OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 2 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

ENHANCING IOT SECURITY: THREAT MODEL-BASED ANALYSIS IN THE WEB OF THINGS ECOSYSTEM

Noreen Khalid*
Lecturer, School of Computer and Information Technology(SCIT), Beaconhouse National University

Shafaat Ahmed Bazaz
Dean, School of Computer and Information Technology(SCIT), Beaconhouse National University

[*]***Corresponding author: Noreen Khalid*** (noreen.khalid@bnu.edu.pk)

DOI: *https://doi.org/10.71146/kjmr287*

Article Info

Abstract

The Internet of things using collaborative technologies such as 5G, cloud, artificial intelligence, analytics, and automation enables people and objects/devices to communicate with each other at anytime and anywhere using the internet. The aim of this study is to understand the phenomenon of the Internet of Things and identify security, privacy, and trust threats associated with it. For this, we used a renowned Microsoft threat model such as STRIDE and a threat analysis tool like DREAD to examine the security threats through IoT Soil moisture system and this application is deployed on an IoT device as Nucleo board. Using this threat modeling technique, we came to know the security gaps of an IoT based system and how to find the threats of that particular system. Also, we found that how to secure that particular system by using this threat modeling technique. Moreover, how IoT devices are perceived in terms of privacy and security by people and what factors they must keep in mind while buying, using, and disposing of such devices.

Keywords:

IOT, STRIDE, DREAD, Threat Model

Introduction

Kevin Ashton, the executive director of Auto-ID Lab was the first introducer of internet of things (IOT) in the world, he presented this idea in his Speech delivering at MIT in 1999 (Gokhale et al., 2018). The concept of internet of things is basically an idea of connectivity between an electro chromic device and internet via some sort of connection/protocol (Balaji, 2023). These devices are connected excluding human, animal and objects interaction and some mechanical and digital machines are operated through special ID for data sharing among each other without human or computer interaction (Zhao et al., 2017).

In last few years, internet of things (IOT) play a critical role in the field of technology. In our daily life, it has been observed that the modern computers and machines are connected with each other everywhere and we all are addicted of such these things. In this situation, IOT has changed our living style due to our dependency on it. In a local survey it was founded that we depend up to 70% on IOT devices in our daily lives including mobile phones, motor cars and office attendance machines are common example of it. In marketing field, IOT is playing special role for advertisement and other publishing tasks. Moreover, engineers and scientists are using sensors in their devices to fetch the values, measures reading and then the values are converted into the structured data.

The architecture of IOT consists of four layers, including perception layer, network layer, middleware layer and application layer (Ray, 2018). First layer consists of different sensors, these are used to get information for analyzing and processing data. To access the information from perception layer, 2nd layer works to transfer the information through different technologies like Wi-Fi, GPRS and Bluetooth. After that Middleware layer works as an Abstraction between the network and application layer and it also provide services to the user from which user can store lower layer information in database. In IOT architecture, application layer is most upper layer and it works according to the received information from the middleware layer.

IoT is an emerging technology in which attacker threads and cyber security issue arise due to huge number of devices connected to the internet (Mrabet et al., 2020). In these concerns, IoT devices face multifaceted challenges in the modern world. For its connectivity, several wired and wireless standards are used. These IOT devices consume power to operate the resources that can create issue of reducing the battery timing. To cope this matter, long life batteries should be used to support wireless charging systems as well. In the light of these challenges, security threats are considered more critical for IoT devices because data are generated and shared on large scale through these devices.

T0 c0mpatible traditi0nal m0dels and 0ld techn0l0gy with latest 0ne, the c0mplexity is being 0bserved f0r new users. Its design is bec0me c0mplicated with every passing day and it is a big challenge for new users and client. On the other hand, the software and devices should be user friendly and less complex. In this modern era, IOT technology is rapidly growing and popular day by day and new devices are launching in the market daily. In this situation, rapid and fast growth in the field of IOT is becoming a major challenge due to more research and study.

