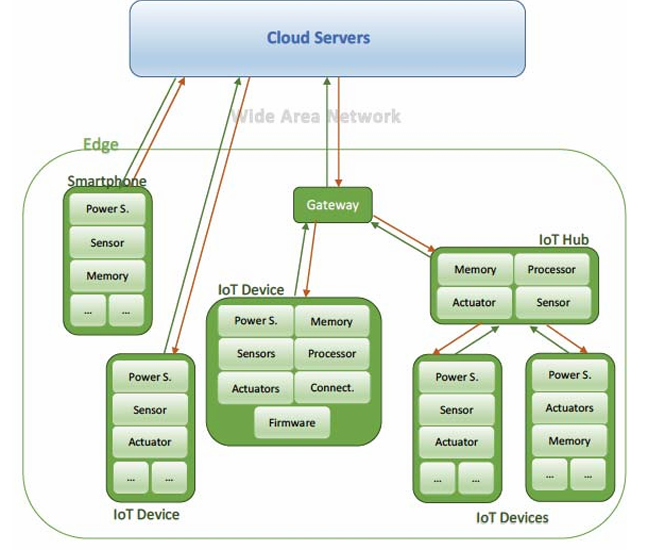
**SMART HOME SECURITY ARCHITECTURE**

****

**Components:** Sensors, Actuators, Memory, Processors, Memory, Power Source, Firmware

**Devices:** IoT Devices, IoT Hubs, Residential gateway, Smart phones/tablets/Computers

**SECURITY FUNCTIONS:**

Security functions address the devices themselves and their interfaces (e.g., web services and mobile apps). The requirements for cybersecurity by design can be categorized as follows:

* Basic Security Measures – security related events must be logged and users should be notified about every event and uncertainty.
* Networking and Communication – communication should be protected against disclosure, modification, replay and denial of service.
* Cryptography – confidentiality, integrity and authenticity must be protected by using strong cryptography. Keys must be managed securely, and use of a trusted infrastructure is encouraged.
* User Data Protection – confidentiality, integrity and authenticity of user data must be protected. Confidentiality protection must be in line with data privacy issues.
* Identification, authentication, authorization – strong authentication methods must be used as well as access control mechanisms. Passwords and sessions should be managed accordingly.
* Self-Protection – hardware and software self-protection should be activated. Data used to enforce these security functions should be protected and hardening should be used to reduce the attack surface.

**SECURITY GUIDELINES:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Sub Category | Guideline | Standard | ID |
| System and Information Integrity | Firmware Updates | Regularly update device firmware to patch bugs, fix vulnerabilities, and add new functionalities. Ensures devices are protected against known vulnerabilities and potential cyber threats. | NIST - SI-02 |  |
| System and Information Integrity | Monitoring the Network | Implement tools to monitor IoT device connections during message transfer. Enables the detection of unusual activities or potential security breaches, enhancing overall network security. | NIST - SC-05(03) D |  |
| Authentication | Multi Factor Authentication | Utilize multi-factor authentication (MFA) and device-based authentication. Identify the type of MFA used by the application. Determine whether the MFA implementation is robust and secure. Attempt to bypass the MFA. | OWASP - 4.4.11 | WSTG-ATHN-11 |
| Authentication | Digital Signature | Use device certificates or unique identifiers for IoT hubs to ensure that only authorized hubs can connect to the network. | NIST - CM-14 |  |
| Network Security | Security and Configuration | Review the applications’ configurations set across the network and validate that they are not vulnerable. Validate that used frameworks and systems are secure and not susceptible to known vulnerabilities due to unmaintained software or default settings and credential | OWASP - 4.2.1 | WSTG-CONF-01 |
| Network Security | VPN | Utilize secure virtual private networks (VPNs) to create encrypted communication channels within the network, ensuring that data is accessible only to authorized users. | OWASP - Acess Control - Best Practice |  |
| Cloud Storage | Access control | Users accessing cloud platforms for smart home services should use strong, unique passwords. Utilize OAuth or other secure authentication mechanisms for users connecting their devices to cloud services. Ensure that data transmitted between smart devices and the cloud is encrypted using secure protocols. | OWASP - 4.5.5 | WSTG-ATHZ-05 |
| Firewall | Access | Define concise policies for firewall rules and basic network access in the warehouse. Provide visual representations for easy understanding. | NIST - Best Practice |  |
| HTTP methods |  | Enumerate supported HTTP methods. Test for access control bypass. Test HTTP method overriding technique | OWASP - 4.7.3 | WSTG-CONF-06 |
| Wireless communication | ZigBee Network Security | Implement encryption and authentication measures for ZigBee devices. Protects against man-in-the-middle attacks and firmware compromises. | OWASP - Best Practice |  |