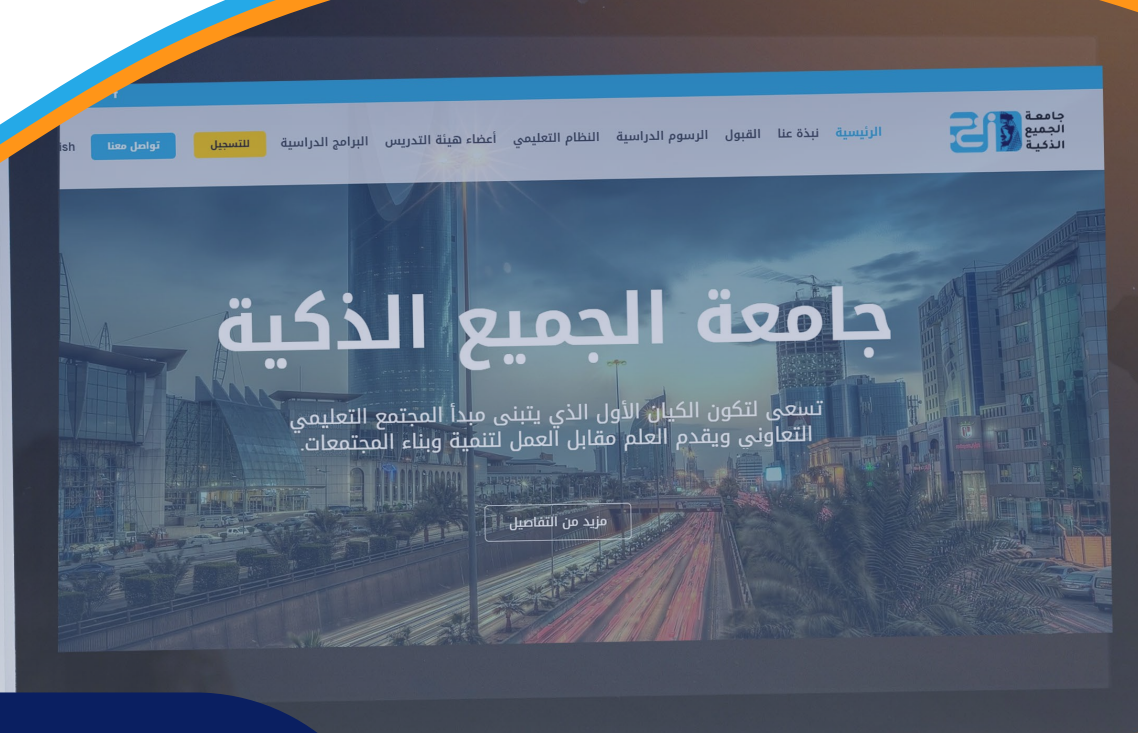




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



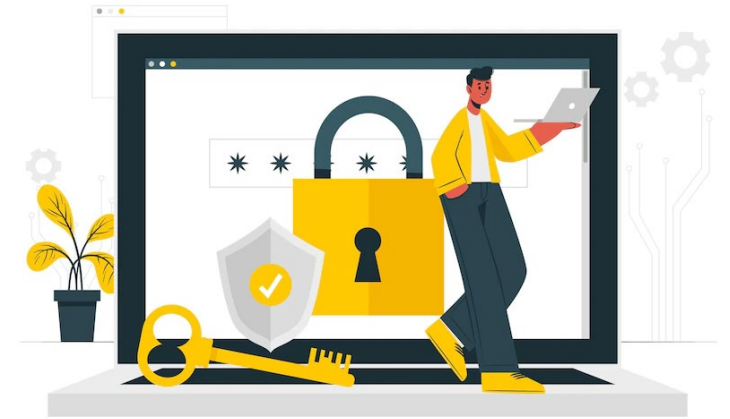
IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 9

Controlling Access & Security
of Data

Chapter 09

Cryptography

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.



