CHANDIGARH UNIVERSITY
Discover. Learn. Empower.

University Institute of Engineering
AIT-CSE

Privacy and Security in IoT - CSD- 433

Topic – Insufficient Authentication/Authorization,

Secrecy and Secret-Key Capacity , Transport Encryption

Lecture – 1.7

Delivered by

Er. Gaurav Soni (E9610)

Assistant Professor, AIT-CSE

DISCOVER . LEARN . EMPOWER

Privacy and Security in IoT

Course Objectives

CO Number	Title
CO1	To identify various privacy and security requirements in Internet of Things
CO2	To learn cryptographic techniques for a secure IoT system
CO3	To understand various Trust Models used in IoT

Privacy and Security in IoT

Course Outcome

CO Number	Title	Level
CO1	After successful completion of this course students will be able to understand the security requirements in IoT.	**Understand**
CO2	After successful completion of this course students will be able to understand the authentication credentials and access control.	**Understand**
CO3	After successful completion of this course students will be able to implement security algorithms to make a secure IoT system.	Implement

This will be covered in this lecture

INSUFFICIENT AUTHENTICATION/AUTHORIZATION

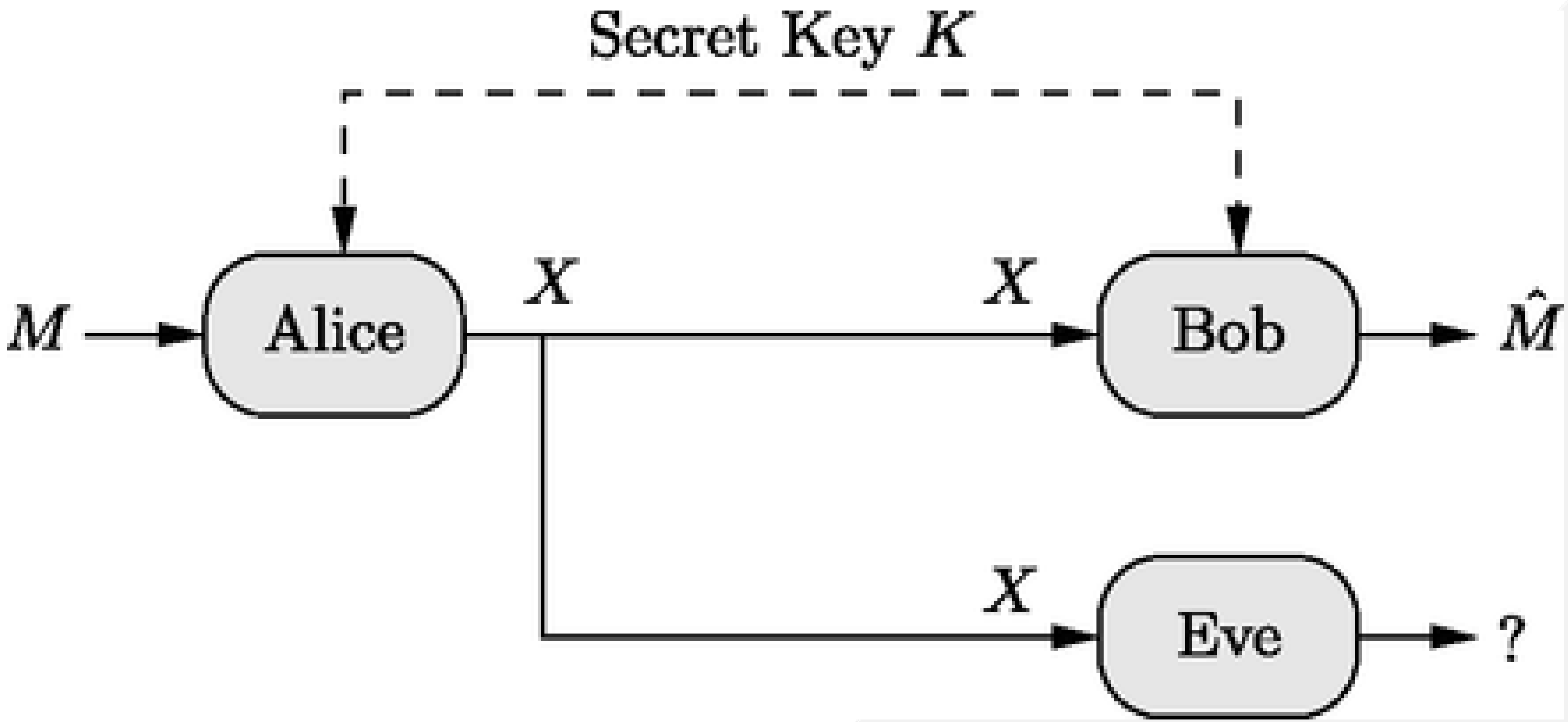
Security Challenges due to Insufficient Authentication/ Authorization

