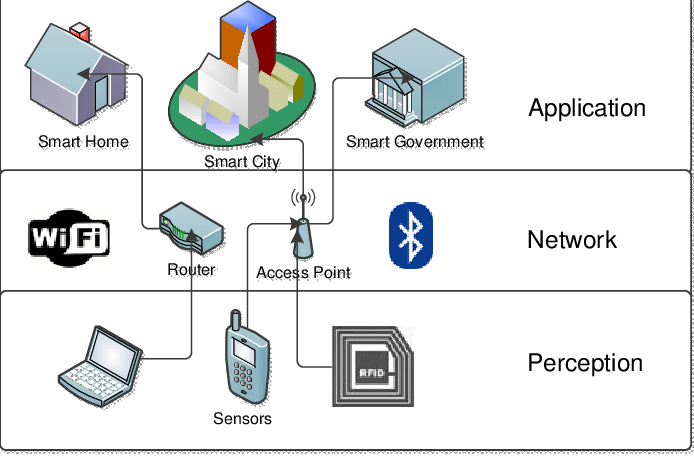
# **2.0 BACKGROUND STUDY**

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 concept of the different layers in an IoT system, and the concern of security threats prevailing in an IoT network.

## **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

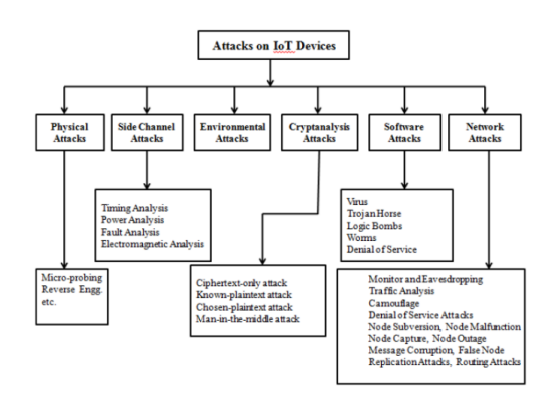
The network layer is the middle layer of the IoT three-layer architecture and it is used to determine the route of information provided by the perception layer. The collected data are transmitted to the uppermost layer (Application layer) securely over the Internet. This layer consists of different network 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

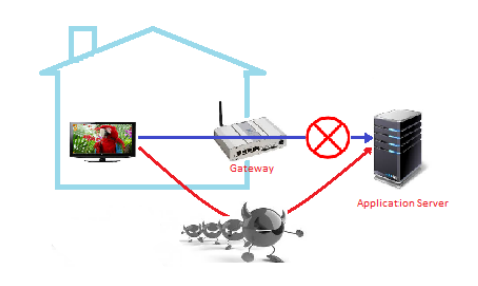
Tampering node is a type of physical attack in which an attacker gains physical access to an IoT device or node and modifies its hardware or software components or even examining the nodes in order to compromise its security or disrupt its operation. For example, the attacker may change the device’s 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

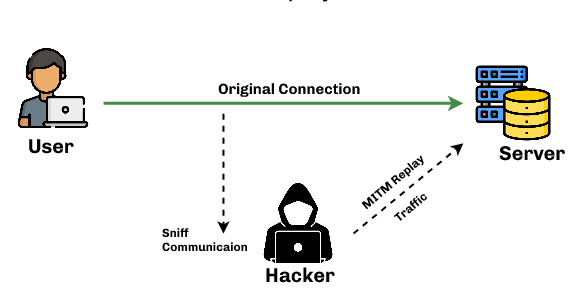
In a smart home, when the collected data from sensors are transmitted to the application server, data packets are collected by attackers by altering the routes in the gateway. Although SSL certification is applied, attackers can still avoid the forged certificate. As a result, the original data transmitted 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**