Encryption and secrecy are absolute requirements of IoT deployments. They are used for securing communication, protecting firmware, and authentication. **Regarding encryption, there are generally three forms to consider:**

- **Symmetric key encryption:** Encryption and decryption keys are identical. RC5, DES, 3DES, and AES are all forms of symmetric key encryption.
- **Public Key encryption:** The encryption key is published publicly for anyone to use and encrypt data. Only the receiving party has a private key used to decrypt the message. This is also known as asymmetric encryption. Asymmetric cryptography manages data secrecy, authenticates participants, and forces non- repudiation. Well-know internet encryption and message protocols such as Elliptic Curve, PGP, RSA, TLS, and S/MIME are considered public keys.



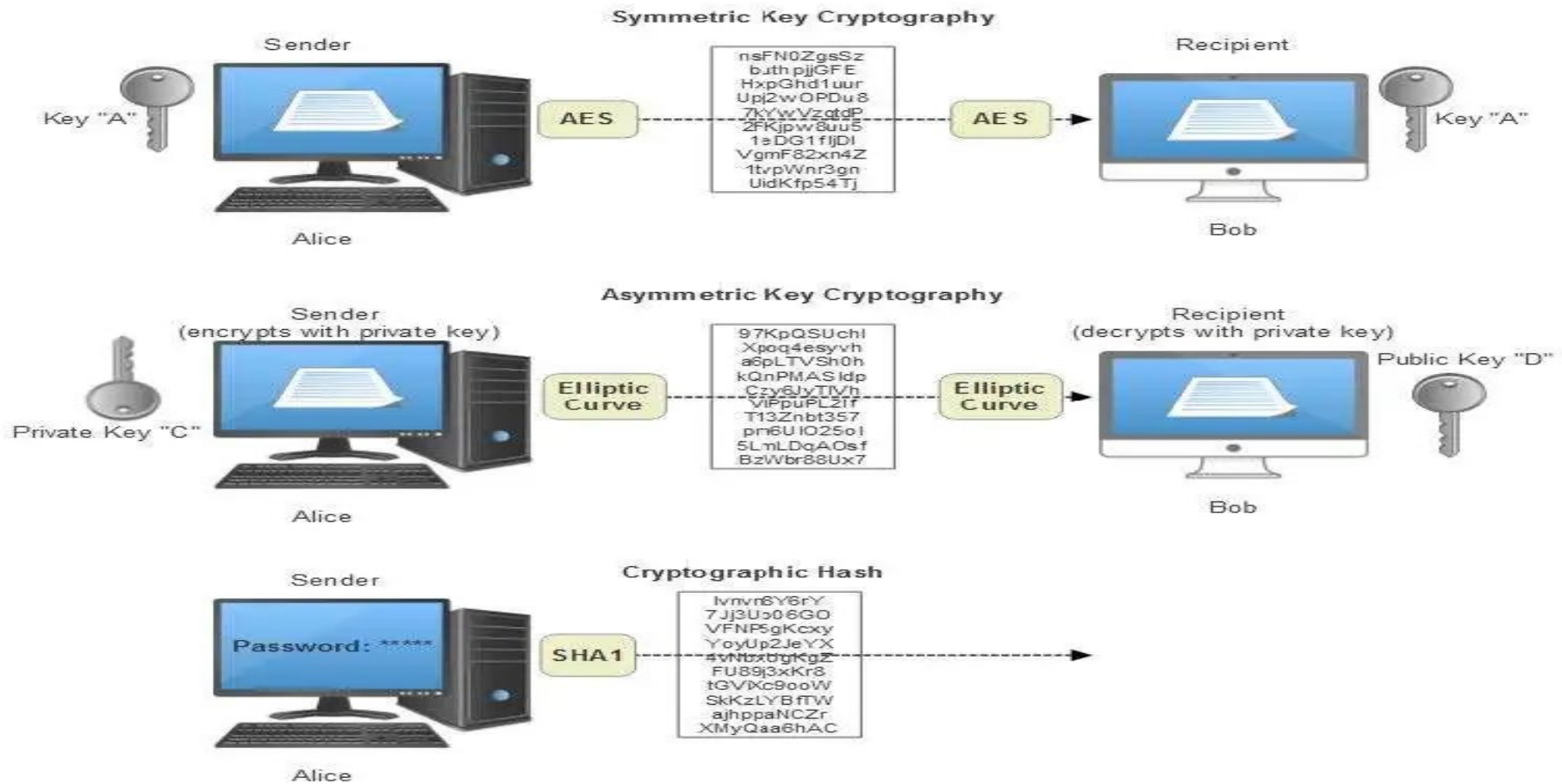
- **Cryptographic hash:** Maps data of arbitrary size to a bit string (called the digest). This hash function is designed to be “one way”. Essentially, the only way to recreate the output hash is to force every possible input combination (it cannot be run in reverse). MD5, SHA1, SHA2, and SHA3 are all forms of one-way hashes. These are typically used to encode digital signatures such as signed firmware images, message authentication codes (MAC), or authentication. When encrypting a short message like a password, the input may be too small to effectively create a fair hash; in that case, a salt or non-private string is appended to the password to increase the entropy. **A salt is a form of key derivation function (KDF):**

