Transactions on Computer Systems and Networks

Sandeep Saxena
Ashok Kumar Pradhan *Editors*

Internet of Things

Security and Privacy in Cyberspace

Springer

Transactions on Computer Systems and Networks

Series Editor

Amlan Chakrabarti, Director and Professor, A. K. Choudhury School of Information Technology, Kolkata, West Bengal, India

Transactions on Computer Systems and Networks is a unique series that aims to capture advances in evolution of computer hardware and software systems and progress in computer networks. Computing Systems in present world span from miniature IoT nodes and embedded computing systems to large-scale cloud infrastructures, which necessitates developing systems architecture, storage infrastructure and process management to work at various scales. Present day networking technologies provide pervasive global coverage on a scale and enable multitude of transformative technologies. The new landscape of computing comprises of self-aware autonomous systems, which are built upon a software-hardware collaborative framework. These systems are designed to execute critical and non-critical tasks involving a variety of processing resources like multi-core CPUs, reconfigurable hardware, GPUs and TPUs which are managed through virtualisation, real-time process management and fault-tolerance. While AI, Machine Learning and Deep Learning tasks are predominantly increasing in the application space the computing system research aim towards efficient means of data processing, memory management, real-time task scheduling, scalable, secured and energy aware computing. The paradigm of computer networks also extends it support to this evolving application scenario through various advanced protocols, architectures and services. This series aims to present leading works on advances in theory, design, behaviour and applications in computing systems and networks. The Series accepts research monographs, introductory and advanced textbooks, professional books, reference works, and select conference proceedings.

More information about this series at https://link.springer.com/bookseries/16657

Sandeep Saxena · Ashok Kumar Pradhan
Editors

Internet of Things

Security and Privacy in Cyberspace

Springer

Editors
Sandeep Saxena
Director-IQAC and Professor-IT
IMS Unison University
Dehradun, Uttarakhand, India

Ashok Kumar Pradhan
Department of Computer Science
and Engineering
SRM University
Amaravati, Andhra Pradesh, India

ISSN 2730-7484 ISSN 2730-7492 (electronic)
Transactions on Computer Systems and Networks
ISBN 978-981-19-1584-0 ISBN 978-981-19-1585-7 (eBook)
https://doi.org/10.1007/978-981-19-1585-7

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Contents

Editors and Contributors

About the Editors

Prof. (Dr.) Sandeep Saxena working as a Director-IQAC and Professor-IT in IMS Unison University, Dehradun, Uttarakhand, India. He has received his Ph.D. degree in CSE from NIT Durgapur, West Bengal. He has received his MS degree in Information Security from the Indian Institute of Information Technology, Prayagraj. He has received his B.Tech degree in CSE from U.P.T.U. Lucknow. He has more than 13 Years of Teaching and Research Experience. His areas of interest and research include Security and Privacy in Blockchain Technology and Cloud Computing, Architecture Design for Cloud Computing, Access control techniques in Cloud Computing, and Blockchain Technology.

He has performed the role of a key member in more than 10 International Conferences as Keynote Speaker/Organizing Secretary/Organizing Chair/Session Chair. He has written 3 technical books for UP Technical University, Lucknow, and published multiple research papers in reputed international journals and conferences. He has published more than 30 research papers in reputed peer-reviewed journals/conferences indexed by (Scopus, SCIE, Google Scholars, DBLP) with high impact factors, more than 10 Patents published, and 2 Patents are Granted. He is participating in multiple professional societies like IEEE (Senior Member), IAASSE (Senior Member), Life Time Member in CSI, and Life Time Member in CRSI.

Ashok Kumar Pradhan is an Associate Professor in the Department of Computer Science and Engineering, School of Engineering and Applied Science at SRM University, Amaravati. He received his M.Tech. degree from the National Institute of Technology (NIT), Rourkela, India, in 2010. He received his Ph.D. degree from NIT Durgapur, India, in 2015. His areas of interest and research include security and privacy in blockchain-based IoT, architecture design for blockchain-based IoT, access control techniques in blockchain-based IoT, blockchain-enabled ecosystem in healthcare, agriculture, and supply chain, experimental prototyping, and testbeds

for blockchain-based IoT. He has published over 20 research papers in reputed peer-reviewed journals and conferences. He is a lifetime member of cryptography and security and the Indian science congress association.

Contributors

Pradeep Kumar Arya Department of Computer Science, BML Munjal University, Gurgaon, India

Sunil Kumar Bharti Galgotias College of Engineering and Technology, Greater Noida, India

Prachi Dahiya Delhi Technological University, New Delhi, India

Kunal Das Acharya Prafulla Chandra College, Kolkata, WB, India

Bhaskara Santhosh Egala SRM University, Amaravati, Andhra Pradesh, India

Goldie Gabrani Department of Computer Science and Engineering, BML Munjal University, Gurgaon, India

S. B. Goyal City University, Petaling Jaya, Malaysia

Shubham Gupta Department of Computer Science and Engineering, SRM University, Amravati, Andhra Pradesh, India

Sunil Gupta Department of Cybernetics, School of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, India

Bharathi V. Kalghatgi ECE Department, Pes University, Bangalore, India

Sahil Kansal Galgotias College of Engineering and Technology, Greater Noida, India

Umang Kant Delhi Technological University, Delhi, India

Inderpreet Kaur Galgotias College of Engineering and Technology, Greater Noida, India

Vinod Kumar Delhi Technological University, Delhi, India

Sushma Malik Institution of Innovation in Technology & Management, Janakpuri, New Delhi, India

Yahye Adam Omar City University, Petaling Jaya, Malaysia

Ashok Kumar Pradhan SRM University, Amaravati, Andhra Pradesh, India

Anamika Rana Maharaja Surajmal Institute, Janakpuri, New Delhi, India

Arindam Sadhu Maulana Abul Kalam Azad University of Technology, Kolkata, WB, India;
Greater Kolkata Engineering and Management, Kolkata, WB, India