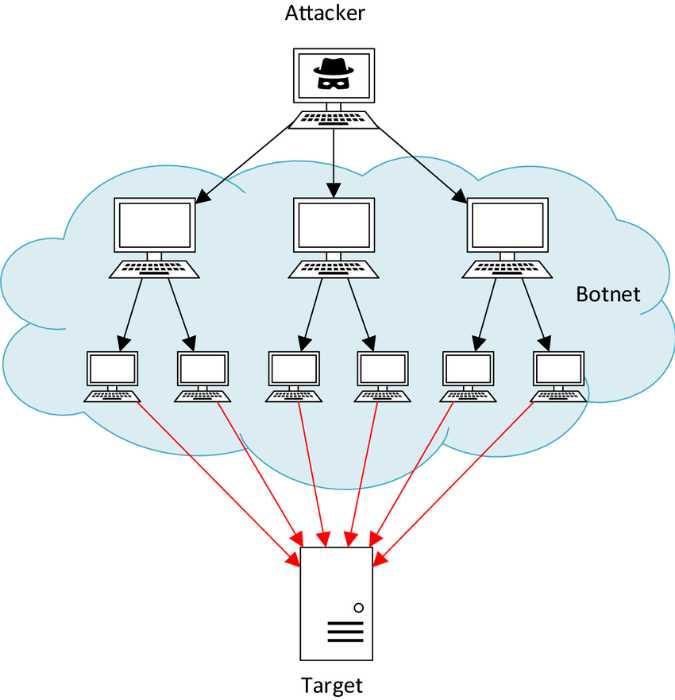
In IoT, the network layer is particularly important because of the large number involved in the network. It is responsible for ensuring that the data packets have reached their intended destination through communication networks such as Wi-Fi. If the network layer is compromised, it can result in a variety 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

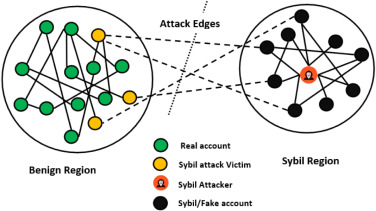
An attacker can corrupt the routing tables of routers in the network to redirect traffic to a malicious destination.

* 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

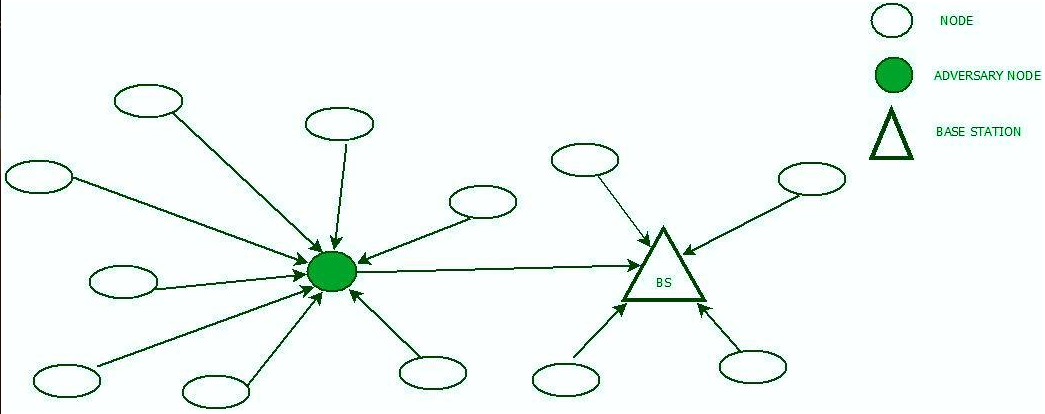
In this type of attack, an attacker creates multiple identities to other nodes in the network so that he can appear in more than one place at a time. As a result, he manipulates the flow of data. For example, in a WSN (Wireless Sensor Network), voting system single node can vote multiple times.