Elements of cryptography. The next slide contains the **symmetric, asymmetric, and hashing functions**. Note the key usage in symmetric and asymmetric cryptography. Symmetric has the requirement of using identical keys to encrypt and decrypt data. While faster than asymmetric encryption, the keys need to be secured.



Chapter 09

Cryptography in IoT



A secure system should provide several assurances such as **confidentiality, integrity, and availability** of data as well as **authenticity and non-repudiation**. When used correctly, crypto helps to provide these assurances.

Cryptography can ensure the confidentiality and integrity of both data in transit as well as data at rest. It can also authenticate senders and recipients to one another and protect against repudiation.

Software systems often have multiple endpoints, typically multiple clients, and one or more back-end servers. These client/server communications take place over networks that cannot be trusted. Communication occurs over open, public networks such as the Internet, or private networks which may be compromised by external attackers or malicious insiders.



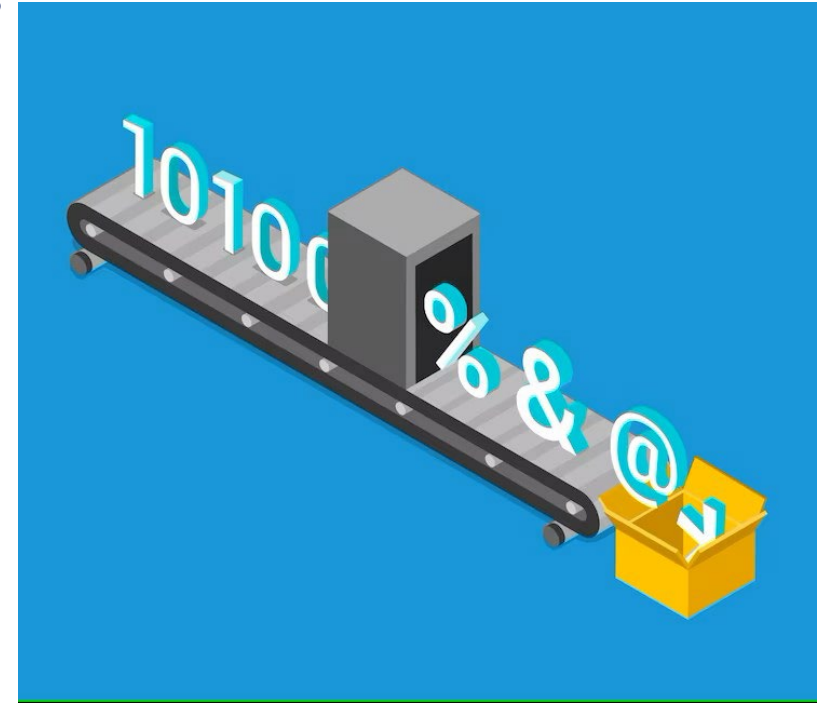
It can protect communications that traverse untrusted networks. **There are two main types of attacks that an adversary may attempt to carry out on a network:-**

1. Passive attacks involve an attacker simply listening on a network segment and attempting to read sensitive information as it travels. Passive attacks may be online (in which an attacker reads traffic in real-time) or offline (in which an attacker simply captures traffic in real-time and views it later—perhaps after spending some time decrypting it).
2. Active attacks involve an attacker impersonating a client or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them on to their intended destination (or dropping them entirely).



