|  |  |  |  |
| --- | --- | --- | --- |
| LockGitech Door Lock | TR-64 Reference | TR64 Explanation | Description |
| Wi-Fi Module | * CS-02 * CS-03 | CS-02: Cryptographic algorithms for WPA2  CS-03: WPA2 employs symmetric AES encryption. | (CS-02/CS-03)  Integrated Wi-Fi module for wireless communication uses WPA2, which supports symmetric AES encryption. |
| ESP8266/ESP32 | * AP-02 * RS-01 | AP-02: Multi-factor authentications  RS-01: Device support integrity self-test, error detection and correction for critical functions | (AP-02) Use of OTP and fingerprint on the ESP8266 for 2FA unlocking of the door.  (RS-01) Checks the connection between AWS, Telegram, fingerprint, RFID, Keypad and LCD if they are all working and functional. |
| One-Time-Password | * CS-01 | CS-01: Random number generator for OTP. | (CS-01) Using a random number generator for the generation of One-time password. |
| LCD Module | * DP-01 | DP-01: Confidentiality and integrity of sensitive data protected at rest. | (DP-01) Only displays necessary information, such as door opening and closing, whilst not disclosing the RFID UID and fingerprint UID. |
| Servo Motor | * AP-03 | AP-03: Physical access restriction should be implemented to protect against unauthorised access to a device’s physical interface. | (AP-03) Motorized mechanism responsible for physically controlling the locking and unlocking mechanism of the door, offering secure and reliable operation. |
| Fingerprint Sensor | * IA-01 * IA-03 | IA-01: Client credentials should be stored securely, salted hashed, encrypted.  IA-03: Unique, non-modifiable and verifiable identities should be established for clients. | (IA-01/03) Fingerprint sensor is securely stored locally on the sensor, and the identities are non-modifiable as they are biometrics of a person. |
| Amazon Web Services IoT Core | * CS-02 * CS-04 * NP-03 * NP-04 * FP-01 * IA-02 * AU-01 * AU-02 * AU-03 | CS-02: Cryptographic algorithms employed.  CS-04: Use of RSA, and X.509 certificate chain  NP-03: Employ TLS when for TCP payloads.  NP-04: Employ TLS when using MQTT  FP-01: Security data elements in transit are protected  IA-02: Client should be authenticated before establishing connections, and after pre-defined intervals.  AU-01: Significant events are audited, such as telegram commands.  AU-02: Audit logs are protected from modification, deletion etc.  AU-03: Audit logs are encrypted. | (CS-02/CS-04) Use of industry standard asymmetric cryptography, such as X.509 and RSA.  (NP-03/ NP-04) AWS IoT Core employs RSA certificates for TLS certificates.  (FP-01) Data logging of telegram handle and commands are encrypted by MQTT and WPA2 protocol.  (IA-02) The Esp8266 is authenticated using the Ca-client certificate to certify the client, AWS certificate.  (AU-01/02/03) AWS IoT Core services are employed to conduct data logging of the Telegram messages to the bot. It is also digitally signed automatically, and send to a publish server, where it is encrypted in transit by the MQTT protocol. |
| RFID | * IA-03 | IA-03: Unique and non-modifiable identities for users. | (IA-03) RFID is unique to each user, and should be non-modifiable for users. |
| Telegram bot | * CS-02 * IA-02 * IA-03 * MT-01 | CS-02: Cryptographic algorithms should be industry recognised.  IA-02: Client should be authenticated before establishing connections.  IA-03: Unique, non-modifiable and verifiable identities should be established for clients and servers.  MT-01: A strong password policy (for user access) should be enforced. | Utilizes industry-accepted cryptographic techniques (CS-02) for secure communication.  (IA-02) Check if telegram user has been registered, (IA-03) and telegram handles are unique to each telegram user.  (MT-01) A strong password policy for telegram users (more than 8 characters for example) |