*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

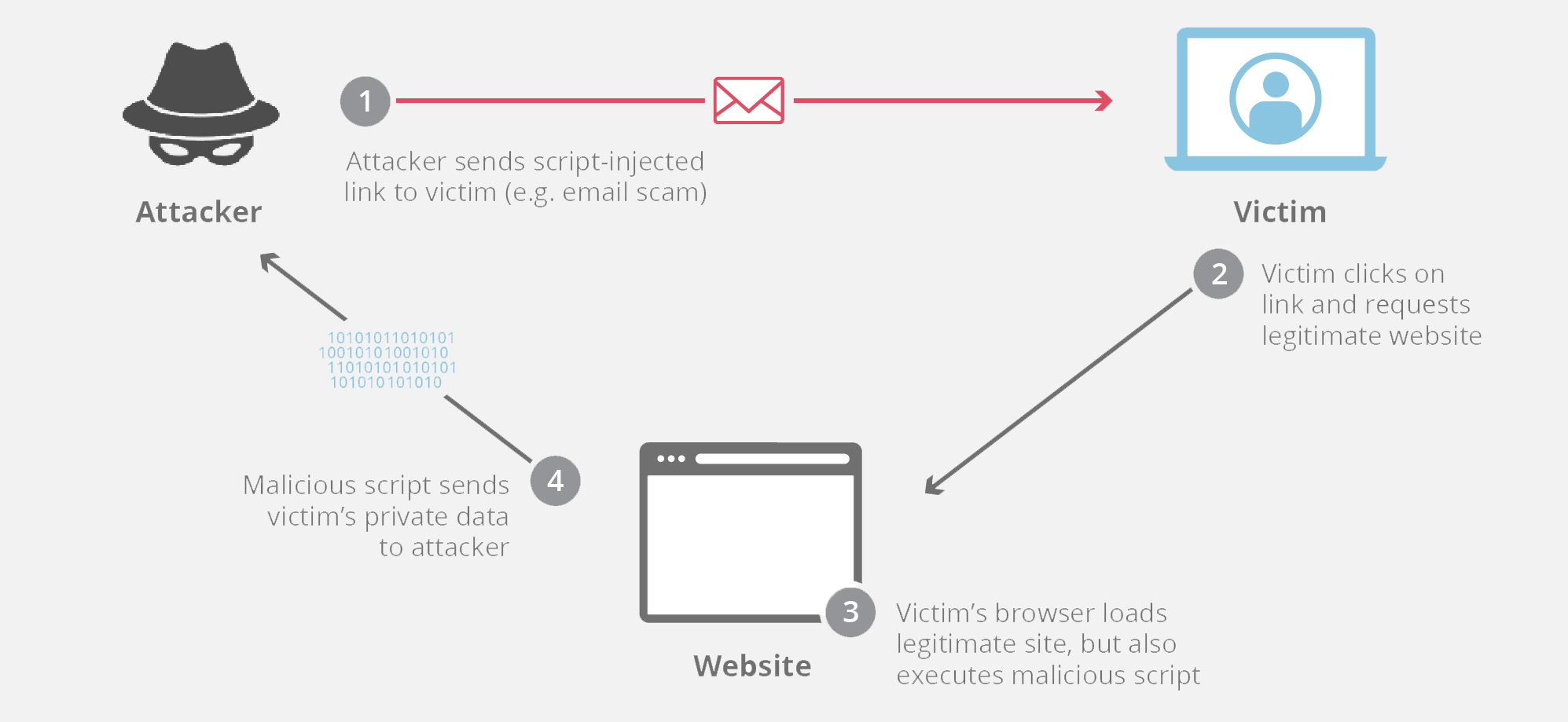
SQL injection is a type of attack where an attacker can inject malicious SQL statements into an application database, allowing them to bypass authentication mechanisms and modify, insert or delete sensitive data stored in the database.

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 over Wi-Fi with critical reviews**

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

**2.3.1 Research Study 1- Bad Token: Denial-of-Service attack on WPA3**

Despite WPA3 mechanism is a better alternative compared to WPA2 mechanism in terms of security strength, this article makes prominent that WPA3 can still be vulnerable to security threats. Attackers usually utilize bad token in a race condition to cause a denial-of-service attack. This happens by delivering false authentication messages that contain a bad token (WPA3 authentication confirm value) during the WPA3 authentication. This in turn does not allow legitimate wpa supplicant to connect to a WPA3 network. Lounis et al. have shown the demonstration of this attack on a WPA3-SAP network using Raspberry Pis and Wi-Fi Linux utilities, hostapd2.7 and wpa\_supplicant-2.7.

On the other hand, one WPA2 attacks namely, the Ghost attack, could also cause vulnerabilities to legitimate WPA3 clients.

The ghost-attack takes advantage of a vulnerability in Wi-Fi supplicants and authenticators, which makes them incapable of authenticating the initial association request and response. A spoofed association response frame can be injected by an attacker in a race condition scenario, causing the protocol to proceed in such a way that Wi-Fi supplicants abandon the authentication process.

**Critical Analysis**

This article has proposed a time-based countermeasure to prevent this DoS attack on WPA3 during a race condition scenario. However, creating time intervals between incoming packets may slow down the response time thus affecting the network performance. In the future, Wi-Fi supplicants and access points should be designed in such a way that Management Frame Protection (MFP) is automatically enabled so that only legitimate management frames are accepted by access points.