The **confidentiality and integrity** protections offered by cryptographic protocols such as **SSL/TLS** can protect communications from malicious eavesdropping and tampering. Authenticity protections provide assurance that users are actually communicating with the systems as intended. **For example, are you sending your online banking password to your bank or someone else?**

It can also be used to protect data at rest. Data on a removable disk or in a database can be encrypted to prevent disclosure of sensitive data should the physical media be lost or stolen. In addition, it can also provide integrity protection of data at rest to detect malicious tampering.



Chapter 09

Data at Rest State

“Data at rest” is data that is not being used or transferred.

This means that the data is likely being stored on a hard drive, flash drive, or another device. The term can also refer to data stored in a cloud service, such as Microsoft Azure or Amazon Web Services (AWS). Data at rest is easier to secure, but thieves typically see this data as a more attractive target because there’s more of it to steal. Data at rest is also more vulnerable to malicious attacks from employees who have access to the storage network.



- **Keep Your Storage Organized**

Disorganized or unclassified data storage can create unnecessary vulnerabilities that hackers will exploit. Creating a well-maintained and well-documented storage system will help you to keep an eye on all of your information and to notice whether anything has been disturbed. Classifying your data based on how valuable or vulnerable it is will also help you to allocate your defense resources correctly.

- **Encrypt Your Data**

Data encryption translates your data into a code that is undecipherable to anyone without the correct encryption keys. Encrypting your data while it is stored means that even if unauthorized access happens, the encrypted data will not be of use to the thieves. Encryption is a powerful tool that can keep information from falling into the wrong hands.

- **Practice Due Diligence**

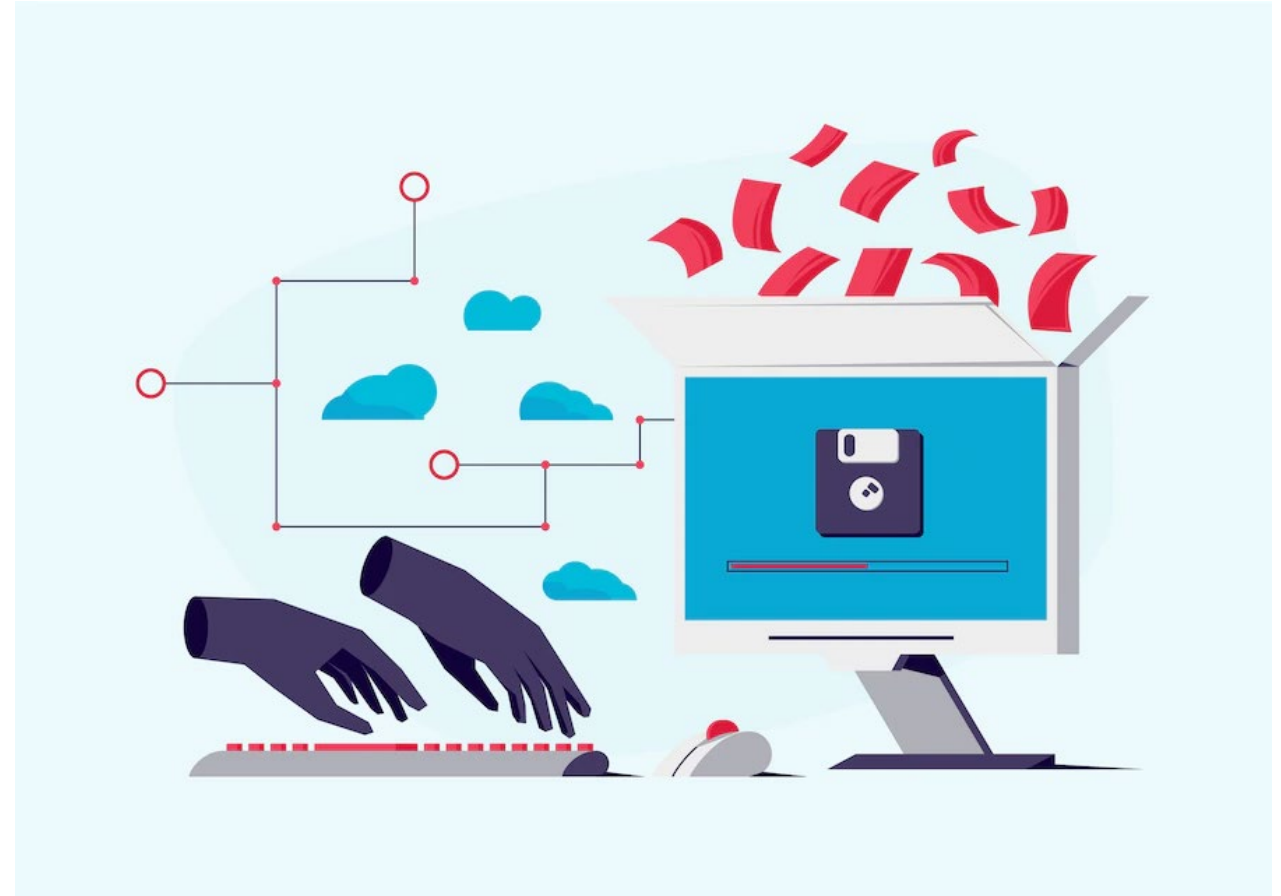
It's imperative that you understand where your data is stored and what safeguards are in place. If you're using cloud storage, your server will likely have a number of protections in place; those are a great addition to a strong defense strategy. Depending on these outside controls alone, however, can have disastrous results. Whatever cloud services you use, you still have a responsibility to create security controls for your storage and make sure the data is safe.



