IOT SECURITY

DR. NINAD DILEEP MEHENDALE

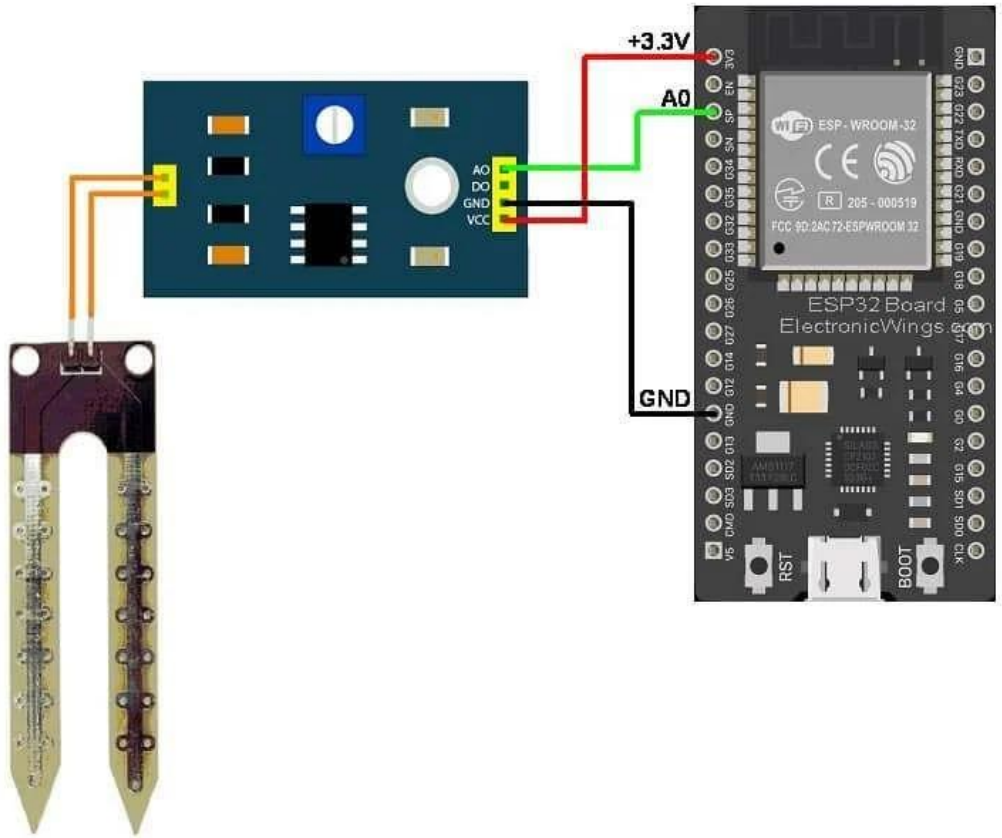
- #include <WiFi.h>
- #include <ThingSpeak.h>

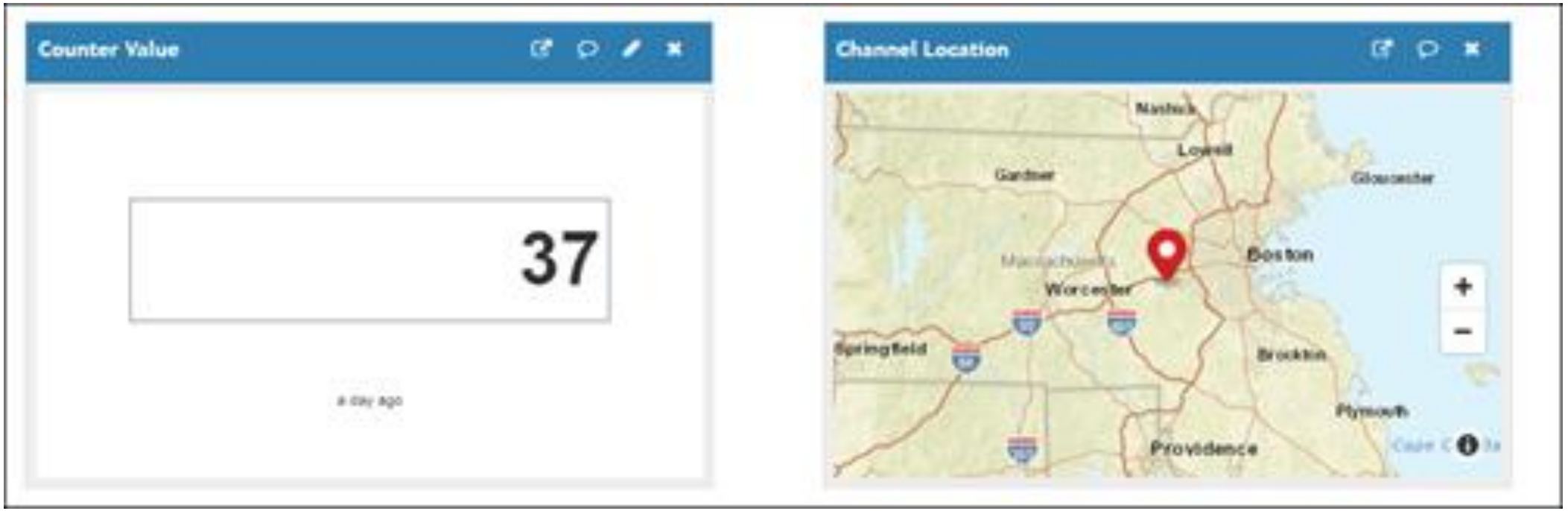
- const char* ssid = "your_ssid";
- const char* password = "your_password";

- unsigned long channelID = 123456;
- const char* apiKey = "your_api_key";

```
void setup() {
  Serial.begin(9600);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  ThingSpeak.begin(client);
}
```

```
void loop(){
  float temperature = analogRead(A0);
  ThingSpeak.writeField(channelID, 1, temperature, apiKey);
  delay(15000);
}
```


+3.3V
A0
GND
AO
DO
GND
VCC
ESP - WROOM-32
ESP32 Board
ElectronicWings.com
RST
BOOT


Counter Value
37
a day ago
Channel Location
Nashua
Lowell
Gardner
Gloucester
Boston
Worcester
Springfield
Brockton
Plymouth
Providence

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 1. **Authentication and Authorization:**
- - Ensuring that only authenticated and authorized devices and users can access IoT resources and data.
- - Implementing robust authentication mechanisms, such as passwords, certificates, or biometrics.
- - Defining fine-grained access control policies to limit the actions and data accessible by different entities.

AAV FRAMEWORK

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 2. **Data Encryption:**
- - Encrypting data both during transmission and storage to protect it from unauthorized access and interception.
- - Using strong encryption algorithms to ensure data confidentiality and integrity.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 3. **Secure Communication Protocols:**
- - Employing secure communication protocols like HTTPS, TLS/SSL to establish encrypted connections between devices and servers.
- - Avoiding the use of vulnerable or outdated protocols that could be exploited by attackers.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 4. **Secure Boot and Firmware Updates:**
- - Ensuring that IoT devices have a secure boot process to prevent the installation of unauthorized or malicious firmware.
- - Providing a secure mechanism for updating device firmware to patch vulnerabilities and improve security.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 5. **Device Identity and Management:**
- - Assigning unique identities to each IoT device to track and manage them effectively.
- - Implementing a centralized management system to control device access and configurations.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 6. **Secure API and Cloud Interfaces:**
- - Securing application programming interfaces (APIs) and cloud interfaces to prevent unauthorized access to IoT services and data.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 7. **Tamper Detection and Prevention:**
- - Incorporating tamper detection mechanisms in IoT devices to detect physical attacks or unauthorized access attempts.
- - Implementing measures to protect critical components from tampering.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 8. **Intrusion Detection and Prevention:**
- - Installing intrusion detection systems (IDS) to monitor network traffic and detect potential malicious activities or anomalies.
- - Implementing intrusion prevention systems (IPS) to block or mitigate detected threats.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 9. **Privacy Protection:**
- - Incorporating privacy-by-design principles to safeguard users' personal data and ensure compliance with data protection regulations.
- - Anonymizing or pseudonymizing data when possible to protect user identities.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 10. **Physical Security:**
- - Securing physical access to IoT devices and infrastructure to prevent unauthorized physical access.

SECURITY REQUIREMENTS IN IOT ARCHITECTURE

- 11. **Secure Software Development Practices:**
- - Following secure coding practices during IoT application and firmware development to minimize vulnerabilities.

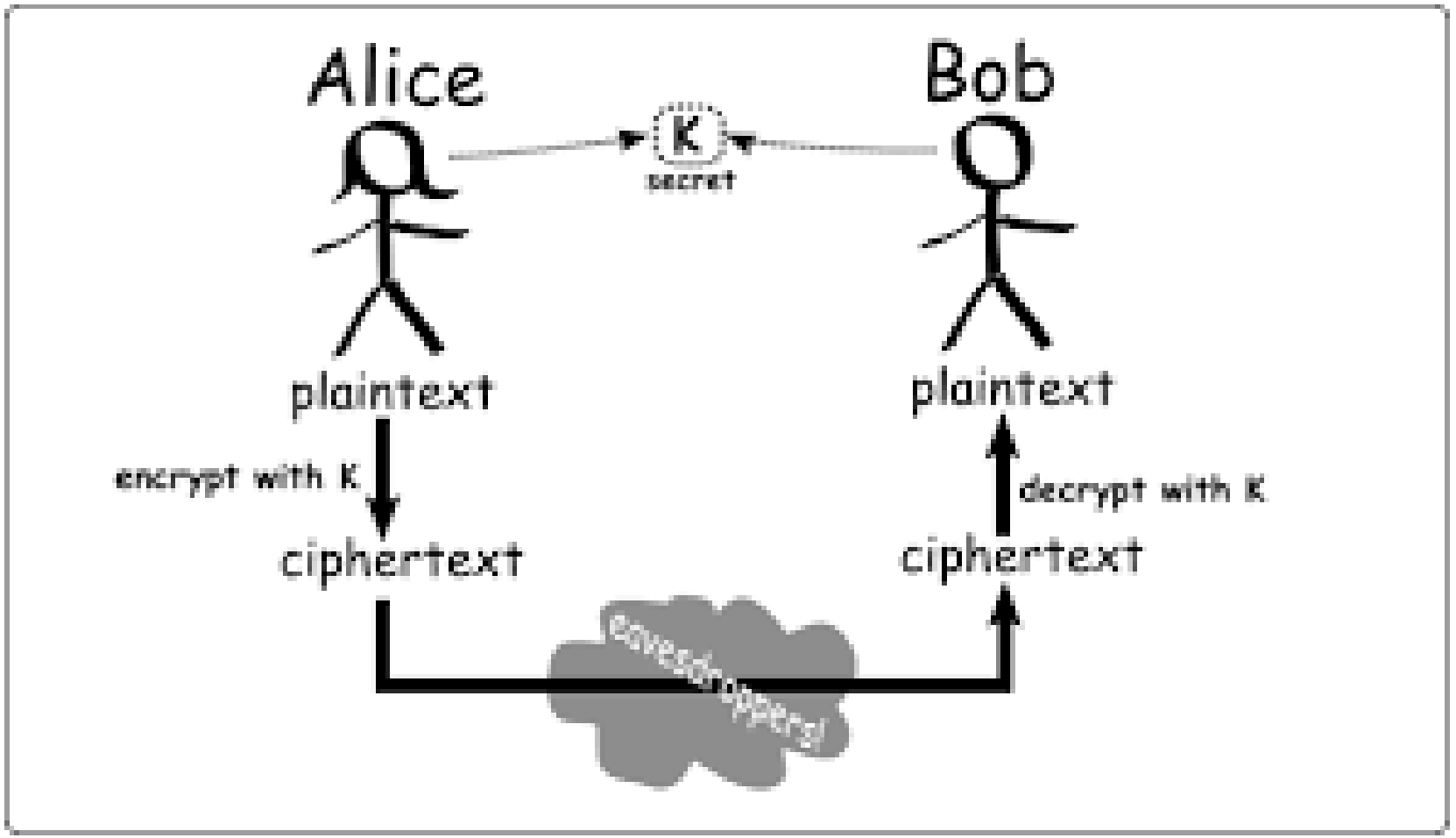
SECURITY REQUIREMENTS IN IOT ARCHITECTURE

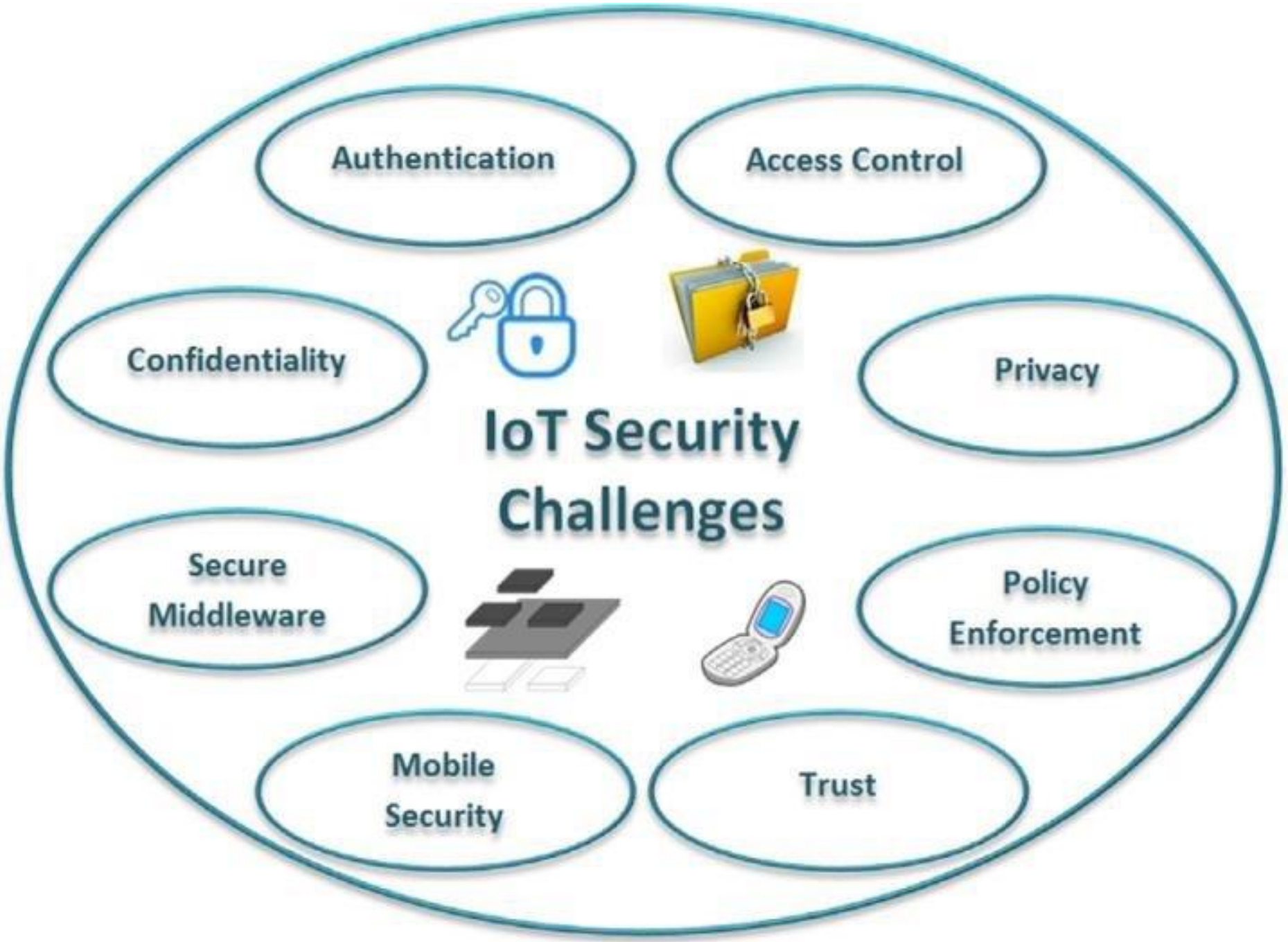
- 12. **Regular Security Audits and Testing:**
- - Conducting regular security audits and penetration testing to identify and address potential weaknesses in the IoT architecture.

IOT SECURITY REQUIREMENTS

Layer	Security Requirements
Perception	Lightweight Encryption
	Authentication
	Key Agreement
	Data Confidentiality
Network	Communication Security
	Routing Security
	Authentication
	Key Management
	Intrusion Detection
Application	Authentication
	Privacy protection
	Information Security Management

ENCRYPTION


Alice
Bob
K
secret
plaintext
plaintext
encrypt with K
decrypt with K
ciphertext
ciphertext
eavesdroppers!


