

Özyegin University

CSC-399 Communications Security

**PROJECT TITLE:**

Security Analysis of Water Metering Management Systems in Smart Cities

**Student Name:**

Özgür Yılmaz

**Project Topic:**

Water Metering Management – Smart Cities

**Local LLM Model Used:**

LLaMA 2 – 13B (Ollama Local Deployment)

**Instructor:**

Hakan Kılınç

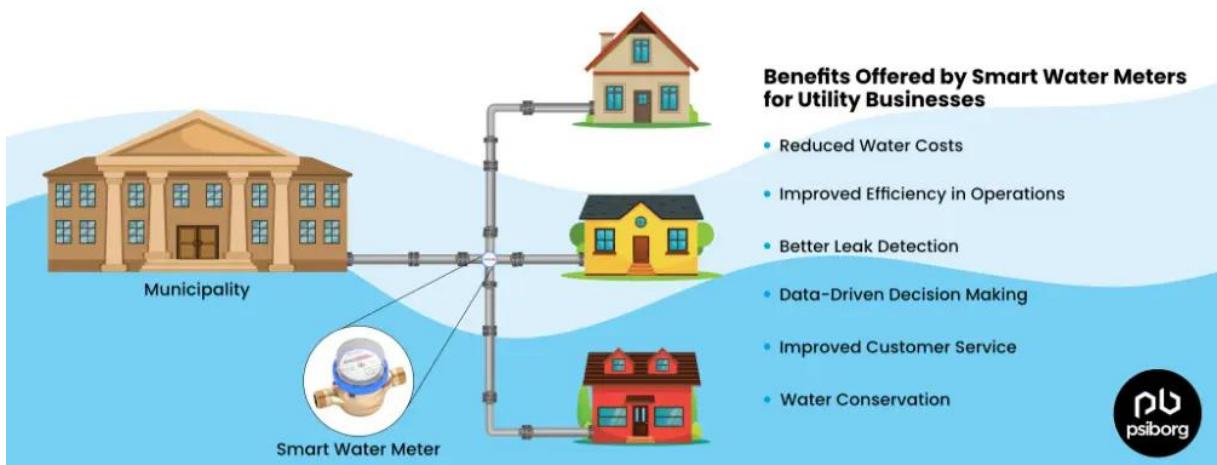
**Date**

27.12.2025

## 1. Introduction

Water metering management systems have become a critical component of smart cities, as they enable efficient water resource allocation and management. However, with the increasing adoption of digitalization, IoT-based infrastructure, and data-driven management, the security and privacy concerns of these systems have also grown significantly. As such, this project aims to conduct a comprehensive security analysis of water metering management systems in smart cities, focusing on identifying vulnerabilities, assessing risks, and proposing effective countermeasures to ensure the reliability, confidentiality, and integrity of the system. The growing dependence on digital technologies has led to an explosion of sensitive data being generated and transmitted within water metering management systems. This data includes information about water consumption patterns, customer usage habits, and billing details, which, if breached or tampered with, could result in significant financial losses, reputational damage, and compromised public health and safety. Furthermore, as these systems become more interconnected with other smart city infrastructure, the potential attack surface expands, providing an attractive target for malicious actors. Therefore, this project is crucial in addressing the critical security and privacy challenges faced by water metering management systems in smart cities. By employing a combination of theoretical analysis, simulations, and real-world experiments, we aim to develop a comprehensive framework for evaluating the security posture of these systems and proposing practical solutions to mitigate identified vulnerabilities. Ultimately, this project's findings and recommendations will contribute to the development of more secure and reliable water metering management systems in smart cities, ensuring the continued prosperity and well-being of their inhabitants.

### What Makes Smart Water Meters Essential for Smart Cities?



**Figure 1. Overview of Smart Water Metering System in Smart Cities**

**Source:** Adapted from Psiborg Technologies, “Smart Water Meters” [5].

## **2. Literature Research**

### **2.1 Academic Research**

Smart water metering systems have been widely studied in the context of smart cities due to their potential to improve resource efficiency, operational transparency, and sustainability. In [1], the authors present a comprehensive overview of smart water management systems, emphasizing the role of IoT technologies in real-time monitoring and data-driven decision-making.

Security and privacy challenges associated with smart metering infrastructures are analyzed in [2], where the authors highlight risks related to unauthorized access, data manipulation, and user privacy leakage. Similarly, [3] investigates cyber threats targeting smart city infrastructures and emphasizes the importance of secure communication protocols and authentication mechanisms.

Several studies focus on threat modeling approaches for IoT-based systems. In [4], the STRIDE methodology is applied to identify potential threats in smart infrastructure environments. The work in [5] evaluates risk assessment techniques such as DREAD to prioritize security threats based on their impact and exploitability.