Chapter 09

Data at Motion State

This refers to data moving from one location to another, such as between two storage devices. This includes downloads, transfers, or any other means of taking data from one place to another. Of the three states, data in motion is by far the most vulnerable. In particular, Man in the Middle (MitM) attacks (where a malicious actor inserts himself into a transaction or transfer) are easier to execute with data in motion.



- **Secure Your Network**

Your company will need to access and transmit data to provide the best service for your clients; leaving critical data in storage is simply not an option. This means that your private network must be secured and protected so that data is safe while in transit. There are a variety of ways to secure your network, such as implementing firewalls or using encrypted connections and SSL certificates. Whatever method you choose, your goal should be to assure that no outside actors are able to see or acquire sensitive data while it moves within your company.



- **Restrict Access to Data**

An important part of data protection is knowing who has access to it and who is responsible for any transmissions. This means that restricting data access on a need-to-know basis and implementing access logs can help you track when data is being moved and who was responsible for moving it. If a breach occurs at this level, access control will make it easier to determine where it originated and what must be done to prevent future breaches.



- **Encourage Good Security Hygiene**

The safety of data transmitted within your company depends on the security of your staff's accounts. Usually, data will be transmitted via email or messaging apps, and your employees need to have unique names and strong passwords to keep that data secure. A multi-factor authentication is also a great option for protecting data, and your employees should be encouraged to implement such protection on their accounts. Endpoint security should also be a concern, and any laptops or mobile devices used by your staff must be secured. Training your staff on the importance of data security should be an integral part of your overall data management plan.



This refers to data being accessed or used at any given moment. If you are creating, deleting, editing, or processing your data, then it is “in use” until such time as it is stored (at rest) or transferred (in motion). Data is in use when it’s accessed or consumed by an employee or corporate application. Whether it’s being read, processed or modified, data is at its most vulnerable in this state because it’s directly accessible to an individual, making it susceptible to attack or human error – both of which can have significant consequences. Encryption is essential to protecting data in use, and many businesses will shore up their encryption solutions with additional security measures like authentication and permissions for data access.



- **Data controls start before use:** Protections for data in use should be put in place before anyone can access the information. Once a sensitive document has been compromised, there is no way to control what a hacker does with the data they've obtained.
- **Double down on identity management:** Identity theft has become increasingly popular, especially with people sharing more of their data online than ever. Identity management solutions help businesses ensure users are who they say they are before they access any documentation, reducing the risk of fraud.
- **Manage the right to access:** Whether they use digital rights protection, information rights management (IRM) or another method, leading companies use security solutions to limit the actions a user can take with the data they access. For instance, a manager may have full access to a confidential performance report, while their employees can only read the document, with no option to edit or share it with colleagues.



