**Ensuring Device Security**

To ensure our device security. First, we will get every device’s mac address and store it in the database called “Device Authentication”. Secondly, we will set a strong password to secure the database to make sure the database is safe. After that, if any device’s mac address is outside of our network and tried to access our device. Our system will find that device’s mac address and compare it by using the registered mac address list from the database. If the mac address is not on the list, then the system will notify us to remove the unknown device .

**Data Transferred Between Devices and Server and while in Storage**

1. **Throttling :**

To prevent the server overload by handling legitimate requests from the client and processing them which will cause the server crash. We will use throttling measures to limit the number of requests sent by the user and drop the server when the user sent my request at the same time. For example, if the user sends the first request, the server will ignore the rest of the requests in these 30 minutes.

**2. Input Validation**

We can use input validation in each blank that needs the user to type something. The input validation will verify is the user input type is allowed or not. It will also make sure the length, type, and format that the user types in are acceptable. Only the validated value can be processed, it helps to counteract any commands inserted in the input string. For example, we can use regular expressions to make sure the data input is valid.

**3. Strong Password, Change Password Often**

To prevent IoT attacks, we will set a strong password and change the password for every device and database in our network. For example, the password must have at least 8 letters which include 1 uppercase letter, 1 lowercase letter, 1 special character (! @#$%^&\*) and a number. Then, change the password per month with a different password than the previous one.

**4. Use the “POST” method**

We will use the “POST” method instead of the “GET” method in getting the information that is input from the user. It is because the “GET” method, will show the user’s information in the URL link but the “POST” method wouldn’t. For example, we will use the “POST” method in the HTML file which requires the user to submit their information.

**5. IAM Role**

IAM Role is an IAM identity that let us can create an account with specific permissions. It is like an IAM user, in that it has an AWS identity with permissions policies that determine what the identity can and cannot do. (AWS, 2020) The Ec2 and MySQL databases prevent the user can access the database and Ec2 without permission.

**6. SSL certificate**

Secure Sockets Layer (SSL) is a cryptographic protocol that is used to secure communications over the computer network. For example, HTTPS. It is because HTTPS use a key called A to encrypt communication content by using symmetric encryption. After that, HTTPS will use asymmetric encryption to encrypt key A and send it to another party. If the key does not fall into another party, then the transmitted data will not be decrypted by another party

# References

AWS, A., 2020. *https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles.html.* [Online]   
Available at: https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles.html  
[Accessed 2021 October 2021].

Infosys, 2021. *Infocyte.* [Online]   
Available at: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/  
[Accessed 17 October 2021].