hazard mitigation (such as a disaster recovery plan) results in a \$4 savings in response and recovery costs for society.

As information technology systems have become more vital to the smooth functioning of a business, and potentially the economy as a whole, the necessity of assuring their continuing operation and speedy recovery has grown.

Control Measures: Control measures are processes or systems that can help companies mitigate or eliminate specific dangers. Numerous strategies can be incorporated into a disaster recovery strategy (DRP). Disaster recovery planning is a component of a broader process known as business continuity planning.

It entails preparing for the restoration of applications, data, hardware, electronic communications (such as networking), and other information technology infrastructure.

IT disaster recovery control measures can be classified into the following three types:

1. **Preventive measures** - Controls aimed at preventing an event from occurring.
2. **Detective measures** - Controls aimed at detecting or discovering unwanted events.
3. **Corrective measures** - Controls aimed at correcting or restoring the system after a disaster or an event.

Strategies:

- Regular backups to tape and off-site storage
- On-site disc backups that are automatically transferred to off-site disc, or off-site disc backups that are created directly to off-site disc
- Data replication to an off-site location, which eliminates the requirement for data restoration (only the systems must then be restored or synced), frequently utilising storage area network (SAN) technology.
- Private Cloud solutions that copy management data (VMs, Templates, and discs) into the private cloud's storage domains. These management data are kept in an xml format called

OVF (Open Virtualization Format) and may be recovered from the Data Base in the event of a disaster. For instance, Disaster Recovery with OVir.

- Hybrid Cloud systems that replicate data both on- and off-site. These technologies provide fast failover to on-premises hardware, but servers may also be brought up in cloud data centres in the case of a physical disaster. Quorum, Cloud from Persistent Systems, and Ever Safe are all examples.
- the use of high-availability systems that duplicate both the data and the system off-site, allowing for continued

access to systems and data even in the event of a disaster (often associated with cloud storage)

DATA PROCESSING

"The collecting and manipulation of data pieces to generate meaningful information" is what data processing entails. It may be thought of as a subset of information processing in this sense, defined as "the change (processing) of information in any manner visible by an observer."

The phrase is frequently used to refer to a class of commercial data processing software in the context of a business or other organisation.

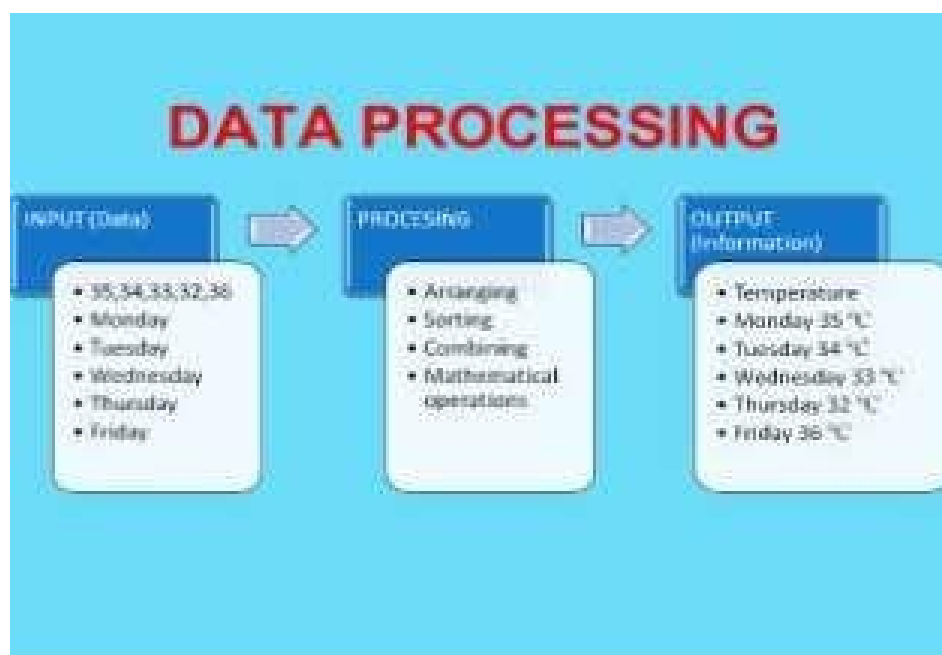


Fig 4 Block diagram of data processing

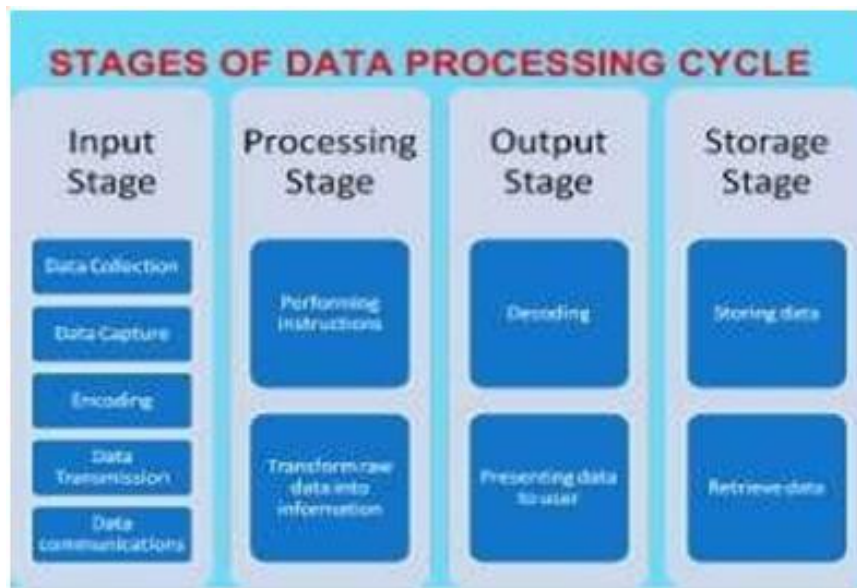


Fig 5. Stages of data processing cycle

A. Processes:

- Validation - Assuring that the information provided is "clean, accurate, and helpful."
- Sorting entails "arranging objects in a certain order and/or in separate groups."
- Summarization is the process of condensing detailed information into its most important parts.
- Aggregation is the process of merging numerous pieces of information.
- Analysis - "the gathering, organising, analysing, interpreting, and presenting of facts."
- Reporting — a set of detailed or summarised data or calculated data.
- Classification - divides data into different groups.

B. Applications:

1) Data processing for commercial purposes

Commercial data processing entails a big amount of input data, a small number of computer processes, and a huge amount of output data. An insurance business, for example, must maintain track of tens of thousands of policies, print and distribute bills, and receive and process payments.

2) Data evaluation

The words data processing and information systems are regarded too broad in scientific and engineering fields, thus the more specialist term data analysis is usually used instead. Data analysis employs specialised and very precise algorithms and statistical computations

that are rarely seen in the regular corporate context.

CRYPTOGRAPHY

Cryptography is a means of storing and transferring data in such a way that only those who are supposed to read and process it may do so.

Cryptography and cryptology, as well as cryptanalysis, are closely linked subjects. Microdots, blending words with visuals, and other techniques for hiding information in storage or transit are all examples of cryptography. (See fig6)

1. Confidentiality (A. Cryptosystem) (the information cannot be understood by anyone for whom it was unintended)
2. Reliability (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the information's creator/sender cannot subsequently dispute his or her intentions in creating or transmitting the information)
4. Authentication (the sender and receiver may verify each other's identities as well as the information's origin and destination).

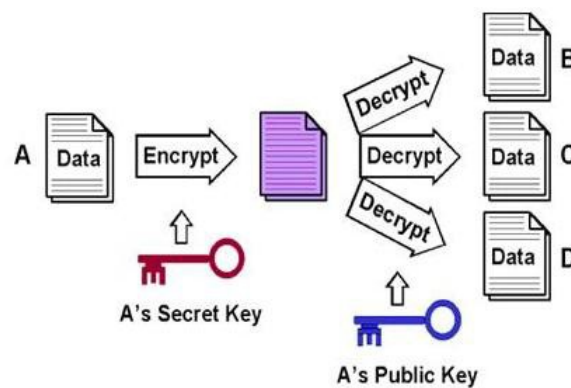


Fig 6. Diagram for cryptography concept



Fig 7. Working process of cryptography

B. Type

1) Symmetric-key cryptography:

In cryptography, symmetric-key techniques are those in which both the sender and the receiver use the same key to encrypt information (or, less commonly, in which their keys are different, but related in an easily computable way)

2) Public-key Cryptography:

Unlike with private-key cryptosystems, where the public key can be freely transmitted, public-key cryptosystems need the private key to be kept hidden. An encryption system that uses public keys is one in which the public key is used for encryption, while the private or secret key is used for decoding.

WIRELESS NETWORK SECURITY

Wireless security refers to the prevention of unwanted access to or damage to computers that are connected to a wireless network.

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the two most common types of wireless security to be found (WPA). Due to the fact that WEP is a notoriously insecure security standard, wireless networking is susceptible to a number of security issues. Cybercriminals have discovered that wireless networks are

relatively easy to break into, and they have even used wireless technology to hack into wired networks in some cases. Consequently, it is critical for businesses to develop effective wireless security policies that protect against unauthorised access to critical resources on their networks. To enforce wireless security policies, Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are frequently used in conjunction with one another.

A. The Existing Threat Situation

Wireless security is only one aspect of computer security; however, organisations may be particularly vulnerable to security breaches caused by rogue access points because of their reliance on wireless technology. If an employee (or other trusted entity) brings in a wireless router and plugs it into an unprotected switch port, the entire network can be exposed to anyone who comes within range of the wireless signals. As another example, a networked computer with a wireless interface that is connected through an open USB port may be compromised, which could result in access to confidential materials being gained by an intruder.

B. The possibility of air interface and link corruption.

As a result of the high level of effort required to maintain communication and the high level of effort required to intrude, there were relatively few dangers when wireless technology was first introduced. The variety of risks that wireless technology users face has grown in recent years as the service has become more popular and the technology has become more widely available. Today, there are a large number of security risks associated with current wireless protocols and encryption methods, owing to user carelessness and ignorance, as well as at the corporate IT level. Hacking methods have also become much more sophisticated and innovative as a result of wireless technology's proliferation.

C. The concept of wireless network prevention:

- For closed networks (such as those used by home users and businesses), the most common method is to configure access restrictions in the access points themselves. Encryption and checks on the MAC address are two examples of restrictions that may apply. Wifi Intrusion Prevention Systems (WIPS) may be utilised to

provide wireless LAN security in this type of network configuration.

- For commercial providers, hotspots, and big businesses, having an open and unencrypted wireless network that is totally segregated from the rest of the network is frequently the ideal approach. The users will initially have no access to the Internet or other local network resources since they will be unable to connect to the network. Commercial providers often route all web traffic through a captive gateway that accepts payments and/or authorises transactions. Another option is to require users to connect securely to a privileged network through the use of a virtual private network (VPN).

The security of wireless networks is inferior to that of wired networks; in many offices, intruders can easily visit and connect their own computer to the wired network without difficulty, thereby gaining access to the network; it is also frequently possible for remote intruders to gain access to the network through backdoors such as Back Orifice. Using end-to-end encryption in conjunction with independent authentication on any resources that should not be accessible to the public may be a good overall solution.

D. Security Measures:

SSIDhiding: Hiding the SSID is a simple but unsuccessful way to try to safeguard a wireless network (Service Set Identifier). This provides only rudimentary security against all but the most innocuous intrusion attempts[6].

MAC ID filtering: One of the most basic approaches is to allow access only from pre-approved MAC addresses. MAC ID filtering is included in most wireless access points. An attacker, on the other hand, can easily sniff the MAC address of a trusted client and impersonate it.

Static IP Addressing: DHCP is used by most wireless access points to assign IP addresses to clients. Requiring clients to provide their own addresses makes it more difficult for an intruder to connect onto the network, but it offers little security against a clever attacker [7].

E. Mobile Devices: As the number of mobile devices using 802.1x interfaces grows, so does the security of these devices. While open standards such as Kismet are aimed at protecting laptops, access point solutions should also provide coverage for mobile devices. Host-based solutions featuring an 802.1x interface for mobile phones and PDAs.

There are three types of security on mobile devices:

1. Protecting against ad hoc networks is number one.
2. Establishing connections with rogue access points
3. Wireless IPS solutions now provide wireless security for mobile devices using mutual authentication approaches such as WPA2, as explained above.

Mobile patient monitoring devices are becoming an increasingly important aspect of the healthcare business, and they will eventually become the preferred means of obtaining and executing health checks for patients in rural regions. Security and dependability are crucial for these sorts of patient monitoring systems since they can impact a patient's state and, if compromised, might keep medical practitioners in the dark regarding the patient's status.

CONCLUSION

We've learned that computer and internet security are essential in today's world. There are far too many attackers out there attempting to obtain personal information from their victims. As a network user, you should be aware of ways to avoid or defend oneself from being hacked or

experiencing data loss. We may defend ourselves from intruders and viruses by utilising effective net-protection and antivirus software. Nowadays, one of the most pressing issues is computer security and privacy.

REFERENCES

1. R.D. Atmaja, M.A. Murti, J. Halomoan, and F.Y. Suratman, "An Image Processing Method to Convert RGB Image into Binary", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 3, No. 2, 2016, pp. 377-382. DOI: 10.11591/ijeecs.v3.i2.pp377-382.
2. Computer networks (4th edition), Andrews Tabebaum, Data management, Search engine.
3. E-tutorials.org, computer privacy and security.
4. Wikipedia.org, E-commerce, Cryptography and Wireless network security.
5. www.ipc.on.ca, Computer security and privacy diagrams.
6. www.istockphoto.com