Individual - Unauthorized tracking of people's locations

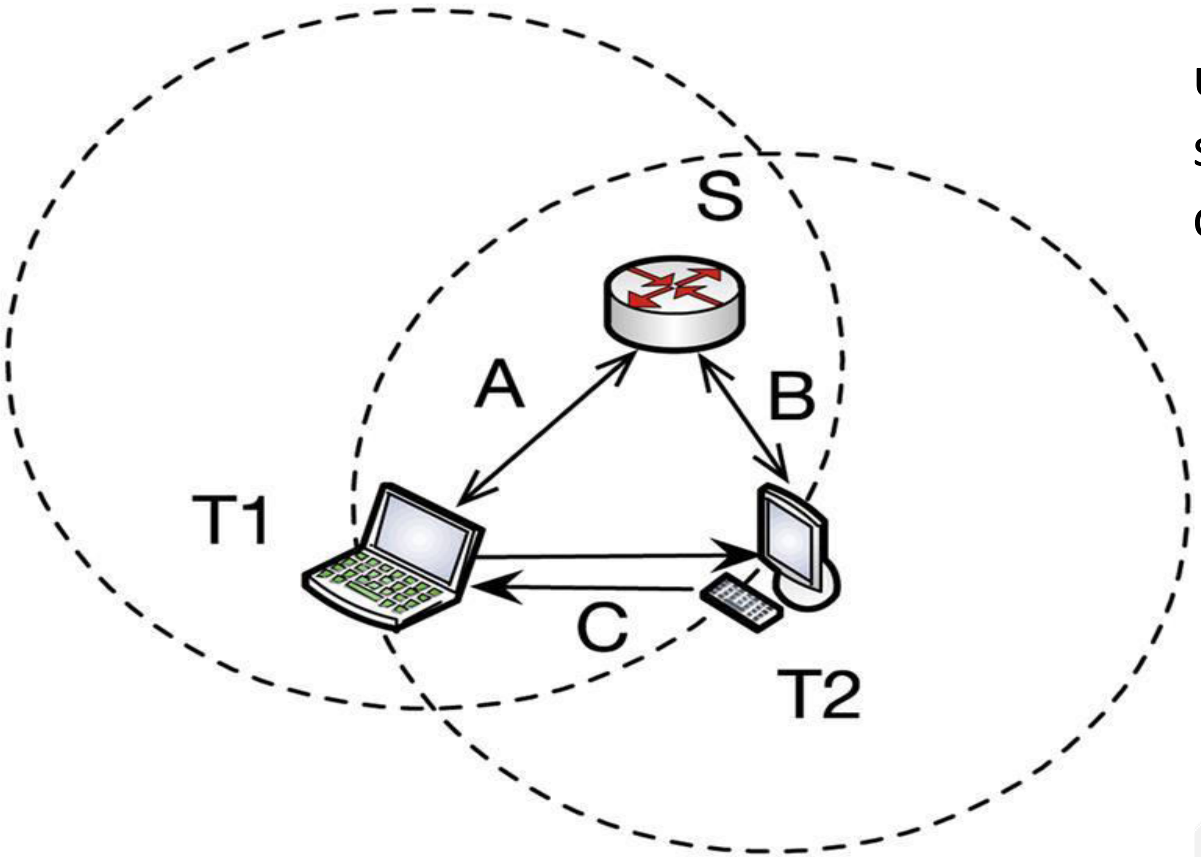
Business Area - Manipulation of financial transactions through unauthorized POS and POS access.

Ability to Access the IoT - Ability to gain unauthorized access to IoT edge devices to manipulate data by taking advantage of the challenges related to updating software and firmware of embedded devices (e.g., embedded in cars, houses, medical devices).

Shannon’s Cipher System- Secrecy and Secret-Key Capacity



Shannon’s Cipher System- Secrecy and Secret-Key Capacity



The confidential communication is impossible unless the Gaussian main channel has a better signal-noise rate (SNR) then the Gaussian wiretap channel.

Shannon’s Cipher System- Secrecy and Secret-Key Capacity

✓**Secrecy capacity (i.e., the maximum transmission rate at which the eavesdropper is unable to properly decode any information) is equal to the difference between the two channel capacities.**

✓ **The confidential communication is impossible unless the Gaussian main channel has a better signal-noise rate (SNR) then the Gaussian wiretap channel.**