Sandeep Saxena Director-IQAC and Professor-IT, IMS Unison University, Dehradun, Uttarakhand, India

Rishi Raj Singh School of Computer Science UPES, Dehradun, India

Manish Thakral School of Computer Science UPES, Dehradun, India

Raveena Yadav Delhi Technological University, Delhi, India

Chapter 1
Pre-requisite Concepts for Security and Privacy

Inderpreet Kaur, Sunil Kumar Bharti, and Sandeep Saxena

1.1 Principles of Cryptography

We need to preserve records of everything that happens in our lives. In other words, information could be a valuable asset a bit like the other. Information must be safeguarded against cyber-attacks because it is a valuable asset. In order to be safe, information must be protected against illegal access (confidentiality), protected from unlawful change (integrity), and accessible only to authorize parties when needed (availability) (Failed 2019; Hambouz et al. 2019) (Fig. 1.1).

1.1.1 Confidentiality

The most common feature of information security is confidentiality. We must safeguard our private information. An organization must protect itself against actions that jeopardize the confidentiality of its critical data. Confidentiality of data usually refers to it being known to only approve user data. Confidentiality is an important layer of data security. Control of confidential information is the major worry in the military. The operation of an organization necessitates the concealment of some information from others. It ensures that confidential information can be accessed only by an authorized person and should be reserved away from all those who are not authorized to access them.

I. Kaur · S. K. Bharti
Galgotias College of Engineering and Technology, Greater Noida, India
e-mail: Inderpreet.kaur@galgotiacollege.edu

S. Saxena (✉)
Director-IQAC and Professor-IT, IMS Unison University, Dehradun, Uttarakhand, India
e-mail: sandeep.research29@gmail.com

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_1

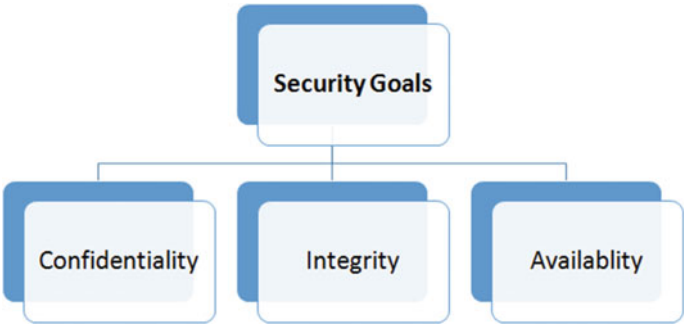

Fig. 1.1 Taxonomy of security goals (https://www.includehelp.com/cryptography/introduction.aspx)

Confidential data means the data can only be accessed by that user only to whom it belongs.

For example, in banking the account details of customer need to be kept undisclosed. Only account holder can view their bank account summary. Only account user is allowed to access the bank account details like bank statement, available balance, etc. Others cannot have right to use these bank details. Hence, this data is called confidential data.

The confidential data have two related concepts, namely data confidentiality and privacy.

Data confidentiality: This phrase ensures that confidential or sensitive information is not disseminated with unauthorized entities.

Privacy: The most popular understanding of privacy evokes feelings of withdrawal, seclusion, secrecy, or being hidden from public view, but without any negative undertone.

A collapse of confidentiality is the illegal confession of information. Confidentiality extends not just to information storage, but also to information transmission. When a piece of information is conveyed, it is referred to as a piece of data. It must be saved on a remote computer, and when data from a remote computer is retrieved, it must be wrapped during transmission.

Confidentiality ensures that no unauthorized users have access to the information shared. Applications, processes, other systems, and/or humans could all be users. When designing a system, make sure there are enough control devices in place to enforce confidentiality, as well as policies that dictate what authorized users can and cannot do with the data. Data must be protected within and outside the automotive, when it is stored (data at rest), sent (data in motion), and processed, in order to maintain confidentiality in automotive systems (data in use). Data in use can be protected with memory protection. Cryptography is excellent at safeguarding the

confidentiality of data in transit and at rest, but it adds computational complexity and increases latency; thus, it should be used with caution in time-critical applications.

Confidentiality with Symmetric Encryption

Symmetric encryption is a standard approach for ensuring data confidentiality when it is stored or transmitted. After that, the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), both block encryption approaches, are used (Martin 2011).

Strong passwords, multifactor authentication, data isolation, encryption, and assigning appropriate user permission levels to clients are just a few of the steps that can be taken to ensure confidentiality. However, before applying such controls, it is critical to divide your information resources into several groups based on the potential for loss if an unauthorized individual contacts them. The stronger the security rights, the greater the negative impact.

The common threats to confidentiality are:

Eavesdropping Attacks

Hackers intercept, destroy, or change data sent between two devices in eavesdropping attacks.

Spy, sometimes known as espionage or tracking, intercepts data transferred between devices across an unsecured network. Eavesdropping occurs when a client connects to an insecure network and transfers confidential business data to a coworker, to give a more thorough description.

Because data is transmitted via an open network, hackers can use a variety of methods to erase it (Ma et al. 2016).

Eavesdropping attacks are notoriously difficult to detect. Errors, unlike other types of network attacks, may not have a substantial influence on the operation of networks and equipment (Tugnait Oct. 2016).

Eavesdropping Methods

Hackers can use a variety of tactics to initiate attacks via eavesdropping. Multiple eavesdropping devices are typically used in these assaults to eavesdrop in conversations and network operations.

A hidden error that is actually installed in a workplace or house is a good example of an electronic eavesdropping device. Bugs may be hidden under a chair or on a table, or the microphone could be hidden in a common object like a bag or a pen. This is a straightforward procedure, but it may result in the installation of equipment that is more difficult to detect.