- **Reactive protection does not work:** Once a company's data is breached, the task shifts from protection to risk management and damage control. Instead of playing catch-up, businesses should identify which data is at risk and build proactive defense mechanisms to head off attacks before they materialize.
- **Smart classification equals smart protection:** By categorizing all of their data and understanding its risk profile in every state, companies will be in the best position to choose the most effective protection measures. Implementing automatic protocols will also ensure that accurate defense measures are triggered when data shifts between states, so that it always has the highest level of protection.

Data Backup



Access control and authorization can be important in all IoT application domains, in particular if the underlying IoT system and the services it provides are not meant to be publicly available or available for free. Clearly, one would not like to give free access to his home automation system to a stranger. Similarly, access to security and surveillance services should be restricted to the owner or the operator of the building or location being physically protected by those services. Industrial automation and process control systems are not supposed to be accessible for entities that are not part of the industrial facility or its contractors, and healthcare IoT systems must also be restricted to the patient and authorized medical staff. Transport and retail IoT systems are meant to be available to the public, but still certain parts of even those systems should be restricted to their operators. In the retail case, consumers should not have access to stock and order information of the retailer, whereas in the transport case, certain services should be authorized only to distinguished entities (e.g., to emergency vehicles).

Trustworthy computing is a general requirement, and it means that one must be assured that the system and its services work as expected by the user at any time and in all conceivable situations. It is also a fundamental requirement, as if it cannot be satisfied, then other requirements, such as proper access control and authorization, could not be satisfied either, or at least, one would never be sufficiently assured that they are enforced properly. This is because system and service level security requirements are typically satisfied by implementing security mechanisms on the underlying computing platforms, and those implementations should be trustworthy. More specifically, the trustworthy computing requirement means that the computing environment on which the system is running, and services are provided is difficult to corrupt by attackers. This covers the requirement to protect IoT devices from being hacked or infected by malware. In addition, trustworthiness requires assurance, which means that not only it is difficult to compromise system components, but it is possible to verify that the system is still in a healthy state, if it is, and if not, it can be brought back to a healthy state.

Denial-of-Service protection makes it difficult for attackers to render the services provided by the IoT system unavailable or substantially under-performing. This is a requirement similar to availability of information, but here we require availability of services rather than just information. Also, this requirement complements the trustworthy computing requirement in the sense that making it difficult for attackers to corrupt services (i.e., modify them) may not be sufficient to ensure that those services are available at all. In other words, system components may be intact, and hence, the service semantics may be unchanged, and yet the service may not be available. As an example, consider a typical DoS attack: the service is flooded with requests and overloaded, such that it cannot serve legitimate requests anymore. The service is still the same semantically, system components remained uncorrupted, yet the service became unavailable. Hence, the DoS protection requirement is needed besides the trustworthy computation requirement to fully express what we expect from a secure IoT system.

Protection against **DoS attacks** is important in all IoT application domains for two reasons. First, the very purpose of any IoT system is to provide some service; if this service can be rendered unavailable easily, then the entire IoT system becomes useless. Second, it is indeed rather easy to mount DoS type attacks against any kind of IT system, because such attacks do not need access to the system and corruption of the system components, as we explained above. As IoT systems consists of IoT devices that are often resource constraints, and they often operate in environments with special conditions, DoS attacks seems to be easier to carry out against IoT systems than against “traditional” IT systems.



Privacy means that human users can control how private information about them is stored, processed, and used in the IoT system and beyond. This requirement is relevant in application domains where the IoT system handles user related private information. This is not the case in industrial automation and process control applications, but privacy issues must be considered in all other IoT application domains. In home and office automation applications, generated data may reveal the users' behavioral habits, in security and surveillance applications, as well as in transportation applications, data may reveal the users' location, in retail applications, data may reveal user preferences towards certain types of products and also their shopping behavior, and finally, in healthcare applications, data may reveal the users' illnesses or other types of medical problems. Essentially, as IoT is meant to convert our everyday life easier by using embedded intelligence in everyday objects, it seems to be unavoidable that IoT systems observe humans and collect data about them.

