STEP 1: IDENTIFY ASSETS

For our smart home, the primary assets include:

Devices: Smart locks, cameras, thermostats, smoke detectors, and home assistants.

Data: Personal identification information, financial data, and usage patterns.

Infrastructure: Home Wi-Fi network, connected cloud services, A website for managing IoT devices.

STEP 2: IDENTIFY THREATS (THREAT MODEL)

Victim: The victims are every family member who uses the smart home system.

Adversary: In this situation, there are various types of adversaries, with the primary group seeking economic benefits. Their objectives include stealing personal financial information, hijacking devices for ransomware attacks, or incorporating devices into botnets for use in larger scale cybercrimes such as DDoS attacks.

Threats:

1- Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks

2- Adversary use DoS(denial of service)attacks to target smart home system

STEP 3: ASSESS IMPACT

Threat 1: Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks

1.Damage to assets:
In our design, we use a web interface to manage and control IoT devices. XSS (Cross-Site Scripting) and CSRF (Cross-Site Request Forgery) attacks exploit the weaknesses of the web, targeting security vulnerabilities in the IoT devices' web interfaces. They can steal users' personal information, session tokens, and other sensitive data, or unlock smart door locks, alter the configurations of other critical devices, posing a threat to the users' physical safety.

2.Cost of remediation:
Remediating vulnerabilities and enhancing system security may require additional technical investment and resources, and the attack incident could damage users' trust in the IoT website. Furthermore, legal liabilities arising from data breaches must also be considered.

Threat 2: Adversary use DoS(denial of service)attacks to target smart home system

1.Damage to assets:
Adversaries overload our servers with a flood of requests or data packets, causing our smart home system to be unable to process user requests, leading to users being unable to use our services normally. It affects users' trust in the service, which could lead to customer loss in the long term. Moreover, it may also impact the company's revenue.

2.Cost of remediation:
Enhancing server and bandwidth capacity, as well as purchasing DoS protection services, will exert financial pressure. Moreover, if the attack leads to data breaches or service disruptions, we will need to face legal litigation, which also represents a significant expense.

STEP 4: PRIORITIZE THREATS

Threat 1: Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks
Threat 2: Adversary use DoS(denial of service)attacks to target smart home system

STEP 5: DESIGN THE THREATS

1. Create a simple website to serve as the management interface for our smart home system, then collect data over a period of time from smart TVs and smart cameras, as well as fictional personal information (such as passwords for smart door locks or biometric data, bank card PINs, and other sensitive information), and place this information into a secondary page of the website.
2. We will use JavaScript to write a piece of attack code and insert it into a request code (for example, a family message board feature). The purpose of this attack code is to capture the user's username and password. When the browser receives this request, it will store the attack code in the database along with it. When a user logs back into the website, their browser will execute this attack code, and we will obtain the user's username and password.

Step 6:Design security-oriented applications/systems

- Develop a website/application that simulates the scenario of a reflected XSS/store XSS attack and notifies users when an attack occurs.
- Dynamic content is built using Javascript and HTML, deliberately leaving holes where scripts can be injected via URL parameters.
- Monitor potential attack attempts by analyzing HTTP requests, employing regular expressions, or other string matching techniques to detect malicious scripts.
- Trigger an alert mechanism and log the attack details when the system detects a potential reflected XSS attack.
- Implement a user notification system to send security alerts to users via email or in-app notifications when an attack is detected.

Innovation / Area of research

- Usage of blockchain technology, zero knowledge proof protocol for authentication.

- AI based models for anomaly login detection, Generative Adversarial Networks (GAN) based AI systems which can run constantly and can enhance the system by running both generator(attacker) and discriminator(defender).

- Location-based graphs for validation

Ethical consideration

- **Privacy** : Prior collecting any data from the users, consent should be obtained, also data should be protected by barriers. The sensitive data should be encrypted.

- **Biases** : Any face detection models for threat detection should be free from biases on race and community.

- **ESG Impact** : A thorough analysis should be done on data collection, thereby avoiding any redundancy in data.

- **Community Impact / Mental health issues** : The surveillance mechanism should be balanced, so that no one feels intimidated.