Although all the technological advances have made digital listening easier and easier, many attacks still rely on capturing phone calls. This is because the phone has electricity, a built-in microphone, hiding hole space, speakers, and it is easy to install holes quickly. An eavesdropper can verify the conversation in the room where the phone is located and call a phone anywhere in the world.

Modern computerized telephone systems can intercept calls electronically without directly touching the equipment. Hackers can send signals through the phone line

and listen in any discussion in the same room, even if the phone is not turned on. Similarly, computer systems include advanced communication devices that allow eavesdroppers to collect communication activities such as voice conversations, online chats, and even keyboards to convey what the user is typing.

In addition, computer systems produce electromagnetic radiation, which can be used by sophisticated intruders to rearrange the contents on the computer screen. These signals can travel hundreds of feet and then be pushed out farther using cables and telephone lines as antennas.

Pickup Device

To eavesdrop on the target, an attacker can utilize equipment that collect sound or images, such as microphones and cameras, and convert them to electronic representations. It should ideally be an electrical gadget that consumes the target room's energy so that the attacker does not need to enter the room to charge or replace the battery. Some listening devices have the ability to store digital data and send it to the listening station. Micro-amplifiers can also be used by attackers to reduce background noise.

Transmission Link

Eavesdropping can be done on the transmission link between the device and the attacker's receiver.

This can be accomplished through the use of radio frequency wiring or transmission, for example unused telephone wires, ungrounded wire conduits, or wires. Some transmitters can operate constantly, but more complex methods involve distant enabling.

Listening Station

A listening station is used to relay talks that have been intercepted due to telephone malfunctions.

After you pick up the phone to make or receive a call, the recorder is activated, and it switches off when the call is finished. An attacker can watch, record, or send signals for processing from a listening station, which is a secure location. It can be found just a few blocks away, in the next room or on the phone. Voice-activated equipment will be installed in the monitoring station, allowing it to listen in and record any action.

Weak Passwords

Attackers can easily get unauthorized access to user accounts with weak passwords, giving them access to company systems and networks. Hackers can interrupt secret communication lines, listen in colleagues' activities and chats, and steal confidential or valuable company data.

Open Network

Attackers can easily eavesdrop on users connected to open networks that do not require passwords and do not utilize encryption to send data. Hackers can track user activities and listen in network connections.

Encryption Cracking

Hackers employ encryption cracking tools to break the secrecy by attempting to overcome the network encryption used when delivering data, and data packets can be intercepted. The software's functionality varies depending on the hacker's goals. There are three basic encryption–decryption techniques, each of which decrypts sensitive data in a different way. IT firms in Ottawa can greatly improve network security for all clients and successfully defend against customer threats by understanding these tools (Al-Mohammed et al. 2020).

Traffic Injector

The traffic injector's main function is to inject encrypted communications into a network that have been forged by hackers. For traffic injection, there are two basic objectives. One is to send the recipient a new message, which normally occurs when the hacker has access to the decryption key for the message delivered to the user. Another goal of traffic injection is to retrieve encrypted and plain text messages. After that, the hacking tool compares the two messages to determine their meaning. Airplay and WepWedgie were the two tools employed in the most recent attack (Sala et al. 2021).

Decryption Tools

Decrypting messages usually necessitates the use of two tools. The first tool is used to gather the decryption packets. Today's prominent data packet gathering tools include Wireshark and Prism dump. The second tool examines the collected data packets in order to determine the encryption key. Although the most recent tools use simple algorithmic procedures to decrypt data packets, the tools that collect the data packets are responsible for the majority of the burden. To evaluate and decrypt the key, at least 5 million frames are necessary.

Brute-Force Attack Tools

Brute-force attacks are interested in collecting data packets and attempting to decipher the encrypted code using a large number of key dictionaries stored in it. Until the correct key is found or all keys have been used, the software attempts to decode the data packet with the key. A dictionary-based attack is another name for this type of assault. Decryption takes a lengthy time with brute-force attack methods, ranging from a few days to a few weeks. To function properly, they also necessitate sophisticated CPUs and other resources. The brute-force assault tool Air Snort is widely used (Bhowal et al. 2017).

For example, companies that provide computer services in Ottawa must ensure that their customers are protected against decryption tools by researching them and applying various techniques to ensure that messages carried across the customer's network are not disrupted or modified.

1.1.2 Integrity

Information must be updated on a regular basis. When a client deposits or withdraws money from a bank, the balance of her account must be updated. Changes must be made by authorized individuals and through permitted procedures in order to maintain integrity. Integrity violations are not always the consequence of malevolent behavior; a system disruption, such as a power surge, can also cause undesirable changes in data. Integrity refers to ensuring that data is accurate, full, trustworthy, and in its original form. Data that is missing or damaged can cause more harm than benefit.

Information integrity measures protect data from illegal alterations. These safeguards ensure that the data is accurate and trustworthy. Data kept in the system as well as data exchanged between systems, such as email, must be protected. It is not only required to limit access at the system level in order to maintain integrity, but also necessary to ensure that system users can only change information that they have been legally permitted to change.

Data integrity protection, like confidentiality protection, extends beyond the limits of vandalism. Accidental changes, such as human errors or data loss due to system failures, should also be prevented by effective integrity countermeasures. The financial industry must ensure that transactions on their systems are not manipulated with, even though all system owners must have confidence in the integrity of their data. In February 2016, cyber thieves fraudulently took $ 1 billion from the Central Bank of Bangladesh account at the Federal Reserve Bank of New York, in one of the most egregious recent breaches of financial data integrity. The hackers devised a well-thought-out strategy that included gaining the necessary credentials to make withdrawals, infecting the banking system with malware, destroying the transfer database records, and suppressing the confirmation messages to alert banking authorities to fraud. The majority of the transfers were halted or payments were recovered after the plan was detected, but the crooks were still able to make more than US $ 60 million. Integrity can be protected with a variety of countermeasures. Unauthorized users are prevented from making unauthorized access with access control and strong authentication. Hash checking and digital signatures can assist confirm that the transaction is genuine and that the file has not been tampered with. Management controls, such as division of roles and training, are just as critical as data integrity protection (Failed 2020).