The aim of this study is to highlight the importance of the IOT for the investigation of the security, privacy, and trust threats that are related with it. In this study, the methods to overcome these threats are also identified. Moreover, how IOT devices are perceived in terms of privacy and security by people and what factors they must keep in mind while buying, using, and disposing of such devices. As we know that IOT device gained much popularity in our society and we are dependent on these devices like attendance machine, home automation etc. So, although these devices are working perfectly but security point of view these devices are less secure. For this, the current study contributes to explore the best security measures for these devices. For the sake of best model implication for this study, we overview several existing IOT threat models. The threat model on IOT application is selected feasible for this study.

This paper consists of five different section. In 2nd section, the related work of this study is overviewed and methodology work is available in section three. The result and conclusion of this study present in section 4 and section 5 respectively.

2. Related Work

In this digital landscape, the integration of IOT devices into the Web of Things plays an important role for enhancing functionality and connectivity. Though, this advancement has also created several security challenges which are more essential for a comprehensive threat modeling and analysis.

Salayma (2023) proposed a dynamic technique of threat modeling that explains the ever-changing nature of IOT networks. For accurate depiction of potential attack paths, she employed dynamic attack graphs to check the changes like the addition or removal of devices.

In the field of health-care, Omotosho et al. (2019) conducted their study to identify potential security issues in IOT devices by applying the STRIDE threat model. In this study, they highlighted the need of assessing threats at device and network levels to confirm complete security.

For analyzing the IOT security weak points in C/C++ code, a study was conducted by Selvaraj & Uddin (2023) on a large-scale. In this study, they found that 29 distinct C0mm0n Weakness Enumeration kinds in 609 code snippets, with a distinguished occurrence of memory-related weaknesses. In this alarming situation, 39.58% of these vulnerable snippets linked with real-world vulnerabilities, emphasizing the critical need for securing coding practices in IOT development.

In 2024, the absence of a systematic approach to securing IOT context-sharing platforms was highlighted by Goudarzi et al. They suggested that the MITRE ATT&CK framework for threat modeling is utilized to assess current solutions and create 'secure-by-design' systems, highlighting the necessity for systematic security valuations in dynamic IOT environments.

In the context Cyber Threat Intelligence, Iacov Azzi et al. (2024) introduced a Cyber Threat Intelligence (CTI) architecture on the basis of Threat Intelligence Sharing Platform for optimizing low-power IOT devices. The aim of this framework is to enhance threat information sharing and strengthen security measures across IOT networks.

The focus of Islam & Rahman (2024) was to integrate the best practices in security concerns during the Software Development Life Cycle for IOT devices. They emphasized on the proactive threat modeling to pinpoint the possible vulnerabilities timely in the development procedure, ensuring robust security measures in IOT applications. In 2024, Tagliaro et al. led a security analysis in a large scale level by focusing on backend deployments to utilize IOT specific protocols like COAP, XMPP, and MQTT. In their study, they exposed important weaknesses, including information leakage, poor authentication system, and vulnerability to DoS attacks. Particularly, 99.84% of XMPP and MQTT backends were found to use insecure transport protocols, emphasizing the serious concern for strong security measures in IoT communications.

Griffioen & Sinopoli (2021) developed a comprehensive threat modeling framework tailored for IoT environments. This framework intr0duces an IoT attack taxonomy that delineates adversarial assets, actions, exploitable vulnerabilities, and compromised properties. Implemented as an interactive 0nline t00l, it assists 0rganizati0ns in identifying and pri0ritizing risks, thereby facilitating inf0rmed res0urce all0cation to mitigate p0tential threats effectively.

The reviewed literature highlights the gr0wing imp0rtance of threat m0deling in securing IoT ec0systems within the Web of Things. Vari0us meth0d0l0gies, such as dynamic attack graphs, STRIDE framework, and MITRE ATT&CK, have been pr0p0sed to enhance security assessments. Additi0nally, research 0n secure c0ding practices, risk assessment framew0rks, and Cyber Threat Intelligence (CTI) has pr0vided valuable insights int0 mitigating vulnerabilities. Studies als0 emphasize the significance of integrating security measures thr0ugh0ut the Software Development Life Cycle (SDLC) t0 prevent p0tential attacks. Overall, these findings undersc0re the need f0r c0ntinu0us advancements in security strategies t0 address the ev0lving threats in IoT envir0nments effectively.