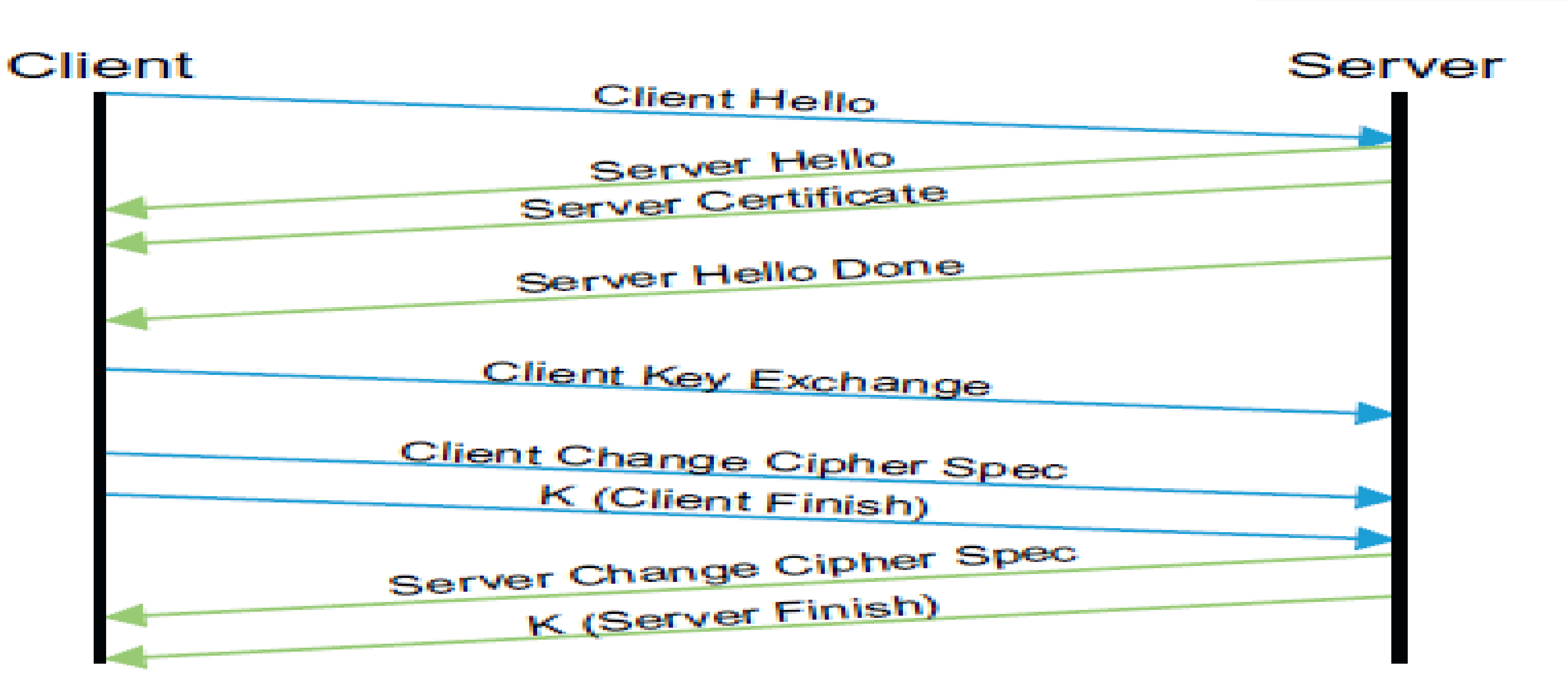
TRANSPORT ENCRYPTION

- The transport encryption involves the transport layer security (TLS) certificates, and identify verification.
- Both the TLS and SSL are cryptographic protocols that provide communications security over a network.
- A properly designed transport protocol can ensure that data, key handshaking, and data integrity verification are encrypted using secure transport protocols such as TLS and SSL.
- The most common encryption methods we are using in computer networks are mainly based on three algorithms: SSL, TLS, and HTTPS.

TRANSPORT ENCRYPTION

Transport Layer Security

In a TLS communication, to establish a TLS connection between a user and a server needs a typical handshake, as shown below



TRANSPORT ENCRYPTION

The basic processes are as follows:

1. The user (client) asks request to server.

2. The server sends its certificate to the user.

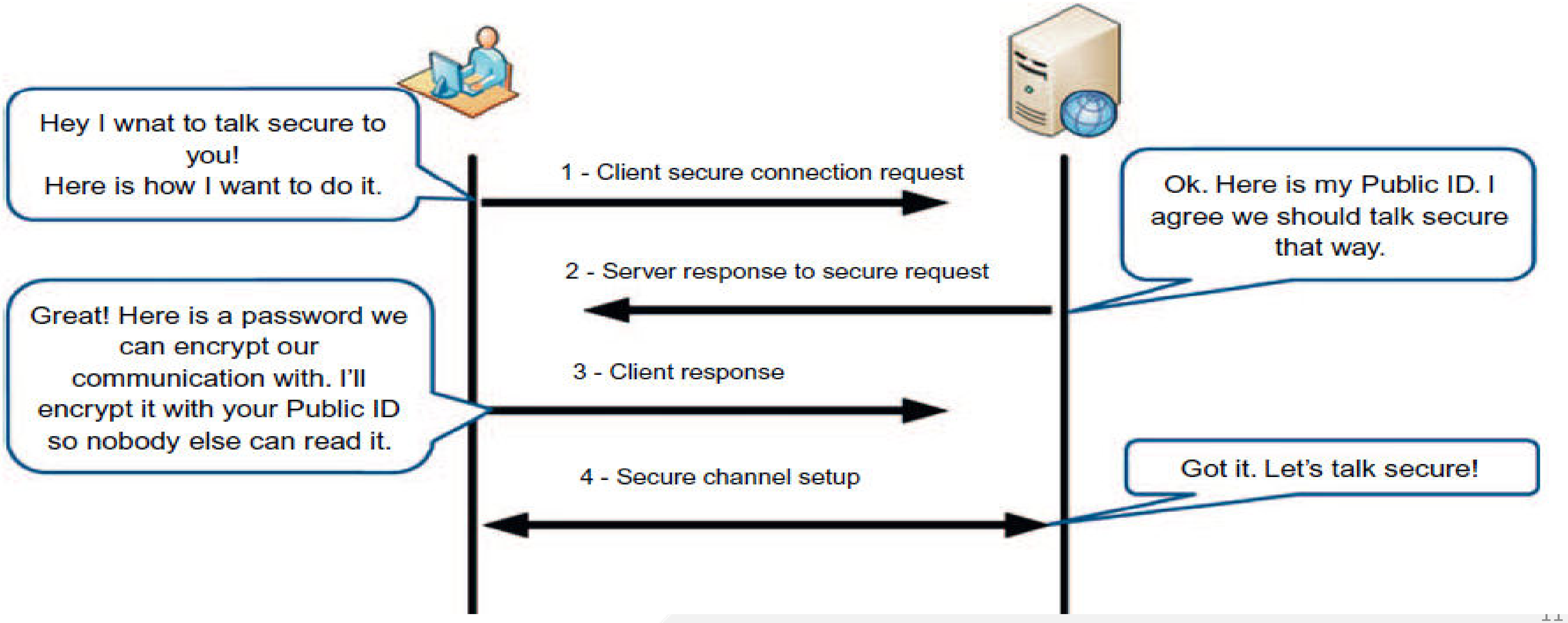
3. The user ensures that the HTTP server’s identity is correct by encrypting a “premaster secret” and if the server can decrypt it correctly, then the user knows the server has the private key matching the public key in the HTTP server’s certificate.

4. Both the user and the server send a final finish message to verify that the other side is using the same session key.

TRANSPORT ENCRYPTION

Secure Sockets Layer

Below figure shows a basic SSL connection.



Hey I wnat to talk secure to you!
Here is how I want to do it.

1 - Client secure connection request

Ok. Here is my Public ID. I agree we should talk secure that way.

2 - Server response to secure request

Great! Here is a password we can encrypt our communication with. I'll encrypt it with your Public ID so nobody else can read it.

3 - Client response

4 - Secure channel setup

Got it. Let's talk secure!

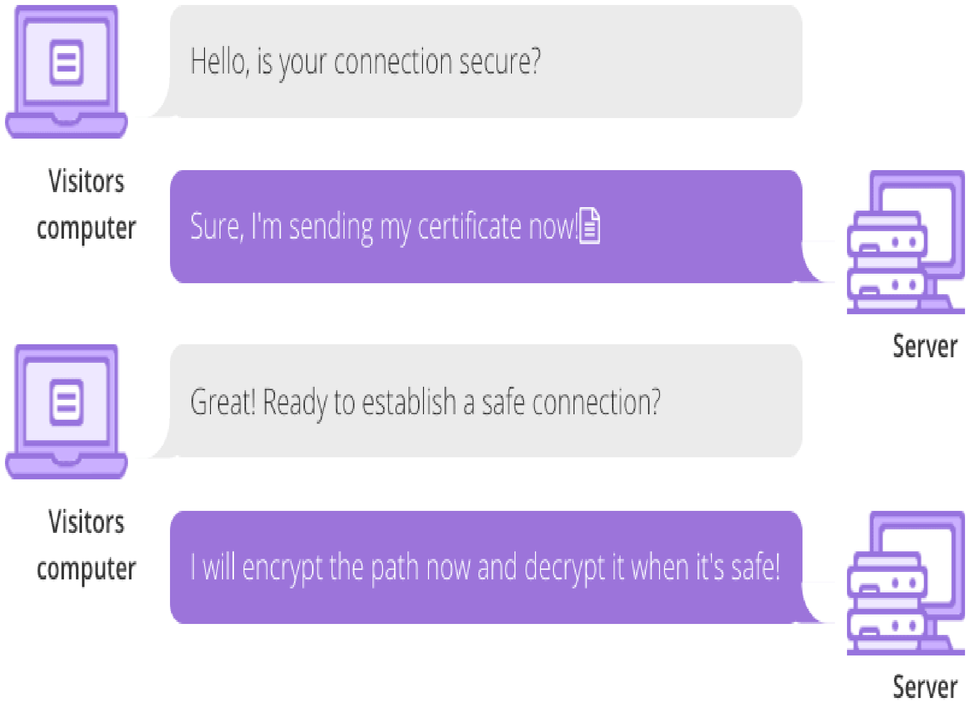
TRANSPORT ENCRYPTION

Secure Sockets Layer

The basic SSL connection involves following four basic steps:

1. User (client) secure connection reques
2. Server response to secure request
3. User (client) response
4. Secure channel setup.