Integrity refers to the capacity to assure that the system and its data have not been tampered with in any sense. Data is protected via integrity protection, but the operating system, applications, and hardware are also protected from illegal access. Cyclic Redundancy Check (CRC) is well recognized in automotive systems for providing integrity protection against non-malicious or inadvertent errors; nevertheless, it is not effective for preventing deliberate data alterations. As a result, sensitive data must include a cryptographic checksum for integrity verification. Furthermore, measures must be built to detect when data or system integrity has been compromised and to restore the impacted systems or data to their original state (Xu et al. 2011).

For example if anyone sends a parcel from one place to another. The parcel should be received by the receiver in the same form in which it is sent. In this way, integrity works with data. The data that is sent by the sender should be accurate, complete, and reliable. No alteration should be there while transmitting the data from source to destination.

Imagine what can happen if an organization transfers an employee's salary to an incorrect account owing to corruption of the database holding all employees' account number. This can impact badly on employees' account. This can happen because employee's database was not integrated.

The integrity relates two terminologies together which are as follows:

Data integrity: Assures that only specific and permitted changes are made to information and applications.

System integrity: Assures that a system performs its intended purpose without being harmed by intentional or unintentional unauthorized tampering (IEEE Approved Draft Guide for Engineering 2019).

Integrity refers to safeguarding against unauthorized information change or deletion, as well as ensuring non-repudiation and validity. The unlawful change or destruction of information is referred to as a loss of integrity.

Examples of allergy information from hospital patients kept in the database demonstrate the many features of completeness. The doctor must have confidence that the data is accurate and up-to-date. Assume that an employee with access to read and edit this information (for example, a nurse) purposefully falsifies data in order to ruin the hospital. The database must be rapidly restored to a stable state, and the error must be traced back to the person in authority. Information on a person's allergies is an example of a valuable asset that must be kept safe. Incorrect information can lead to significant fatality to the patient, putting the hospital underneath a lot of pressure (Sterpin et al. 2013).

A website that provides a forum for registered users to discuss particular topics, for example, may be labeled as an asset with a medium integrity criterion. Hackers or registered users can alter or destroy data on the website. The potential harm is minimal if the forum exists solely for the entertainment of its users, makes little to no advertising revenue, and is not used for critical purposes such as research. Webmasters may lose data, money, and time as a result of the attack. Anonymous Internet voting is an example of a system with low integrity requirements. Users can take these polls on many websites, including media organizations.

The following are some of the issues that could jeopardize the integrity of your data:

- Human error
- Compromising a system that lacks end-to-end encryption
- Physical device compromise

1.1.3 Availability

The availability of information is the third component of information security. The information that the organization creates and stores must be accessible to authorized parties. If the information is not readily available, it is pointless. Information must be updated on a regular basis, which necessitates that authorized parties have access to it. Information scarcity is just as destructive to a business as a lack of secrecy or integrity.

When a user enters data into a computer system, availability ensures that the data is available to the user when they require it. Users must have access to computer resources whenever they need them. It ensures that systems are up and running quickly and that authorized users are not refused service (Kang et al. 2014).

Consider the impact on a bank if consumers were unable to access their accounts for transactions. The more important the component or service, the higher the level of availability required.

Consider a system that enables essential systems, applications, and devices to be authenticated. Customers have been unable to access computer resources, and employees have been unable to access the resources required to execute key activities due to service outages. The loss of service translates into a significant economic loss in terms of employee productivity and possibly customer loss. The university's public website, for example, is frequently classified as a medium availability need because it gives information to existing and potential students as well as benefactors. Although such a site is not a critical component of the university's information system, its absence can be embarrassing. Low availability requirements will be assigned to online phone book search applications. Although losing an application for a short period of time can be inconvenient, there are other options for getting this information, such as printed catalog or operators.

In order for an information system to work, it must be accessible to authorized clients. Availability assessments ensure that users have access to the system at all times. Hardware failures, unplanned software downtime, and network bandwidth challenges are all examples of non-malicious threats to availability. Malicious attacks are a collection of several types of damage aimed at causing harm to an organization by denying clients access to the information system. Website availability and sensitivity are paramount for many companies. Even for short periods of time, disruption of website availability can lead to lost revenue, customer complaints, and reputation damage.

DoS (Distributed Denial of Service) attacks are a common way for hackers to interrupt web services. A DoS attack occurs when a hacker floods a server with unnecessary requests, overloading it and reducing service for legitimate users. Service providers have developed sophisticated defenses to identify and fight against DoS assaults over time, but hackers continue to evolve, and these attacks remain a threat. Only challenges to system availability have prompted widespread provisioning actions to protect system availability. Significant hardware redundancy and ready-to-use backup servers and data repositories are required for systems with high

continuous uptime requirements. It is typical to have redundant systems in separate physical locations for large enterprise systems. Software tools for monitoring system performance and network traffic are required. Firewalls and routers are two methods for preventing DoS attacks (Islam and Sabrina 2009).

The higher the level of availability required, the more significant the component or service. Consider a system that enables essential systems, applications, and devices to be authenticated. Customers have been unable to access computer resources, and employees have been unable to access the resources required to execute key activities due to service outages. The loss of service translates into a significant economic loss in terms of employee productivity and possibly customer loss.

1.1.4 Non-repudiation

To repudiate means to deny or contest something. Therefore, non-repudiation must be the ability to ensure that someone cannot deny or contest that thing. This is usually seen in electronic communications where one side denies seeing or signing a contract or paper or cannot be confirmed as the recipient. Non-repudiation means putting measures in place that will prevent one party from denying they received or agreed to a transaction.

1.2 Access Control

Authentication and authorization are the keys to access control. In terms of security, access management is vital (Bauer et al. 2005).

Access Control

It is "the process of approving or rejecting various requests." The following components are considered for this procedure:

- Who was the one who made the request?
- What is being asked for?
- Which rules apply when making a decision on the request?

To begin, the source of a request may be a specific computer, a machine in a specific configuration, or a specific application, such as an Android app.

Second, on a technological level, requests in a machine are issued by a process rather than a human. "For whom or for what is the method speaking while requesting?" the query is transformed into the phrase "what is asked" generally refers to a combination of an action to be performed and the object on which the action will be performed. This is accomplished through the usage of rules. Rules are logical formulations that are evaluated to provide a result. Allow or refuse is the choice.

Fig. 1.2 Relationship between identity, authentication, and access

Access Control (ISO/IEC 27,000, 2009) refers to the process of allowing and controlling access to assets based on business and security requirements. The practice of monitoring and regulating who has access to what systems, information, or data is known as access control. In almost all the cases, access must be restricted to people or computers who have been given authorization. To manage access based on rights, it generally follows the phases of identification, authentication, and authorization. By providing a log, for example, a better accountability method can achieve an entity's responsibility for its activities (Foley et al. 2011).

1.2.1 Identification

The procedure is recognizing or acknowledging a person or system. An identity will be checked during the identification procedure, which may or may not be true. A public piece of information, such as a username or an identification number, is usually provided by the subject (see Fig. 1.2).

1.2.2 Authentication

Authentication is the process of verifying that a user's identity is genuine. Most systems require a user to be authenticated prior to granting access to the system (Saxena et al. 2014). The user does this by entering a password, inserting a smart card, and entering the associated personal identification number (PIN), providing a biometric (e.g., fingerprint, voice pattern sample, retinal scan)—or a combination of these things—to prove they are who they claim to be. The credentials provided are compared to those that have previously been associated with the user. The credential match may be performed within the system being accessed or via a trusted external source. If the credentials match, the system authenticates the identity and grants access (see Fig. 1.2).

Authentication is defined by the International Organization for Standardization (ISO) as "providing assurance that a claimed attribute of an object is actual" (ISO/IEC 27,000, 2009).

In information security, a user is often identified by a username (public) and a password (private information). The username will be used to claim an identity, and the password will be compared to a previously saved user password to confirm the user's identity. The user is authenticated if the username and password match.

Biometric information, such as a fingerprint, or electrical technology, such as RFID tokens or smart cards, can also be used for identification and authentication. Different identifying approaches differ in terms of effort, dependability, and security. A combination of measures (multifactor authentication) may improve security and lower the danger of identity theft; for example, if an RFID tag is used to identify a person, the risk of identity theft is reduced.

The three general features (i.e., components) utilized to authenticate identification are as follows (Yuan et al. 2002).

1. Something the user owns or possesses (for example, a token or smart card)
2. Something the customer recognizes (a phrase or a PIN)
3. Something to which the user alone has access (e.g., biometric identification) (Crowe et al. 2004).

1.2.3 Authorization

It is the process of determining and approving authorized users' access permissions. It also describes what data and actions a properly identified and authenticated person or machine is permitted to access and perform.

1.2.3.1 Access Control Models

Access control models, which govern how individuals can access things, enforce the rules and goals of a given security policy. Here is a quick rundown of the three most common access control models.

1. **Discretionary Access Control (DAC)**: This model allows the owner or the creator who has created the item, such as a file, to control who has access to it and who does not. As a result, identity-based access control is another name for DAC (IBAC) (Li 2008).
2. **Mandatory Access Control (MAC)**: Categories are used in Mandatory Access Control (MAC) to identify what the subject (user) needs to know. When a person's clearance level is higher than or equal to the classification of an item, he or she has access to all of it (data or information). It is also known as a rule-based access control system (Zou et al. 2009).

3. **Role-Based Access Control (RBAC)**: The most generally used paradigm distributes permissions to a subject based on roles or groups. The resources that his or her group(s) or role(s) have access to will be available to the user. For example, an administrator might create a group for a job title or department-related rights and assign the appropriate personnel to it. As a result of this creation of group, administrative labor is decreased (Saxena et al. 2017).

1.2.3.2 Techniques of Access Control

The access control matrix is a system for linking a subject's access permissions to a specific item. It is one of the most commonly used mechanisms for access control. The rows reflect the user's capability table, while the columns represent the resource's Access Control List (ACL). The access rights and privileges that a user has resources on a system, such as files and directories, are identified using an Access Control List.

The following privileges are typical in an operating system and file system environment (Gattiker 2004):

- Read—to read a file or a directory's contents
- Write—to create or edit files/directories
- Execute—this command is used to run a file, such as a program.

1.2.3.3 Implementation of AAA

AAA establishes a uniform framework for managing who has access to a router, what services they can access, and what they can do with it. The sections below discuss the functions of AAA as well as how to activate it. AAA Functions AAA includes three basic components: authentication, authorization, and accounting.

AAA's authentication: This component is responsible for allowing users to be recognized (authenticated). Login access is an example, as are other types of access, such as PPP network access. When a user uses AAA authentication, you specify one or more authentication methods that the router should employ. You might, for example, provide two authentication methods: use an external security server if one is available and utilize the router's local username database if one is not (refer Fig. 1.3).