Identify Needs to Protect IoT

Even if this data collection is not explicitly targeted to collect private information, whatever data such systems collect, it may contain a large amount of extractable private information. This is not a problem in itself if privacy preserving mechanisms are also provided to the users that help them to keep the control on how their private information is used by other entities. Hence, the privacy requirement does not postulate the complete elimination of obtaining private information from data generated by IoT systems, but rather it postulates the need for appropriate privacy preserving mechanisms, and a privacy-by-design approach whenever possible (e.g., in case of new systems just about to be created).



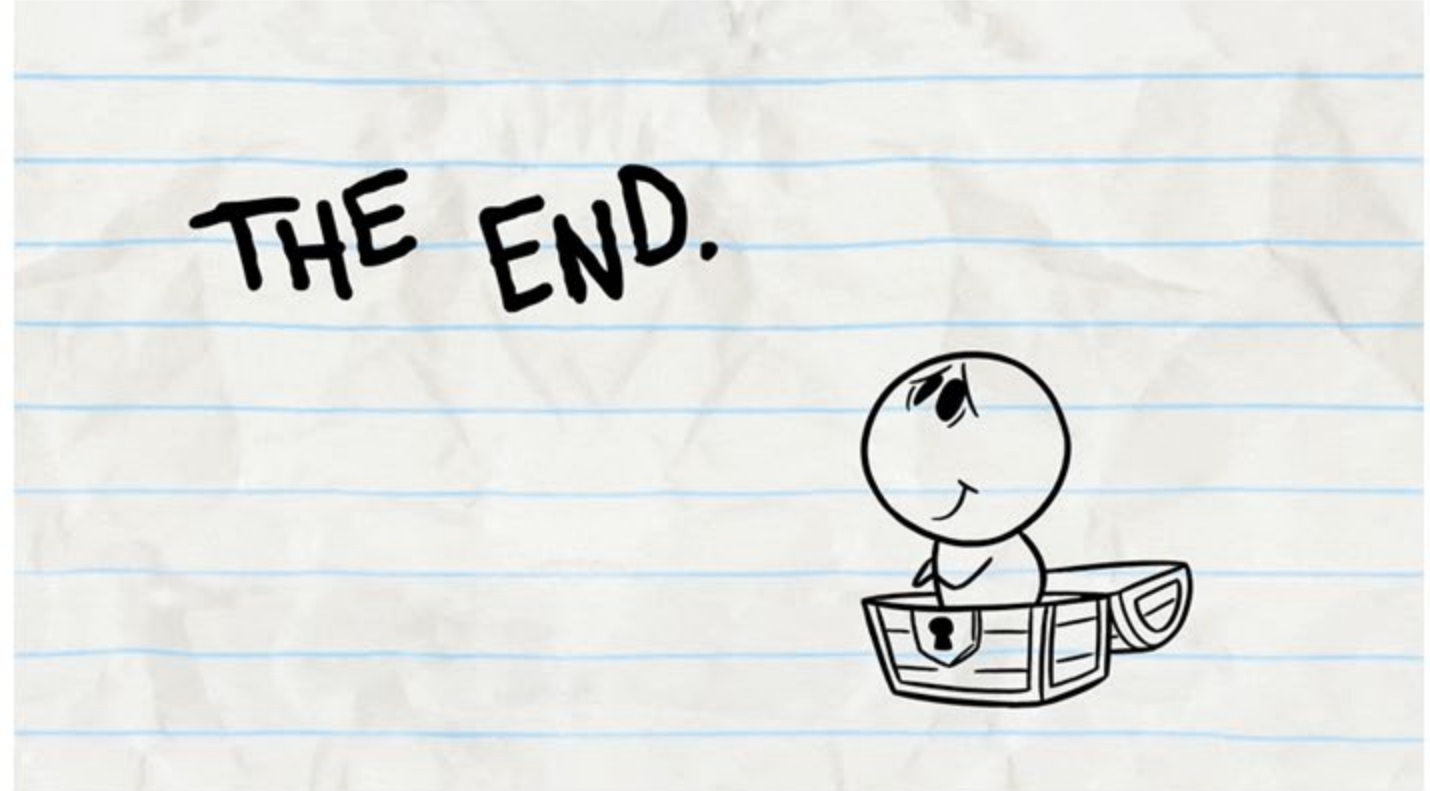
- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
- **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY