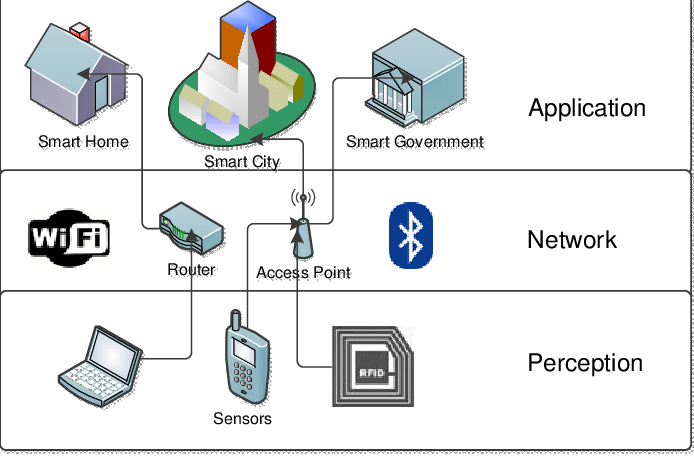
# **2.0 BACKGROUND STUDY**

This section will emphasise on all the research works that have been accomplished before starting this project. This will help us to build an understanding on the whole concept of deep learning models, eventually helping us to evaluate the models performance.

## **2.1 IoT Architecture**

In IoT, each layer has different functionalities and different devices are used in each layer. Due to the lack of standardization in the IoT domain, there are different architectures for IoT that have been proposed namely the three-layer architecture and the five-layer architecture. However, many researchers assert that the three-hierarchical layer architecture is the generally known structure to describe IoT systems and its components. It is formed by the Perception, Network and Application layer.

*Figure 1: Three –layer IoT architecture*

1. Perception Layer

The perception layer is the first layer in the IoT three-layer architecture. The main purpose of this layer is that it takes in information from the real-world environment with the help of IoT devices such as IoT sensors, actuators and sensor gateway. It senses, retrieve and process the data from IoT devices and collected information gets transmitted to the above layer (i.e. the network layer).

1. Network Layer

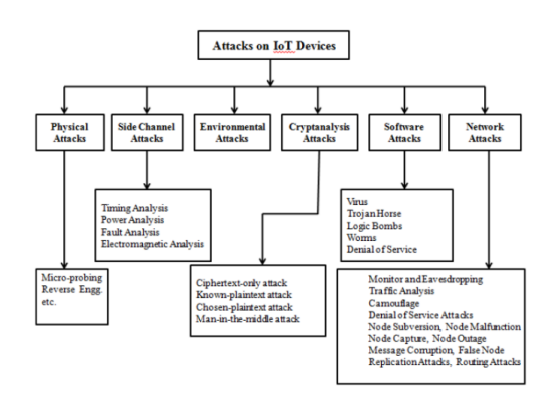
The network layer is the middle layer of the IoT three-layer architecture and it is used to determine the route of information provided by the perception layer. The collected data are transmitted to the uppermost layer (Application layer) securely over the Internet. This layer consists of different network components such as cloud-computing platforms, internet gateways, switching and routing devices and communicates using protocol such as WiFi, LTE, Bluetooth, ZigBee, 5G, etc… Since more and more applications are converging towards cloud technology, Internet gateways are an important part of the network layer.

1. Application layer

The functionality of the application layer is to supply various application service to users. It does so by specifying different deployment scenarios for the IoT, such as in smart cities, smart transportation, smart agriculture and so forth. For example, in a smart home, users can turn on a coffee maker by pressing a button in the app.

## **2.2 Security Challenges in each Layer of IoT**

Due to the rise in the number of IoT devices connected to the internet, security issues and threats are become a concern to the IoT network. Each IoT layers are vulnerable to either passive or active attack. Passive attack is when a system network data is monitored without causing any manipulation to the service whereas an active attack, the attacker stops the connection thus causing the network performance to degrade. Various security challenges facing IoT layers are discussed below:



*Figure 2: Several types of IoT attacks*

### **2.2.1 Types of attack in the Perception layer**

There are three security issues in IoT perception layer. First, the collected data from the sensors are transmitted wirelessly to a gateway or between sensor nodes using wireless protocols, such as Bluetooth, WiFi, zigbee or LoRaWAN, thus making other existing waves to reduce the strength of the wireless signals. Secondly, the IoT node are often deployed in uncontrollable and outdoor environments, making them vulnerable to physical attacks where attackers can easily interfere with hardware components of the sensors and devices. Third is the inherent nature of network topology which is dynamic as the IoT nodes are often moved around different places. The IoT perception layer

mostly consists of sensors and RFIDs, due to which their storage capacity, power consumption, and computation capability are very limited making them susceptible to many kinds of threats and attacks. Types of attacks on the perception layer are as follows:

1. Tampering Node

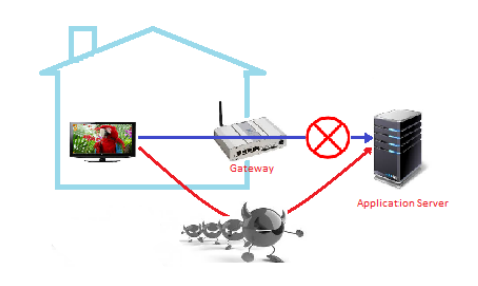
Tampering node is a type of physical attack in which an attacker gains physical access to an IoT device or node and modifies its hardware or software components or even examining the nodes in order to compromise its security or disrupt its operation. For example, the attacker may change the device’s firmware with a malicious version that allows them to take control of the device. Once an attacker has access to the node, confidential information such as cryptographic keys or routing tables may be known.

1. Malicious code injection

This is also a type of physical attack where an attacker exploits a vulnerability in the firmware of a sensor to inject malicious code that would allow them to manipulate data being transmitted or take control of the sensor or entire network. Alternatively, an attacker could exploit a vulnerability in the wireless communication protocols used to transmit data from the sensor to gateway/cloud, allowing them to inject malicious code into the data stream.

1. Falsification

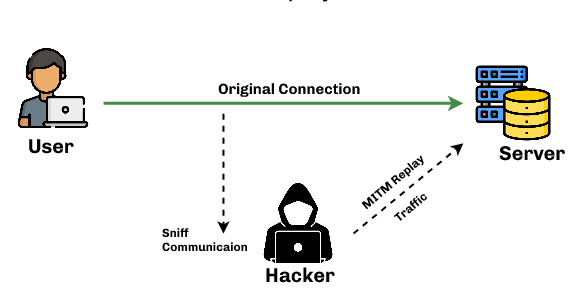
In a smart home, when the collected data from sensors are transmitted to the application server, data packets are collected by attackers by altering the routes in the gateway. Although SSL certification is applied, attackers can still avoid the forged certificate. As a result, the original data transmitted by a sensor may be replaced with false one, which in turn can be used to manipulate the behavior of the IoT system. For example, a false temperature reading may cause the heating or cooling system to turn on or off incorrectly.



*Figure 3: An example of falsification*

1. Replay attack

A replay attack is a type of network attack that occurs when an attacker intercept network traffic between two devices. The attacker then captures the data transmission between two IoT devices, and then replays it at a later time to one of the devices, which makes it to appear as if he was the sender. For example, an attacker could capture a valid command from an authorized user to unlock a smart lock, and then replay the command to the lock at a later time to gain unauthorized access. The goal of this attack is to trick a device to carry out a malicious action.