AAA's authorization: It is the process of implementing regulations by establishing what types of activities, resources, or services a user is permitted to engage in.

AAA's accounting: Accounting is the final component of the AAA architecture, and it keeps track of how much bandwidth a user uses while on the network. The amount of system time or the amount of data delivered and received during a session are examples of this. Accounting is done by keeping track of session statistics and consumption data.

AAA implementation: AAA may be implemented utilizing either the device's internal database or an external ACS (Access Control server) (Decugis 2009).

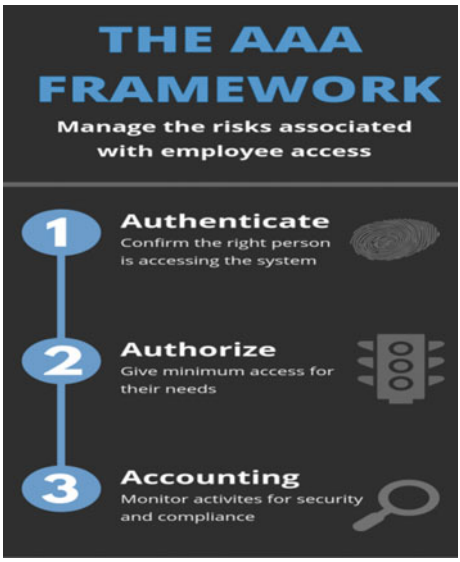

Fig. 1.3 AAA framework

- **Local database**—To implement AAA using the router or switch's local operational configuration, we must first create users for authentication and then give permission levels to those users for authorization.
- **ACS server**—This is the most often used technique. An external ACS server is utilized for both the router and the ACS must be configured, and AAA (which could be ACS hardware or software installed on VMware (Free Virtualization for Windows and Linux Servers)). The setup includes creating a user and a unique customization method list for authentication, authorization, and accounting.

The client or Network Access Server (NAS) makes an authentication request to the ACS server, which decides whether or not to provide the user access to the network resource based on the credentials given by the user.

The concept of virtualization has brought major changes on the concepts of authentication, authorization and accounting part of the business.

Important: If the ACS server fails to authenticate, the administrator should specify that the device's local database will be utilized as a backup in the method list.

AAA in Devices made by CISCO

There are two common methods defined by Cisco for implementing AAA services:

- **Local AAA Authentication**—For authentication, local AAA uses a local database. Self-contained authentication is the name given to this approach. It will be referred to as local AAA authentication in this course. Users authenticate against a local database in the Cisco router, which stores users and passwords. This is the same database that is required to set up the role-based CLI.

- **Server-Based AAA Authentication**—A server-based approach, such as the Cisco Secure Access Control System (ACS) for Windows, links the router to a central AAA server. All users' usernames and passwords are stored on the central AAA server. The router uses either the Remote Authentication Dial-In User Service (RADIUS) or the Terminal Access Controller Access Control System (TACACS+) protocol to connect to the PC with the AAA server. Server-based AAA is more suited when there are many routers and switches.

Once a user has been authorized, a session is established between the router and the AAA server.

The router requests authorization for the client's requested service from the AAA server.

Access Control Server (ACS) is used to provide a centralized administration system for the authentication, authorization, and accounting (AAA framework).

TACACS and RADIUS are the protocols used to communicate between the client and the ACS server.

1.2.4 Accountability

When someone logs into a network and begins working, their activities should be tracked. This can be assisted by a SIEM (Security Information and Event Management) or other auditing and monitoring technology. Knowing what files someone is looking at or attempting to access can assist establish whether more or less authorization is needed. Suspicious behavior may raise questions about whether the individual is trustworthy.

For this reason, all important system activities, events, and processes, such as failed and successful authentication attempts, are logged. An audit trail, also known as an information audit, is a chronological record of system operations that can be used to reconstruct and analyzes the actions of a system.

There are many different forms of network assaults, such as loop attacks, chain attacks, and doorknob attacks. The accountability algorithms may be used in conjunction with distributed recognition to provide robust responsibility for every individual network movements. For accountability, the DRA algorithm can be employed.

1.3 Cryptography

- **plaintext**—the message as it was originally sent
- **ciphertext**—a message that has been coded
- **cipher**—algorithm for converting plaintext to ciphertext
- **key**—information used in cipher that is only known by the sender/receiver
- **encipher (encrypt)**—converting plaintext to ciphertext

- **decode (decrypt)**—retrieving ciphertext from plaintext cryptography
- **Cryptanalysis (code breaking)—**study of the concepts and methods for decoding ciphertext without the knowledge of the key.
- **Cryptology**—Cryptography and cryptanalysis are both included in this field.
- Anyone who needs to verify the CA's statement of public-key ownership can utilize the public key.

Digital certificates, in contrast, still require a chain of trust to ensure that the certificate belongs to the person or organization you believe in and that it has not been tampered with. Criminals are accused of obtaining certificates and then using them to sign malware-infected software. Malicious software was detected.

Cryptography

The rapid advancement of cutting-edge Internet technology and data innovation has led to an increase in the number of individuals, businesses, and government offices joining the Internet. Which has resulted in an increase in the number of criminals attacking businesses by using fictitious websites and sending counterfeit messages? The focus of the assaults and interruptions on the organization is PCs, so if the gatecrashers succeed, a large number of organization PCs will be rendered inoperable. Additionally, a few trespassers with ulterior thought processes see the military and government division as the goal, posing enormous risks to social and public safety (Latif et al. 2020; Ahmad et al. 2009). Cryptography denotes "Covered up Secrets" is concerned with encryption. Cryptography is the study of frameworks for secure communication. It can be used to examine shows that are related to numerous aspects of information security, such as check, data grouping, non-disavowal, and data uprightness.