**2.3.2 Research Study 2- Password Acquisition and Traffic Decryption Based on L2TP/IPSec**

Regarding the fact that L2TP/IPSec is a strong VPN encryption protocol, this paper introduces an attack method to obtain password and to decrypt traffic during transmission of data. This protocol also includes identity authentication, key agreement management, and data encryption transmission mechanisms. (Luo et al., 2020) analyses the vulnerability of key-agreement management, and identity authentication mechanism based on L2TP/IPSec and introduces a practical method to obtain login password and the pre-shared key. The vulnerabilities of data encryption mechanism and the method for password acquisition that occur when traditional attack methods against L2TP/IPSec are being integrated are mapped to the analysis model based on a tree structure. By analyzing the tree structure model, all the possible attacking paths can be obtained against a target and a method for acquiring password and decrypting the traffic are proposed quickly. Similar implementation of this attack are realized which involves cracking the password and restore encrypted information through man-in-the-middle attack.

**Critical Analysis**

This study analyses the vulnerabilities of the L2TP/IPSec protocol in order to provide a method to supervise the network and track suspicious activities in an effective and timely manner. This is done to maintain national security over the internet. However, if the encryption algorithm level of the VPN is high, its bandwidth and transmission speed will be slow. In order to achieve better security and better transmission speed, efficient encryption algorithm such as Advanced Encryption Standard (AES) could be implement to reduce computational overhead and maintain an efficient VPN transmission speed.

**2.3.3 Research Study 3- Man-In-The-Middle Attack in Wireless and Computer Networking- A review**

This article inspects various MITM attacks and a survey was conducted on all the attacks based on impersonation techniques (Bhushan et al.). Various countermeasures involving MITM attacks were presented along with the way that they operate. In a MITM, the attacker targets the packets that are transmitted between endpoints. In this way, confidentiality of data can be eavesdropped and integrity of data can be modified by intercepting the communication. Moreover, we categorize MITM attacks into four categories namely spoofing based MITM, TLS/SSL MITM, BGP MITM and false base station based MITM attack. The operations of these attacks were discussed and solutions to protect against those attacks were also stated. Finally, several cryptographic techniques such as elliptic curve cryptography, key distribution and authentication methods can be implemented as a solution to such attacks.

**Critical Analysis**

The article proposed using cryptographic techniques to protect data transmitted over the network from interception and tampering from attackers. Effective secure communication protocols such as HTTPS, SSH and SFTP could be applied for future directions.

**2.3.4 Research Study 4- Security Issues in IoT: A Survey**

A survey of various security methods that address the issues in IoT security are discussed in this paper, while considering the problems facing with IoT devices such as low-performance CPU, low memory, and limited power battery. These issues are mainly focused on authentication, types of attacks, encryption issues, IoT security framework and IoT hardware-based support. Due to the limitations in the software and hardware components, the process of implementing existing security methods in IoT devices are not easy. Hameed et al. brings up the necessity of applying lightweight encryption algorithms to support the IoT devices and prevent the different types of attacks. The algorithm hides the IoT networking paths, making it difficult to attack. (SPE) which creates additional packet to the network is integrated in this algorithm. These packets that are produced are fake and the aim is to hide the real data packets in the network. However, in order to provide a trusted security, the algorithm still need to be improved before it is implement in an IoT system.

**Critical Analysis**

The algorithm under review proposed an idea of being protected against network attacks. However, the network traffic can be learnt by attackers and they can easily differentiate between the fake and real data. To maintain the confidentiality during network transmitting data, encryption mechanism such as WPA3 should be implemented so attacker will not be able to access sensitive data transmitting packets.

**2.3.5 Research Study 5- IoT Security in Wireless Devices**

Due to the rise in the number of IoT wireless devices connected to the internet, the IoT security still remains a concern. Gauliya et al. have proposed the idea of Elliptic Curve Cryptography (ECC) which is a technique of ensuring efficient encryption of data based on curvy algorithm. Moreover, an attempt has been made to prove the efficacity of this cryptographic algorithm to enhance the IoT security. It encrypts data at a 164-bit platform and in order to crack this algorithm, 1024-bit is required. Despite the fact that large key size is to be used to breach the network, attackers can still find a way to enter into the network. As a solution to this problem, this article introduces the idea of implementing ECC at each layer and every node on wireless devices. This will make the standard protocols to generate new encryption decryption code each time ensuring high security of the wireless devices.