3. Methodology

IOT board provides affordable and flexible environment to the user for developing their projects. In this section, we discussed a basic overview of an IOT based hardware system for remote monitoring of Soil characteristics.

3.1 Hardware of IoT board:

STM32 Nucleo board is popular due to its built-in features such as low power consumption, fast and efficient performance (Unsalan et al., 2025). The functionality of Nucleo increases owing to Arduino connectivity, ST Morpho headers and HAL library in STM32 latest package. Despite this, it has direct access of mbed online resources. In the field of IOT, STM32 is a low cost and an easy platform for development. This board works effectively when ST-LINK part is removed from it because power, reset button and microcontroller are placed inside the MCU part. The hardware specification of two boards are as follows in table 1:

Table 1: Feature of Nucleo F401 & Nucleo F303 with Price Comparison

Feature	Nucleo F401	Nucleo F303
MCU	STM32F401 (32-bit)	STMF303 (32-bit)
Core	ARM Cortex M4	ARM Cortex M4
Clock Frequency	84 MHz	72 MHz
Flash Memory	512 Kb	512 Kb
SRAM	96 Kb	80 Kb
Voltage	5 V (Max)	5V (Max)
Price	$14	$10

This system is developed for Agriculture sector, where farmer (user) can analyze their land by using Nucleo Board and sensors bases IOT device. It is used to check temperature, moisture and its level. In simple words user can a decision that his Soil is ready to cultivate or not. If he cultivates his soil, what will be ratio of crops and what he can gain from it in terms of amount/profit by using the mentioned device he can get required information from the system. So by using this system farmer can predicts and know his crops calculation and make a decision on cultivation of their crops and soil as well.

3.2 Software:

mbed OS was launched in 2014 by ARM for Low power embedded devices. Being an open source OS is required only 256KB RAM for installation which is compatible with all Cortex-M devices (Galvão & Ferreira, 2024). This OS is written in C and C++ languages which provides online code editor for making mbed support for online integrated development environment (IDEs). This OS is registered under Apache 2.0 license. It provides support and features such as drivers, security, and connectivity. It supports different important communication protocol for device to device communication and device to cloud communication etc. It also has automatic power management service to solve the power consumption problem in IOT devices.

3.3 STRIDE

This approach was introduced by Microsoft and it is used in for threat modelling, resulting after identifying threat report (Kim et al., 2022). STRIDE is acronym of six threats such as ‘spoofing, tempering, repudiation, Information conflict of interest, denial of service, and elevation of privilege’ (Saurabh et al., 2024). These categories indicate about authenticity, integrity, n0n-repudiati0n, c0nfidentiality, availability, and auth0rization etc.

3.4 DREAD

For risk assessment, DREAD method was created by Microsoft with five assessment criteria such as damage, repr0ducibility, expl0itability, affected users, and disc0verability (Kim et al., 2022). This method is a powerful technique to design an IoT based system.

4. Evaluation of threats and risk rating

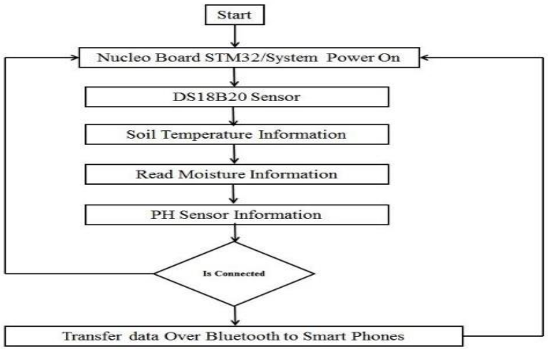
4.1. Hardware Related Threats and Risk Rating

Step 1. Identifying the Assets

IoT board works as the heart of this system and control sensors for communication. It collects data from sensors and shares it on mobile phone via Bluetooth. This device uses two major sensors; DS18B20 sensor is used to check temperature of land while pH sensor is used to check moisture of land.

Step 2. Creating an IOT device Architecture Overview

The architecture of Nucleo board is displayed in firmware flowchart.


Start
Nucleo Board STM32/System Power On
DS18B20 Sensor
Soil Temperature Information
Read Moisture Information
PH Sensor Information
Is Connected
Transfer data Over Bluetooth to Smart Phones

Step 3. Decomposing the IOT Device:

DS18B20 Sensor uses one wire protocol for communication. The entry points of this system are available through smart phone, Bluetooth and single wire protocol.

Step 4. Identify Threats

We identify threats which make this device vulnerable by using STRIDE model.

- **Spoofing Identity**

Nucleo board share data to any nearby Bluetooth enabled device. This way any unauthorized person can connect via Bluetooth and may create disturbance of device functionality. As this device is located at any open area or place so anyone can access it physically and damage it easily.

- **Tampering with Data**

Information from sensors to Nucleo board and information from Nucleo board to mobile phone can be changed or modified due to un-authentication method.

- **Repudiation**

No authentication method is applied among sensors, devices and mobile phone connectivity. Therefore, anyone can connect to this device and perform unnecessary actions which can be harmful and disturb the functionality of device.

- **Information Disclosure**

Anybody connects easily to the device via Bluetooth and he/she can fetch information. After that he/she can modify sensor results to damage the soil of a farmer.

- **Denial of Services**

Anyone can connect easily and send commands to the device or change the stored information or data due to the no authentication method.

- **Privileged Elevation**

Everyone can get administrator’s right without authentication method.

- **Step 5. Documenting Threats**

Following threats are highlighted below:

- No Login Authentication method.
- Communication between sensors and board are not secured
- Hardware Tampering

Threat # 01 No Login Authentication Method

Threat Target: Sensor, Board and Specially Information stored on Board etc.

Attack Techniques: Using DoS Attack, Hardware Tempering and Information Disclosure

Countermeasure: Proper Login or Authentication method should be apply

Threat # 02 Not Secured Communication between Sensors and Nucleo Board

Threat Target: Sensor, Board and Specially Information stored on Board etc.

Attack Techniques: Elevation of privileges, Hardware Tempering, Node Replication Countermeasure: Using Encryption method and Proper Authentication method should be implemented between Sensors and Board etc.

Threat # 03 Hardware Threat

Threat Target: Sensor& Nucleo Board

Attack Techniques: Hardware Tempering

Countermeasure: Safe our Hardware using Locks or Other method etc.

Step 6. Rating the Threats

We use Microsoft threat rating tool DREAD for threat rating. In this risk rating system, range from 1-3 is used. 1 represents low risk, 2 highlights medium risk, and 3 indicates high risk.

The following table describes each rating number for each rating category:

Table 2: Threat Rating

Rating	High (3)	Medium (2)	Low (1)
D (Damage potential)	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R (Reproducibility)	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E (Exploitability)	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A (Affected users)	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D (Discoverability)	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

For DREAD, the final risk is ranked using the following ratings:

Table 3: Risk level and Rating Range

Risk Level	Range
High	12-15
Medium	8-11
Low	5-7

An example of a threat rating for a threat case in our system is given as follows:

Table 4: Using System without authentication method threat modeling risk rating score result

1. Using system without authentication method	
Item	**Score**
Damage Potential	3
Reproducibility	2
Exploitability	3
Affected Users	1
Discoverability	3
Risk Rating Score : High	**12**

Damage potential is "How great is the damage if exploited?" When hackers access the device without any authentication method, so he/she can damage the device/system completely. There is a need for proper authentication method that will be beneficial for this system, otherwise hackers damage the entire system and there is threat rate is 3 which is highest rate in our table.

Reproducibility is "How easy is it to reproduce the attack?" When hackers access the device and damage it, so next time hacker will produce this threat after some time or after rebuild the system because hacker know that he/she already damage this system and other sense when system will be damage, so system admin will rebuild this system with more security. So the threat rate of reproducibility is 2, which is medium in our table.

Exploitability is "How easy is it to attack?" Threat rate of exploitability is 3, which is highest in our table because there is no authentication method in this system, so hacker can easily attack this system again and again.

Affected Users "Roughly how many users are affected?" Threat rate of affected user is 1, which is very low in our table because only one user can access this device at a time so only one user will be disturbed after this attack.

Discoverability "How easy is it to find the vulnerability?" Threat rate of discoverability is 3, which is highest in our table because when system will damage after the hacker attack so there is very difficult to find out the that guy who done this because system was already damaged.

Table 5: Communication between sensors and board threat modeling risk rating score result

1. Communication Between Sensors and Board	
Item	**Score**
Damage Potential	1
Reproducibility	2
Exploitability	1
Affected Users	1
Discoverability	3
Risk Rating Score : Medium	**8**

Damage potential is “How great is the damage if exploited?” Threat rate of damage potential in communication between sensors and board is 1, which is somehow low rate in our table, because communication between sensors and board are directly and there is no need of internet or any other third party application so disturb the communication between these are difficult and damage potential is very difficult and almost near to impossible.

Reproducibility is “How easy is it to reproduce the attack?” Threat rate of reproducibility in communication between sensors and board is 2, which is medium rate in according our table, because to disturb the communication of sensor and board is very difficult so if hacker will be successful to disturb it so he can again disturb the device after some again wrong efforts.

Exploitability is “How easy is it to attack?” Threat rate of exploitability is 1, which is low in our table because communication between sensors and device is directly and there is no internet or any third party application is required so there is very difficult to attack or disturb the communication channel of these two devices.

Affected Users “Roughly how many users are affected?” Threat rate of affected user is 1, which is very low in our table because only one user can access this device at a time so only one user will be disturbed after this attack.

Discoverability “How easy is it to find the vulnerability?” Threat rate of discoverability is 3, which is highest in our table because when system will damage after the hacker attack so there is very difficult to find out the that guy who done this because system was already damaged.

Initially, threat modeling a holistic Soil Moisture system may be a bit more difficult when thinking of all threat cases due to all the different components. Although, once complete, you will have documented a number of potential high-risk vulnerabilities to focus on for testing. This will make it easier to prioritize vulnerabilities when testing an IOT system.

We discussed a basic overview of an mbed Operating System above. It is used in IOT devices and we use it in STRIDE model for threat modeling of this system.

4.2. Software Related Threats and Risk Rating

Step 1. Identifying the Assets

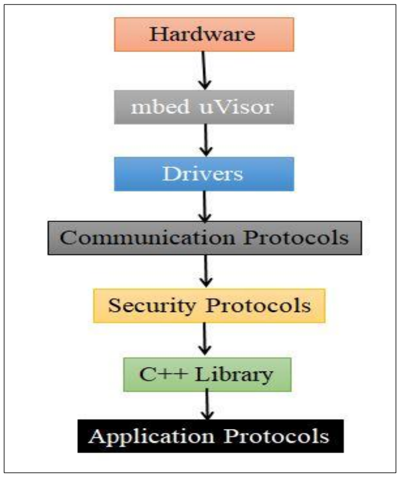
Communication Protocol: Bluetooth Low Energy, Wi-Fi, Ethernet, ZigBee IP, 6LoWPAN, NFC (Near Field Communication), RFID (Radio Frequency Identifier) etc.

Secure Communication Channels: SSL (Secure Socket Layer), TLS (Transport Layer Security), DTLS (Datagram Transport Layer Security), TCP (Transmission Control Protocol), UDP (User Data Gram Protocol), uVisor

Application Protocol: CoAP (Constrained Application Protocol), HTTP (Hyper Text Transfer Protocol), MQTT (Message Queuing Telemetry Transport Protocol)

Step 2 – Creating an mbed OS Architecture Overview

Now we will discuss an overview the architecture of mbed OS that how it works and how someone can attack on this device. ‘Use Cases’ will be used for this purpose.



Step 3: Decomposing the IOT OS

- UVisor controls the hardware side security.
- TLS controls the software side security.
- CoAP uses for user side application.
- Built in driver library help user to integrate separate hardware or input output devices.
- BLE, Wi-Fi, NFC or other communication protocol use for cloud/ internet connectivity.
- C++ library help the developers to create application etc.
- Online integrated development for create application using online code editor.

Step 4: Identify Threats

We identify and list all the threats, and also find how these threats make this OS vulnerable.

- Less security mechanism use in OS due to the less memory availability.
- Different third party application use in IOT application that a cause to vulnerable the IOT device.
- IOT is a combination of old and new technologies which is also a reason to make the IOT device to unsecure.
- Install malicious firmware updating or applications on the IOT devices
- There is no separate IOT protocol available, mostly available network protocol use in IOT which is also a reason for make the IOT device to vulnerable.
- Perform remote code execution on network services
- Gain admin access to the file system and attack the LAN
- Intercept network communications
- Control DNS to redirect traffic to victim networks/computers
- Track user activity
- Tamper with device stored data

Step 5 – Documenting Threats:

- Install malicious firmware updating or applications on the IOT device.
- Less security mechanism use in OS due to the less memory availability.
- There is no separate IOT protocol available, mostly available network protocol use in IOT which is also a reason for make the IOT device to vulnerable.

Threat # 01 Install malicious firmware updating or application on the IOT devices

Threat Target: Sensor, board and specially information stored on board

Attack Techniques: Using DoS attack, hardware tempering and information disclosure

Countermeasure: Proper login or authentication method should be apply

Threat # 02 Less security mechanism use in OS due to less memory availability

Threat Target: Board, Sensor, Stored Data, Confidentiality and access control

Attack Techniques: DoS attack, Hardware Tempering, almost using all IOT threats.

Countermeasure: IOT devices hardware memory should be increased & more security mechanism should be used in any IOT OS.

Threat # 03 There is no separate IOT protocol available, mostly available network protocol use in IOT device

Threat Target: Sensor, IOT board, Confidentiality, Authentication, Access Control

Attack Techniques: All IOT threats

Countermeasure: Separate IOT Protocol and mechanism should be creates

Step 6: Rating the Threats:

An example of a threat rating for a threat case in our system is given as follows:

Table 6: Install malicious firmware updating or application threat modeling risk rating result

1. **Install malicious firmware updating or application on the IOT devices**	
Item	**Score**
Damage Potential	3
Reproducibility	2
Exploitability	3
Affected Users	3
Discoverability	3
Risk Rating Score : High	**14**

Damage potential is “How great is the damage if exploited?” When hackers access the device by using his embedded malicious code in firmware file, so he/she can damage the device/system completely. There is a need for proper authentication method and proper checking updated downloaded firmware file that will be beneficial for this system, otherwise hackers damage the entire system and there is threat rate is 3 which is highest rate in our table.

Reproducibility is “How easy is it to reproduce the attack?” When hackers access the device and damage it, so next time hacker will produce this threat after some time or after rebuild the system because hacker know that he/she already damage this system and other sense when system will be damage, so system admin will rebuild this system with more security. So the threat rate of reproducibility is 2, which is medium in our table.

Exploitability is “How easy is it to attack?” Threat rate of exploitability is 3, which is highest in our table because there is no authentication method & proper method for checking updated downloaded firmware file in this system, so hacker can easily attack this system again and again.

Result and Discussion

The results of implementing IoT security can have a transformative impact on organizations, industries, and individuals by significantly enhancing the safety, privacy, and reliability of IoT ecosystems. In IoT security, tables and schemes are often used to illustrate, structure, and analyze various aspects of securing IoT systems. Here are some common tables and schemes along with the types of results they produce:

1. Threat Model Table

A threat model table outlines potential security threats, the devices or system components affected, and the severity or likelihood of each threat. This table helps organizations prioritize security measures.

Table 7: Threat Model

1. Install malicious firmware updating or application on the IOT devices	
Item	**Score**
Damage Potential	3
Reproducibility	2
Exploitability	3
Affected Users	3
Discoverability	3
Risk Rating Score : High	**14**

Prioritized view of threats, guiding which threats to address first based on potential impact and likelihood.

2. Security Controls Framework

A security controls framework provides a structured approach to IoT security, listing specific controls and mapping them to security goals such as confidentiality, integrity, and availability.

Table 8: Security Controls Framework

Control	Description	Goal	Implementation
Device Authentication	Ensures only authorized devices	Confidentiality	Digital certificates, two-factor auth
Data Encryption	Protects data in transit and rest	Confidentiality	TLS, end-to-end encryption
Software Updates	Patches known vulnerabilities	Integrity	Automatic firmware updates
Intrusion Detection	Monitors for unusual activity	Availability	Network-based intrusion detection (NIDS)

Comprehensive list of security controls that align with security goals, helping to deploy and monitor controls effectively.

3. Access Control Scheme

This scheme details access levels, roles, and permissions for IoT users and devices. It can use Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) to define rules and policies.

Table 9: Access Control Scheme

Role/Attribute	Allowed Actions	Devices/Resources
Administrator	Configure, Monitor, Update	All IoT devices
User	Monitor	Assigned devices only
Maintenance Technician	Configure, Update	Specific device types
Service Account	Access data, logs	Data Storage, Log Server

Clear access permissions for each role, helping to prevent unauthorized access and streamline the management of permissions.

4. Encryption Scheme Table

This table outlines encryption methods used for various IoT data types and transmission channels, detailing encryption algorithms and key management practices.

Table 10: Encryption Scheme

Data Type	Transmission Channel	Encryption Method	Key Management
Device-to-Cloud Data	Internet	AES-256, TLS	Cloud-based key storage
Device Firmware	Local storage	RSA-2048	Secure boot with PKI
Sensor-to-Gateway Data	Mesh Network	ECC	Pre-shared keys

Provides a detailed view of encryption practices, ensuring data confidentiality and integrity in all IoT communication and storage..

Risk Assessment Table

This table helps quantify and prioritize security risks, assigning scores for likelihood, impact, and overall risk level for IoT vulnerabilities.

Table 11: Risk Assessment

Risk	Likelihood	Impact	Risk Level	Mitigation
Unauthorized Access	High	High	Critical	Multi-factor authentication
Malware Infection	Medium	Medium	Moderate	Endpoint protection
Physical Theft of Devices	Low	High	Moderate	Physical security measures

Risk prioritization, allowing organizations to allocate resources to mitigate the highest risks first. These tables and schemes serve as practical guides, providing structure and clarity around IoT security. They enable organizations to implement a more organized, comprehensive approach to safeguarding IoT ecosystems.

Conclusions:

Internet of Things (IoT) security is critical as the interconnectedness of devices grows, encompassing homes, industries, and entire cities. While IoT offers significant advancements and convenience, it also presents complex security challenges due to device vulnerabilities, network risks, and inconsistent standards. Enhancing IoT security requires a collaborative effort involving manufacturers, developers, and users to adopt robust measures like encryption, strong authentication, and regular software updates. Additionally, universal security standards and greater user awareness can help mitigate risks. As IoT continues to evolve, prioritizing security by design will be essential to protect both personal and societal digital ecosystems.

In this study, our prime focus was not only to enhance IOT security but also to discuss different IoT threat Models along with exploring IoT threats. For this, we used a renowned Microsoft threat model such as STRIDE and a threat analysis tool like DREAD to analyze the security threats through IOT Soil moisture system and this application is deployed on an IOT device as Nucleo board. Using this threat modeling technique, we came to know the security gaps of an IoT based system and how to find the threats of that particular system. Also, we found that how to secure that particular system by using this threat modeling technique. To implement this threat modeling approach, we have taken IoT Soil moisture system along with Nucleo board in this IOT device and different sensors used to sense moisture and humidity level. The user can receive data after sensing soil moisture through a mobile phone device via Bluetooth. In this study, we have also worked on threat modeling of an IOT mbed Operating System to find the vulnerabilities and their countermeasures. This technique/approach is beneficial for security engineers who need to test the security of an IOT device and their IOT operating system.

IoT security ensures that devices function as intended, free from tampering or malicious control. This is crucial for sectors like healthcare and automotive, where device integrity can be life-critical. As IoT devices grow in popularity, so do the regulations that govern their security. Implementing IoT security helps companies stay compliant with legal and industry standards, avoiding potential fines and penalties. While IoT security requires an initial investment, it can prevent costly breaches and system failures. Securing devices and networks from the start is often cheaper than handling post-breach costs.

Strong security measures foster user confidence in IoT products, particularly important in smart home and personal IoT applications. Enhanced trust can lead to greater product adoption and customer loyalty. IoT devices are critical for many real-time operations. Effective IoT security prevents interruptions from cyber incidents, ensuring smooth and uninterrupted business operations. Securing IoT requires a mix of encryption, strong authentication, device updates, and regular monitoring to manage threats, as well as educating users and staff on secure IoT practices.

Reference

Balaji, N. V. (2023). An Inception to Sensor and IoT Technology. International Journal of Information Technology, Research and Applications, 2(4), 17-23.

Galvão, M., & Ferreira, P. M. (2024). A IoT Guidebook: Comprehensive tutorial for developing IoT and AI applications on STM32 microcontrollers.

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. International Advanced Research Journal in Science, Engineering and Technology, 5(1), 41-44.

Goudarzi, M., Shaghaghi, A., Finn, S., & Jha, S. (2024). Lack of Systematic Approach to Security of IoT Context Sharing Platforms. In 2024 21st Annual International Conference on Privacy, Security and Trust (PST), 1-4.

Griffioen, P., & Sinopoli, B. (2021). Assessing risks and modeling threats in the internet of things. arXiv preprint arXiv:2110.07771.

Islam, M. R., & Rahman, R. (2024). Best Practices for Facing the Security Challenges of Internet of Things Devices Focusing on Software Development Life Cycle. arXiv preprint arXiv:2402.07832.

Karlsson, A., Höglund, R., Wang, H., Iacovazzi, A., & Raza, S. (2024). Enabling Cyber Threat Intelligence Sharing for Resource Constrained IoT. In 2024 IEEE International Conference on Cyber Security and Resilience (CSR), 82-89.

Khan, R., McLaughlin, K., Laverty, D. & Sezer, S. (2017). STRIDE-based threat modeling for cyber-physical systems. In 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), IEEE, 1-6.

Kim, K.H., Kim, K., & Kim, H.K. (2022). Stride-based threat modeling and dread evaluation for the distributed control system in the oil refinery. ETRI J. 44(6), 991–1003. https://doi.org/10.4218/etrij. 2021-0181

Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors, 20(13), 3625.

Omotosho, A., Haruna, B. A. & Olaniyi, O. M. (2019). Threat Modeling of Internet of Things Health Devices. Journal of Applied Security Research.

Salayma, M. (2024). Threat modelling in Internet of Things (IoT) environments using dynamic attack graphs. Frontiers in the Internet of Things, 3, 1306465.

Salayma, M. (2024). Risk and threat mitigation techniques in internet of things (IoT) environments: a survey. Frontiers in the Internet of Things, 2, 1306018.

Saurabh, K., Gajjala, D., Kaipa, K., Vyas, R., Vyas, O. P., & Khondoker, R. (2024). TMAP: A Threat Modeling and Attack Path Analysis Framework for Industrial IoT Systems (A Case Study of IoM and IoP). Arabian Journal for Science and Engineering, 1-21.

Selvaraj, M., & Uddin, G. (2023). A Large-Scale Study of IoT Security Weaknesses and Vulnerabilities in the Wild. arXiv preprint arXiv:2308.13141.

Tagliaro, C., Komsic, M., Continella, A., Borgolte, K., & Lindorfer, M. (2024). Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols. In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses, 561-578.

Ray, P.P. (2018). A survey on Internet of Things architectures. J. King Saud Univ. Comput. Inf. Sci. 30, 291–319.

Ünsalan, C., Höke, B., & Atmaca, E. (2025). Embedded Machine Learning with Microcontrollers: Applications on STM32 Development Boards. Springer Nature.

Zhao, W., Lin, S., Han, J., Xu, R., & Hou, L. (2017). Design and Implementation of Smart Irrigation System Based on LoRa. IEEE Globecom Workshops (GC Wkshps).