.



Hello, is your connection secure?

Sure, I'm sending my certificate now!

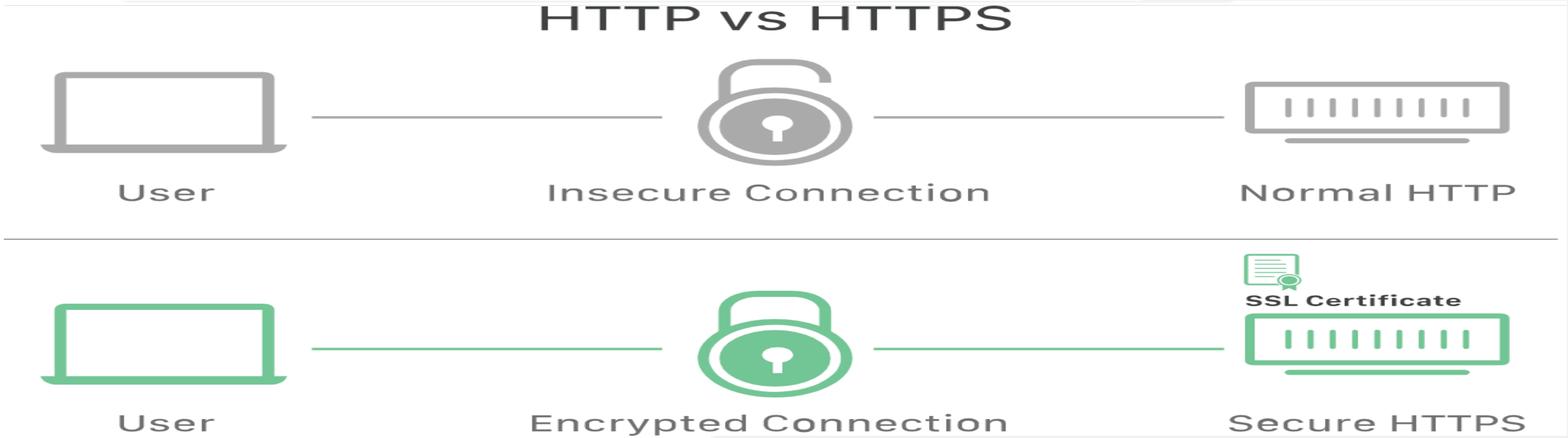
Great! Ready to establish a safe connection?

I will encrypt the path now and decrypt it when it's safe!

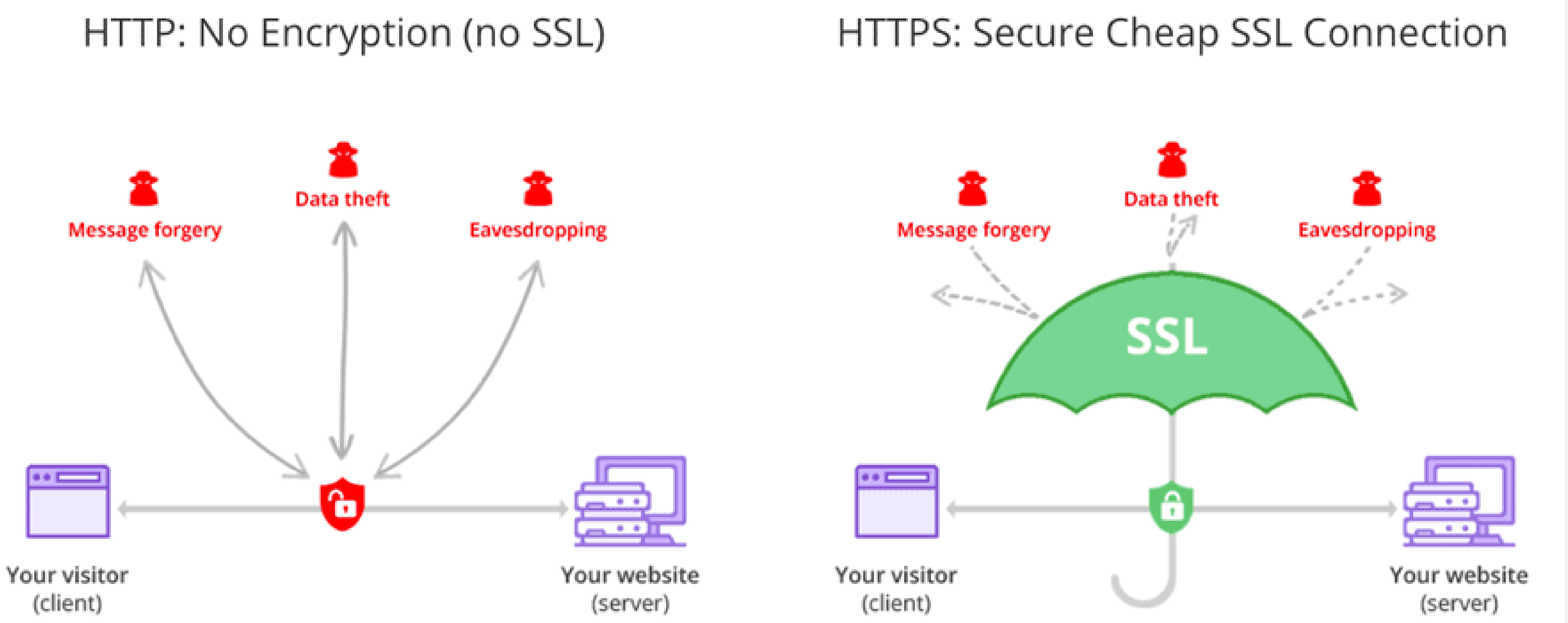
TRANSPORT ENCRYPTION

HTTPS

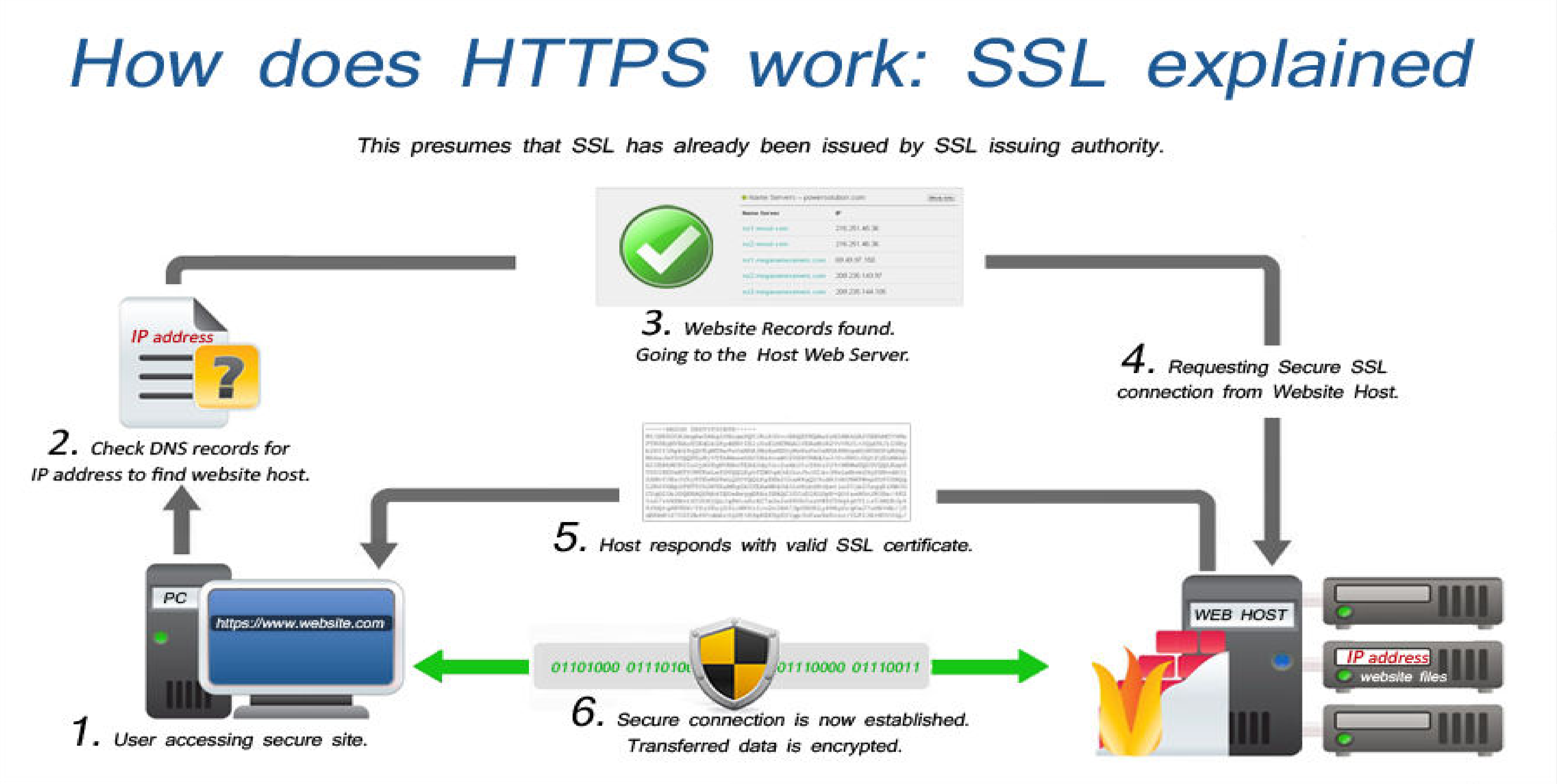
HTTPS is also called HTTP over TLS/SSL or secure HTTP. It is a protocol for secure HTTP connections and is designed for authentication of the visited website and protection of the privacy and integrity of the exchanged information.



TRANSPORT ENCRYPTION



TRANSPORT ENCRYPTION



How does HTTPS work: SSL explained

This presumes that SSL has already been issued by SSL issuing authority.

1. User accessing secure site.

2. Check DNS records for IP address to find website host.

3. Website Records found. Going to the Host Web Server.

4. Requesting Secure SSL connection from Website Host.

5. Host responds with valid SSL certificate.

6. Secure connection is now established. Transferred data is encrypted.

TRANSPORT ENCRYPTION

Transport Trust in IoT

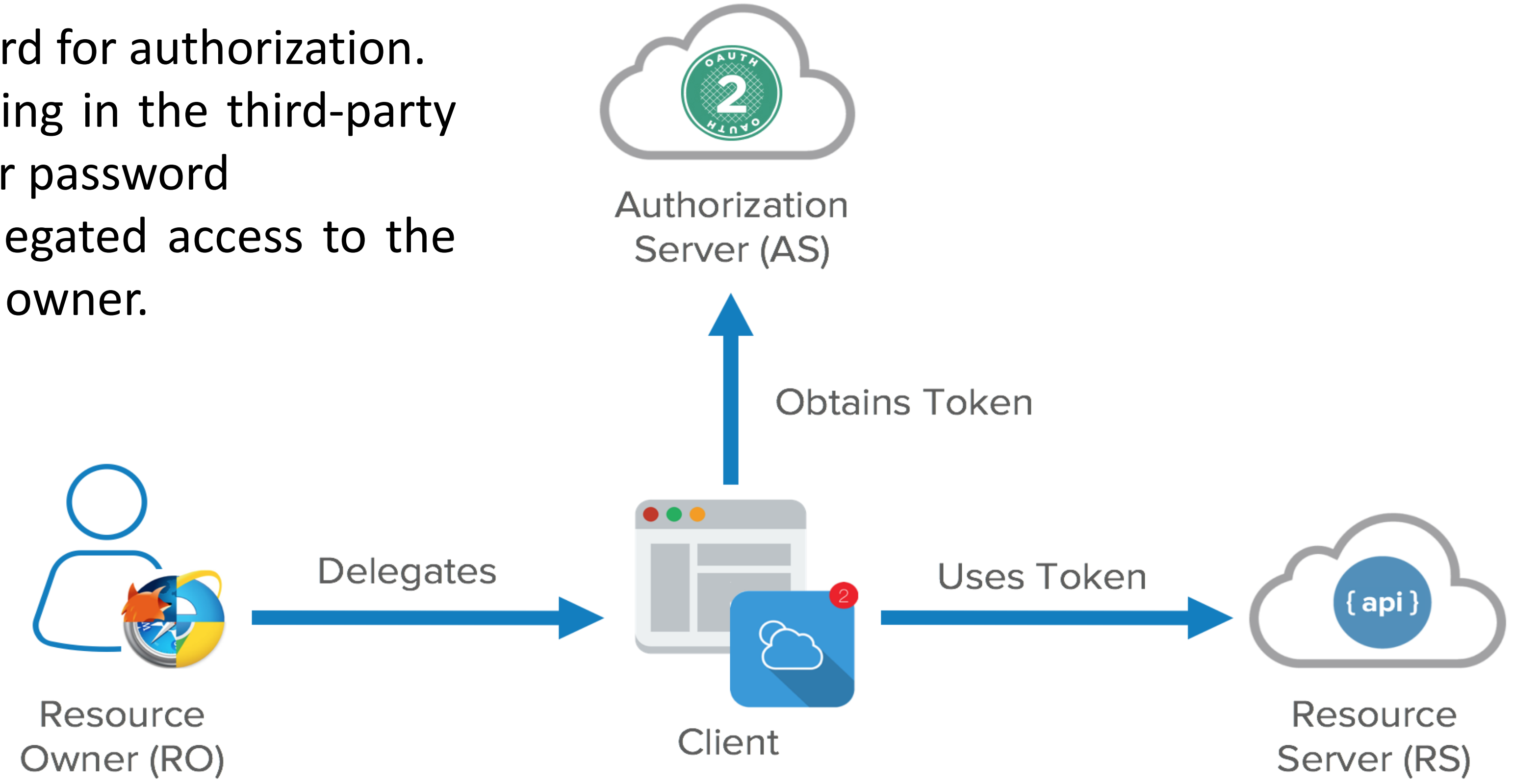
- In IoT, a number of lightweight protocols have been developed to match the needs of security, transmission, and resource consumption. The Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are the two most promising resource limited devices in IoT.