*Figure 4: An example of a replay attack*

### **Types of attack in the Network layer**

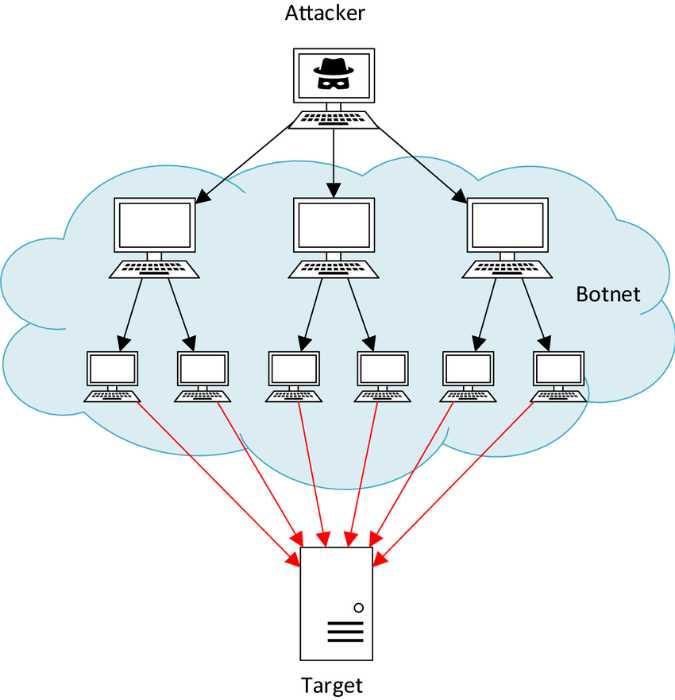
In IoT, the network layer is particularly important because of the large number involved in the network. It is responsible for ensuring that the data packets have reached their intended destination through communication networks. If the network layer is compromised, it can result in a variety of security threats. Types of attacks on the network layer are as follows:

1. DoS (Denial-of-Service)/ DDoS (Distributed Denial-of-Service) attack

A DoS attack is a type of network attack where an attacker sends a large volume of traffic or requests to the target server/system, thus making the network to be congested. This in turn exhaust the system’s resources such as memory, CPU, and network bandwidth. This results in the system becoming unresponsive or slow to respond.

A DDoS attack, on the other hand, work in the same way but attackers typically use botnet, a network of infected computers or devices which are controlled remotely by the attacker, to flood a targeted system with massive amount of traffic.

The aim of these attack is to create an inability for clean traffic to flow, thus preventing legitimate users to have authorized access to the targeted resources. There are several types of DDoS attack such as ping, UDP (User Datagram Protocol) and HTTP flood attack.



*Figure 5: An example of a DDoS attack*

1. Man-in-the-middle

MITM is a type of network attack where an attacker intercepts and modifies the communication, by eavesdropping the keying material, between two sensor nodes who believe that they are communicating directly with each other. As a result, the attacker gains unauthorized access to the network and can eavesdrop on the communication. The attacker can eventually exploit this false sense of security to steal sensitive information being transmitted.

An example of a MITM attack in the context of a smart environment network is provided below:

1. Bob’s smartphone communicates with his smart thermostat to adjust the temperature.
2. The attacker sets up its own wifi hotspot, with the aim to trick Bob into using it. The attacker also sets up a network sniffer to inspect any traffic as it passes through.
3. Once Bob connects to the unsecure wifi hotspot, the attacker is able to intercept the communication between the two devices with them knowing.
4. The attacker can then manipulate the communication by changing the temperature settings, preventing Bob from controlling the thermostat or even obtaining Bob’s login credentials.

MITM attack can be carried out in various forms like ARP spoofing, IP spoofing, SSL stripping, and more.

1. Routing attack

Routing attacks exploit vulnerabilities in the routing protocols used in a network to manipulate the flow of data, leading to unauthorized access, modification, or theft of data. In IoT networks, an attacker may undertake routing attacks in IoT networks in an effort to intercept, reroute, or prevent data packets as they travel across the network. This can be achieved through various methods, such as:

* Routing Table Poisoning

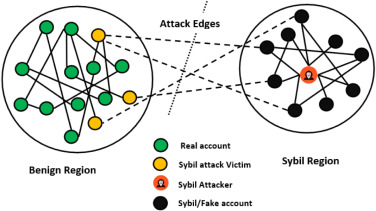
An attacker can corrupt the routing tables of routers in the network to redirect traffic to a malicious destination.

* Wormhole Attack

In this attack, an attacker creates a tunnel between two remote parts of the network to capture or modify data as it passes through.