Authentication
Access Control
Confidentiality
Privacy
IoT Security Challenges
Secure Middleware
Policy Enforcement
Mobile Security
Trust

IoT SECURITY

IoT Security Lifecycle


IoT SECURITY
IoT Security Challenges
01
Confidentiality
02
Authentication
03
Access Control
04
Privacy
05
Policy Enforcement
06
Trust
07
Mobile Security
08
Secure Middleware

IoT SECURITY

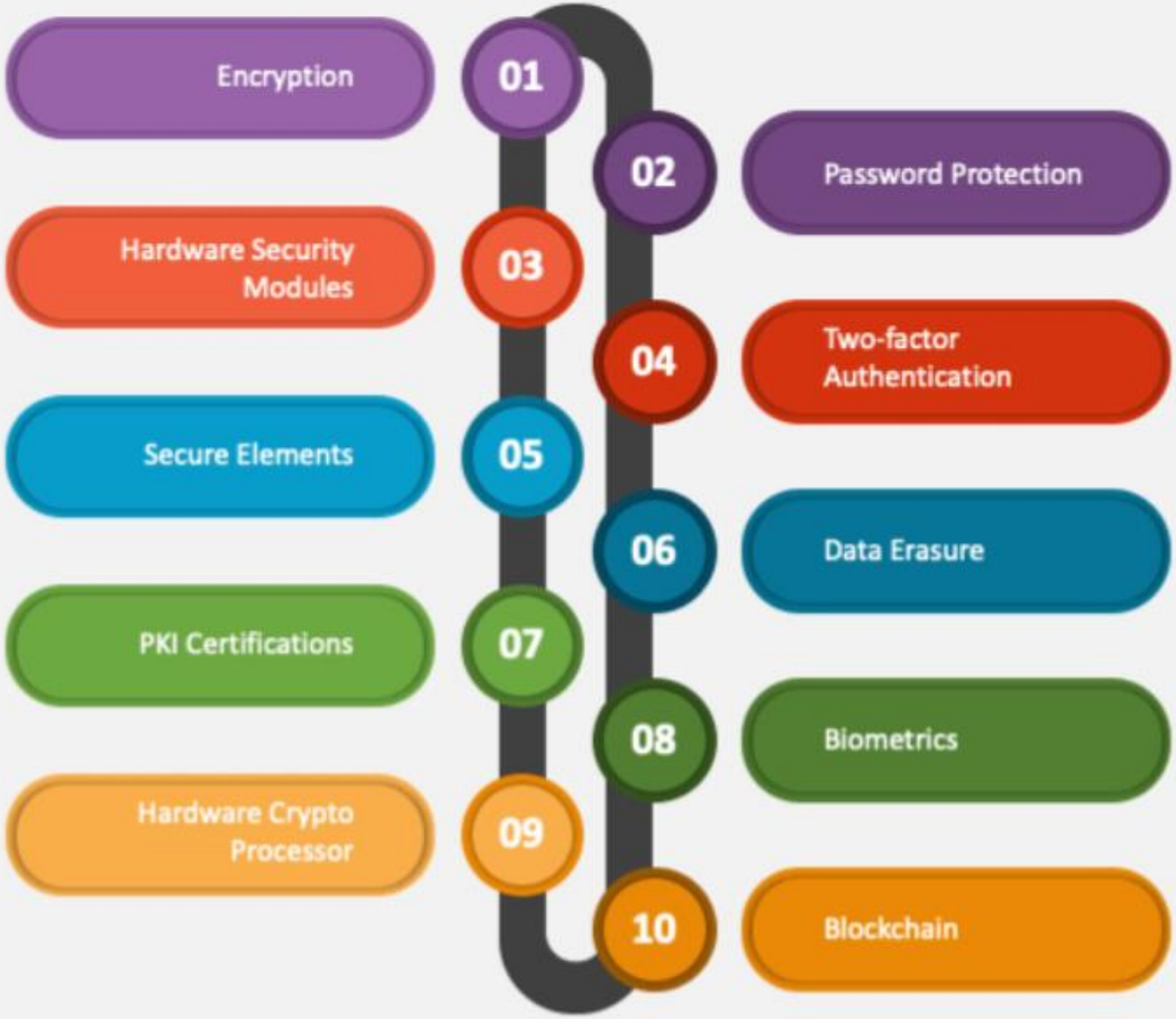
Problems of IoT Security

IoT SECURITY

Ways to Improve IoT Security

IoT SECURITY

IoT Security Tools



WHAT I S SECURITY?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

WHAT I S INFORMATION SECURITY?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology

SECURITY CONCEPTS