The study of writing secret codes is called cryptography. It is primarily concerned with the design and exploration of conventions that hinder opponents. Different views on data security, such as information confidentiality, information reliability, validation and non-repudiation, are very important for encryption today.

Two terms are of decisive importance in cryptographic calculation, they are as follows:

1. *Unconditional Security*

Regardless of the computing power or time available, the code cannot be decrypted because the ciphertext does not contain enough information to clearly identify the plain text.

2. *Computational Security*

The encryption cannot be broken due to inadequate computational resources (for example, the time required for calculations are larger than the age of the universe) (Sasubilli et al. 2020).

Cryptographic framework can be portraying by:

1. Type of encryption activities used:

That can be substitution or rendering of item.

2. Number of keys used

That can be single-key or private/two-key or public.

3. Way of plain text handling

The way plain text is either block or in the form of stream.

1.3.1 Symmetric Encryption

Symmetric and unbalanced encryption strategies are the most common approaches used to encode/ decrypt protected data. When symmetric encryption is required, the same cryptographic keys are used for text encryption and decryption of image content. Although symmetric-key encryption is faster and easier to use, it has the disadvantage of requiring both parties to relocate their shared key (Bani Baker and Al-Hamami 2017) refer Fig. 1.4.

To use symmetric encryption safely, there are two requirements:

- a robust and computationally infeasible encryption algorithm
- a secret key that is only known by the sender and receiver parties

Mathematically we have:

$$Y = E_K(X)$$
$$X = D_K(Y)$$

It assumes that encryption algorithm is known and implies a secure path to distribute key.

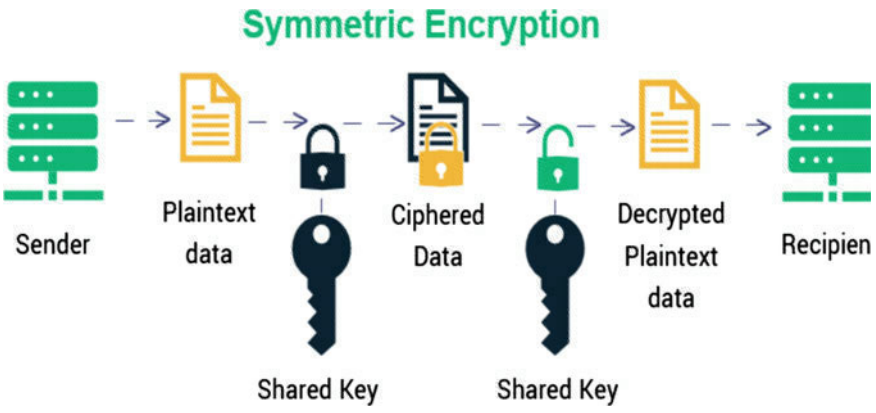

Fig. 1.4 Symmetric encryption

Types of symmetric-key algorithms Symmetric-key encryption:

1 **Classical Substitution Ciphers**

Plaintext letters are substituted with other letters, numbers, or symbols in this method. The well-known schemes under classical ciphers are Caesar Ciphers, Mono alphabetic Ciphers, Playfair Ciphers, Poly alphabetic Ciphers, Vigenère Cipher, Kasiski Method, Auto key Cipher, and One Time Pad (Failed 2014).

2 **Transposition Ciphers**

These methods hide the information by rearranging the order of the letters without changing the letters actually used; however, they are recognizable because they have the same frequency distribution as the original text. Types are Rail Fence cipher, Row Transposition Ciphers, Product Ciphers, Rotor Machines, and Hagelin Rotor Machine.

1.3.2 Asymmetric Encryption/Private Key Cryptography

Asymmetric encryption, commonly known as public-key cryptography, uses two keys. The two keys are a public key that is accessible to the general public and a private key that is only accessible to the user.

Message data is encrypted using a recipient's public key in public-key encryption. Anyone who does not have the coordinating private key will not be able to see the message. This is a privacy strategy (Failed 2014) (Fig. 1.5).

Public key was created to address two major concerns.

The *first* is key distribution, or how to establish secure communications without entrusting your key to a key distribution center (KDC). It does not require secure key distribution, and it does not require anyone else to know your private key.

Another concern is digital signatures, which are electronic stamps that ensure a communication is sent by the specified sender. In electronic stamps, a message is endorsed with the sender's private key, which can be reviewed by anybody who has access to the private key, ensuring the organization's security (Saxena et al. 2014).

Calculations based on public keys are based on two keys that have the following characteristics:

– It is computationally impossible to figure out the decoding key using only the calculation and encryption keys.

When the important (scramble/unscramble) key is known, it is computationally straightforward to encode/decode messages.

– For encryption, one of the two related keys can be used, while the other can be used for decoding (in certain plans) (Figs. 1.6, 1.7, 1.8)
– **Public-Key Cryptosystems showing Secrecy**