**Critical Analysis**

This study discussed how effectively ECC security mechanism encrypts keys using small key size. However, implementing ECC at every layer of a network is challenging due to the complex mathematical algorithm which is involved when finding suitable elliptic curves and generating suitable parameters for the keys. An alternative is to use a security protocol such as SRPP to encrypt keys and it has a better response time in terms of its latency, scalability and packet overhead.

**2.3.6 Research Study 6- Enhanced IoT Wi-Fi protocol standard’s security using Secure Remote Password Protocol**

In IoT based application, Wi-Fi network plays a vital role in creating that network of connected devices. Sometimes, IoT devices are designed with low-security protocol which makes them vulnerable immediate attacks. This research proposes a password protection protocol, SRPP (Secure Remote Password Protocol), which can be implemented Wi-Fi network to prevent brute-force and dictionary attacks. The simulation is done using the GNS3 simulator and performance of the enhanced Wi-Fi security protocol is evaluated with the IoT security model's evaluation metrics such as packet overhead, integrity, network latency, and scalability (Hiba et al., 2022). ECC and TA were the two security mechanism that were selected to compared SRPP mechanism in terms of their response time. The overall simulation results prove that SRPP has better response time when generating encrypted keys and authenticating secret key. Therefore, it is considered as a suitable option of extending Wi-Fi’s module against immediate attacks discussed since it performs very well in terms of integrity, scalable, latency and packet overhead rate than ECC and TA mechanisms.



*Figure 9: SRP protocol against brute force and dictionary attacks*

**Critical Analysis**

This article proposes a security protocol that uses a large number of encrypted prime number group series as cryptographic techniques to make it difficult for attackers to get that exact combination to decrypt the secret key. However, multiple strategies for authenticating keys can be put together for future directions to strengthen Wi-Fi’s security.

* 1. **Comparative analysis of threats over a Wi-Fi IoT network**

This section provides a comparison of all the main cyber threats to IoT network. Their nature/behavior of attack and threat level of attacks are discussed. The threat level of those attacks are categorized into two types according to their behavior and possible solutions to threats.

1. **High-level attack**: Involves manipulation of sensitive data.
2. **Extremely high-level attack**: Involves making the network unresponsive or causing it to crash.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threats Type** | **Threat level** | **Behavior** | **Existing solution** | **Advantage of solution** | **Limitation of solution** |
| Brute force /Dictionary attack | High | It is a password cracking attack where the attacking software used tries every possible combination of passwords until the correct credentials are found. If attack is successfully, an attacker may gain unauthorized access to sensitive information. | Elliptic Curve Cryptography | It encrypts data at a 164-bit platform and in order to crack this algorithm, 1024-bit is required | Difficult to implement due to complex mathematical algorithm which is involved when finding suitable elliptic curves and generating suitable parameters for the keys |
| Denial-of-Service | Extremely high | It is an active attack that disrupts the normal functioning of devices over a network. It involves flooding the network with excessive traffic, causing it to crash. This attack can be launched using tools such as Ping of Death, SYN flood and UDP flood | Use Firewall | It blocks traffic from known malicious sources | When performing deep packet inspection, firewall may add latency to network traffic, thereby degrading network performance |
| Man-in-the-middle | High | It is an eavesdropping attack method. Special devices like WIFI PINEAPPLE can be used as a fake access point and once user connects to it, data can be intercepted and manipulated | Use Virtual Private network (VPN) | Data sent through the network will be encrypted. | Using VPN makes the network slow resulting into a low bandwidth |

ANALYSIS PART

References:

1. <https://ieeexplore.ieee.org/document/8455902>
2. <https://www.researchgate.net/publication/318096417_Security_Issues_in_the_Internet_of_Things_IoT_A_Comprehensive_Study>
3. <https://www.researchgate.net/publication/272488555_A_Critical_Analysis_on_the_Security_Concerns_of_Internet_of_Things_IoT>
4. <https://www.hindawi.com/journals/scn/2021/5533843/>
5. <https://ieeexplore.ieee.org/document/8286004>
6. <https://ieeexplore.ieee.org/document/8058363>
7. <https://www.researchgate.net/publication/337520632_Bad-token_denial_of_service_attacks_on_WPA3>
8. <https://ieeexplore.ieee.org/document/9295700>
9. <https://ieeexplore.ieee.org/document/8344724>
10. <https://ieeexplore.ieee.org/abstract/document/8910320>
11. <https://ieeexplore.ieee.org/document/8822124>
12. <http://pen.ius.edu.ba/index.php/pen/article/view/2728>