Both MQTT and CoAP have following features:

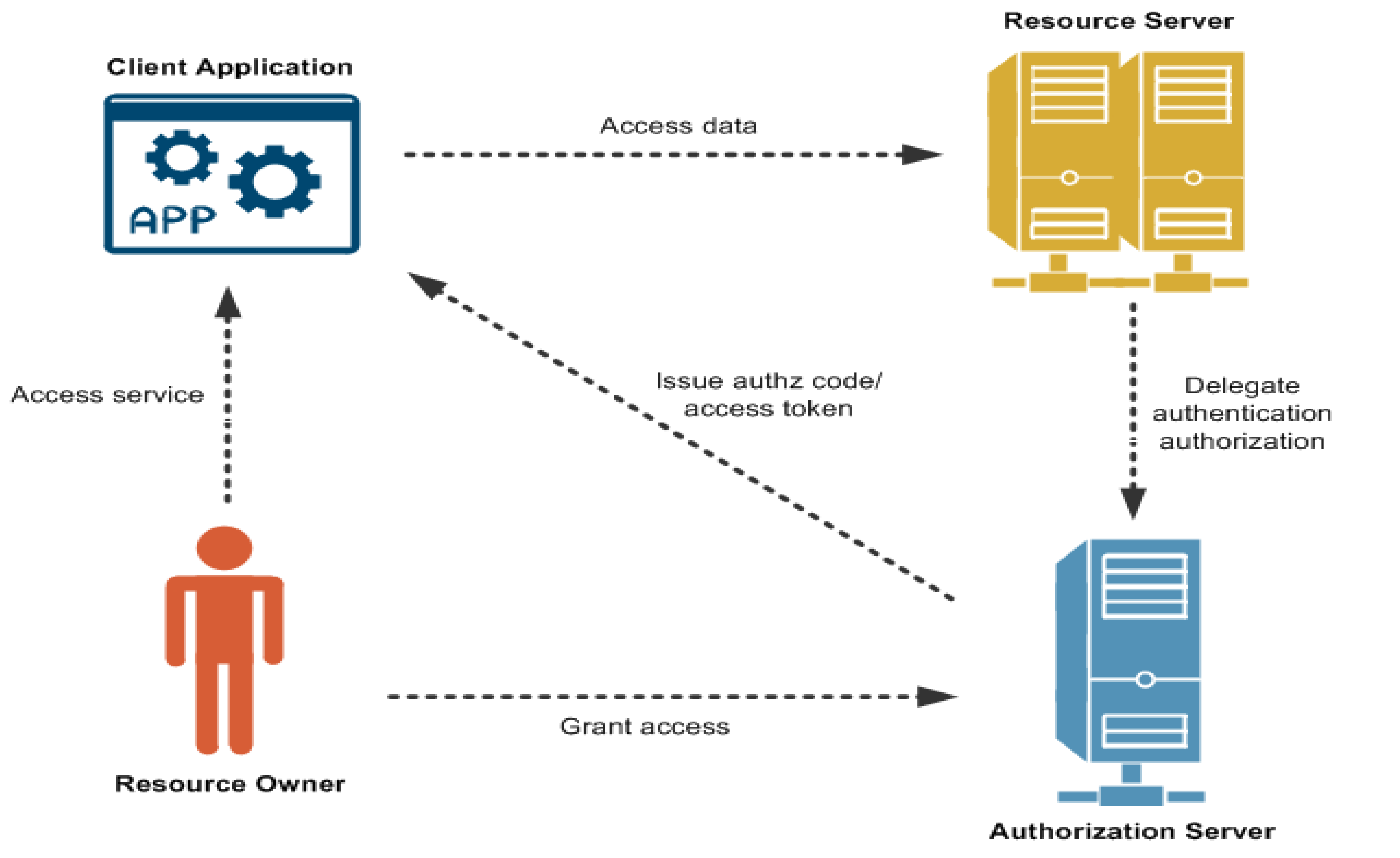
- Are open standard
- Easy to implement
- Provide bandwidth-efficient and uses energy-efficient communication

Authentication/Authorization for Smart Devices OAuth

- The OAuth is an open standard for authorization.
- It is commonly used for logging in the third-party website without exposing their password
- It provides user a secure delegated access to the server on behalf of a resource owner.



Authentication/Authorization for Smart Devices
OAuth



References

- Li Da Xu, Securing Internet of Things, Algorithms, and Implementations, Elsevier
- https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/
- https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture
- http://socpuppet.blogspot.com/2017/06/client-auth-issues-for-mutual-ssltls.html
- https://www.youtube.com/watch?v=CPbvxxslDTU
- https://www.youtube.com/watch?v=EIxdz-2rhLs

Home Assignment

1. List threats which may occur at Cross-Layer
2. Identify the application areas of OAuth

THANK YOU

For queries
Email: gaurav.e9610@cumail.in