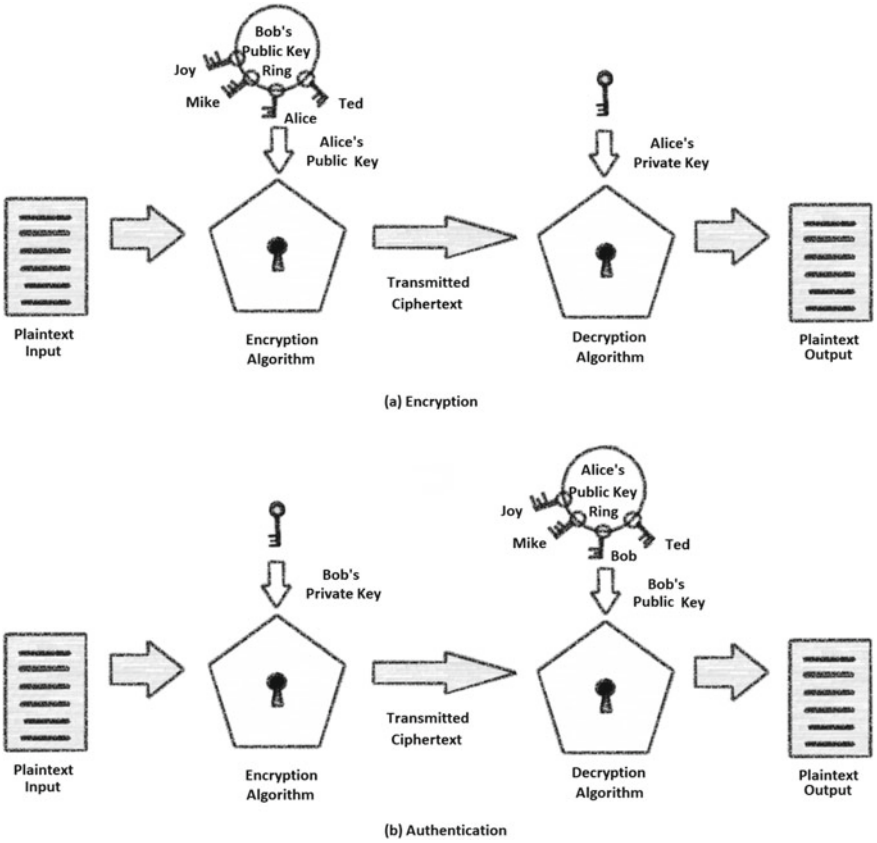

Fig. 1.5 **a** Encryption. **b** Authentication

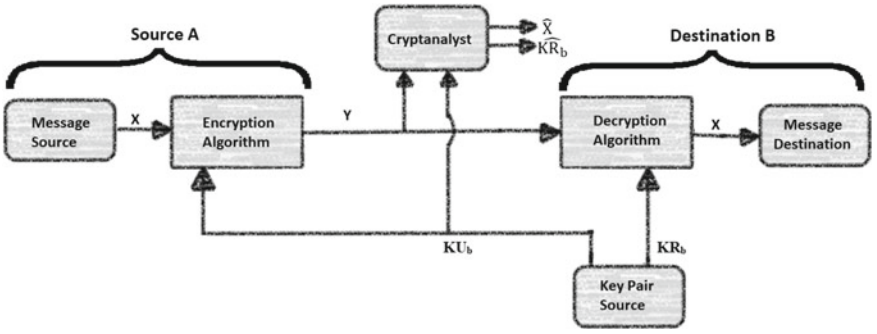

Fig. 1.6 Public-key cryptosystem showing secrecy

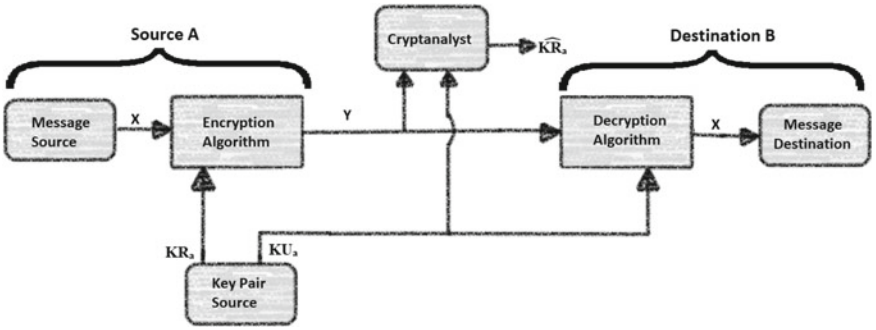

Fig. 1.7 Public-key cryptosystem showing authentication

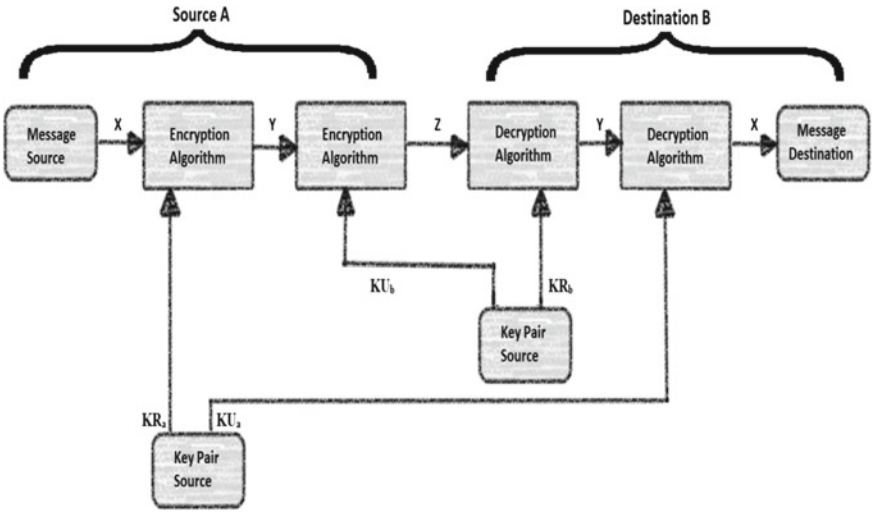

Fig. 1.8 Public-key cryptosystem showing secrecy and authentication

- **Public-Key Cryptosystems showing authentication**
- **Public-Key Cryptosystems showing Secrecy and Authentication**

An open key cryptosystem must meet following conditions:

1. With the appropriate key, encoding or translating a message is simple.
2. Inferring the private key from the open key is impossible.
3. Making a decision on the private key from a selected plaintext attack is impossible.

For the most part, these conditions ensure that scrambled data can be decoded with the appropriate private key. In today's world, three open key calculations are routinely used.