* Sybil Attack

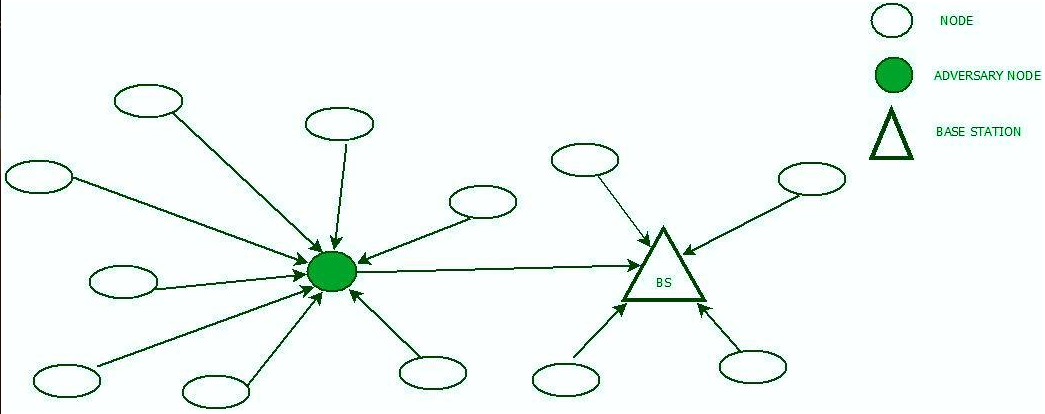
In this type of attack, an attacker creates multiple identities to other nodes in the network so that he can appear in more than one place at a time. As a result, he manipulates the flow of data. For example, in a WSN (Wireless Sensor Network), voting system single node can vote multiple times.



*Figure 6: Sybil attack*

* Sinkhole Attack

An attacker can compromise a node in the network to redirect all traffic towards it, causing a denial of service for the legitimate nodes. The compromised node does this by sending fake routing information to other neighboring nodes that it has the shortest distance path to the base station and guides the traffic from other nodes towards itself. In this way, the malicious node can manipulate the data or drop the packets, thus weakening the security of the network.



*Figure 7: Sinkhole attack*

### **Types of attack in the Application layer**

The application layer is the layer where the actual communication and interaction with the end-users takes place. The issues that it is facing is the lack of proper standards and global policies that manages the communication between different applications. Secondly is the diversity of connected devices that share data will cause large overhead on applications that analyze the data, which can impact on the availability of the service. Thirdly is the fact that it is difficile to integrate different authentication mechanism by application whilst ensuring data privacy and identity authentication. Some general threats to this layer are given below:

1. SQL (Structured Queried Language) injection

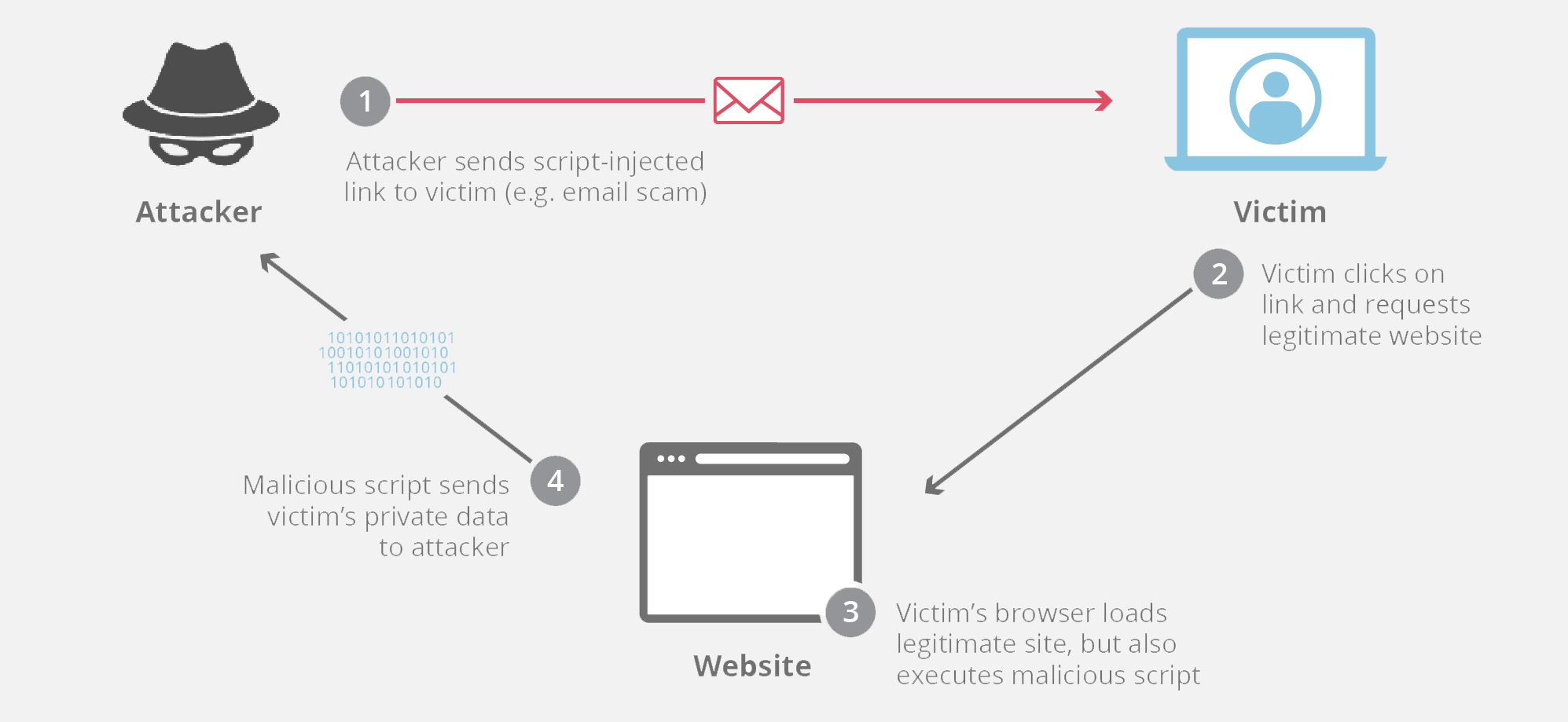
SQL injection is a type of attack where an attacker can inject malicious SQL statements into an application database, allowing them to bypass authentication mechanisms and modify, insert or delete sensitive data stored in the database.

The attacker can insert their own SQL code in a way that the application would accept it as a legitimate query, which would cause the database to be subjected to undesired operations.

1. Cross site scripting (XSS)

Cross-site scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious code into web pages viewed by other users. The attacker can then use this code to steal sensitive information, such as login credentials or session cookies, from the victim's browser.

A user is generally duped into clicking a link in a cross-site scripting attack that directs them to a website with malicious code. The code then executes in the user's browser, allowing the attacker to carry out a range of malicious actions. For example, in a smart home context, an attacker could use cross-site scripting to inject malicious code into a web interface used to control smart home devices. This could allow the attacker to take control of the devices, steal sensitive information, or carry out other malicious actions.



*Figure 8: XSS attack*

## **2.3 Study on Existing Security Threats and Solutions with critical reviews**

The research articles that have been done will be summarized in this part, together with some critical analysis.

IOT network involve devices with different communication protocols, making them more complex and challenging to secure.

<file:///C:/Users/Girish/Downloads/faloul_icitst15.pdf>

<file:///C:/Users/Girish/Downloads/JNIC_Paper11.pdf>

<https://www.geeksforgeeks.org/3-layer-iot-architecture/>

<https://dgtlinfra.com/internet-of-things-iot-architecture/>

<https://www.startertutorials.com/blog/iot-architecture-layers.html#:~:text=Perception%20Layer%3A%20It%20is%20the,the%20users%20via%20user%20interfaces>

<https://onomondo.com/resource-hub/iot-networking-protocols-overview-and-advantages/>

<https://developer.ibm.com/articles/iot-lp101-connectivity-network-protocols/>

<https://named-data.net/wp-content/uploads/2016/02/ndn-0038-1-challenges-iot.pdf>

<https://sci-hub.ru/10.1109/IWCMC.2019.8766455>

<https://theses.hal.science/tel-03141013/document>

<https://ltu.diva-portal.org/smash/get/diva2:1562531/FULLTEXT01.pdf>

<https://www.tutorialspoint.com/3-layer-of-iot-architecture>