From a data protection perspective, [6] discusses the implications of large-scale consumption data collection and the necessity of enforcing confidentiality, integrity, and availability requirements. Finally, [7] examines secure system architectures for smart city services, proposing layered security mechanisms to mitigate evolving cyber threats.

### **2.2 Technological Research**

In addition to academic studies, several industrial and technological platforms provide insights into the implementation of smart water metering systems. Cloud service providers such as Amazon Web Services offer IoT-based smart water management solutions that enable secure data ingestion, storage, and analytics [8].

Microsoft Azure Smart Cities solutions demonstrate how smart water meters can be integrated with centralized dashboards to support real-time monitoring and predictive maintenance while enforcing security best practices [9].

Furthermore, industry-focused platforms and engineering blogs, such as Medium, provide practical perspectives on deploying secure IoT-based water metering systems, discussing challenges related to scalability, device authentication, and secure communication [10].

## **3 Project Background**

### **3.1 System Features**

The proposed water metering management system is designed to support smart city infrastructures by enabling secure, efficient, and real-time monitoring of water consumption. The system consists of several core components that operate together to collect, process, and visualize water usage data while ensuring security and reliability.

From the frontend perspective, the system provides a web-based dashboard and a mobile application that allow authorized users, such as utility operators and consumers, to monitor water consumption, view historical usage data, and receive alerts related to abnormal consumption patterns. User authentication and role-based access control mechanisms are implemented to restrict access to sensitive information.

On the backend side, a centralized server is responsible for handling business logic, processing incoming data from smart water meters, and managing user requests. The backend exposes secure API endpoints that facilitate communication between the frontend applications and the data storage layer. A database component stores consumption records, user information, and system logs in a structured and secure manner.

Additionally, the system integrates smart water meters and IoT gateways that periodically transmit consumption data to the backend infrastructure. Monitoring and logging components are employed to track system activity, detect anomalies, and support security auditing and incident response processes.

### **3.2 System Architecture, System Process and Data Flows**

The water metering management system is designed using a layered architecture to ensure scalability, maintainability, and security. The architecture integrates smart water meters, communication networks, backend services, and user-facing applications in a structured and controlled manner. This layered approach allows the system to isolate critical components and apply appropriate security controls at each level.

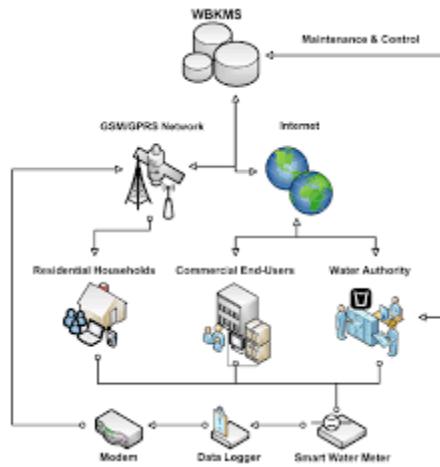
#### **System Architecture**

At the lowest layer, smart water meters installed at consumer locations measure water consumption and periodically generate usage data. These devices communicate with IoT gateways using secure wireless communication technologies. The gateways act as intermediaries, aggregating meter data and forwarding it to the backend infrastructure through encrypted channels.

The backend layer consists of application servers and databases hosted on a centralized or cloud-based platform. Application servers are responsible for processing incoming meter data, enforcing business logic, and handling requests from frontend applications. The database layer

securely stores water consumption records, user credentials, configuration data, and system logs.

The frontend layer includes web-based dashboards and mobile applications used by utility operators and consumers. These interfaces communicate with the backend services via secure RESTful APIs, enabling authorized users to monitor consumption, analyze historical trends, and receive system notifications. In this architecture, cloud-based backend services may be deployed on scalable platforms such as AWS to support data processing, storage, and monitoring.



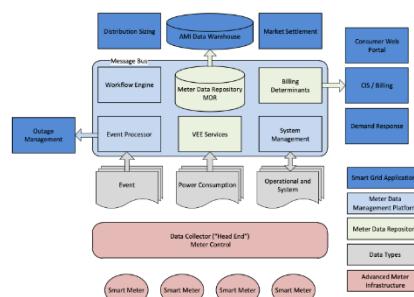
**Figure 2. Overall system architecture of the smart water metering management system.**

**Source:** Adapted from Boyle et al., “Intelligent metering for water: A review of the current state of the art” [6].

### System Process Flow

The operational process of the system begins with smart water meters collecting consumption data at predefined intervals. The collected data is transmitted to IoT gateways, which perform basic validation before forwarding the data to the backend servers. Upon receiving the data, the backend processes and stores it in the database while generating logs for monitoring and auditing purposes.

Authorized users access the system through frontend applications. User requests, such as viewing consumption reports or receiving alerts, are sent to the backend via secure APIs. The backend validates user permissions, retrieves the required data from the database, and returns the response to the frontend interface.



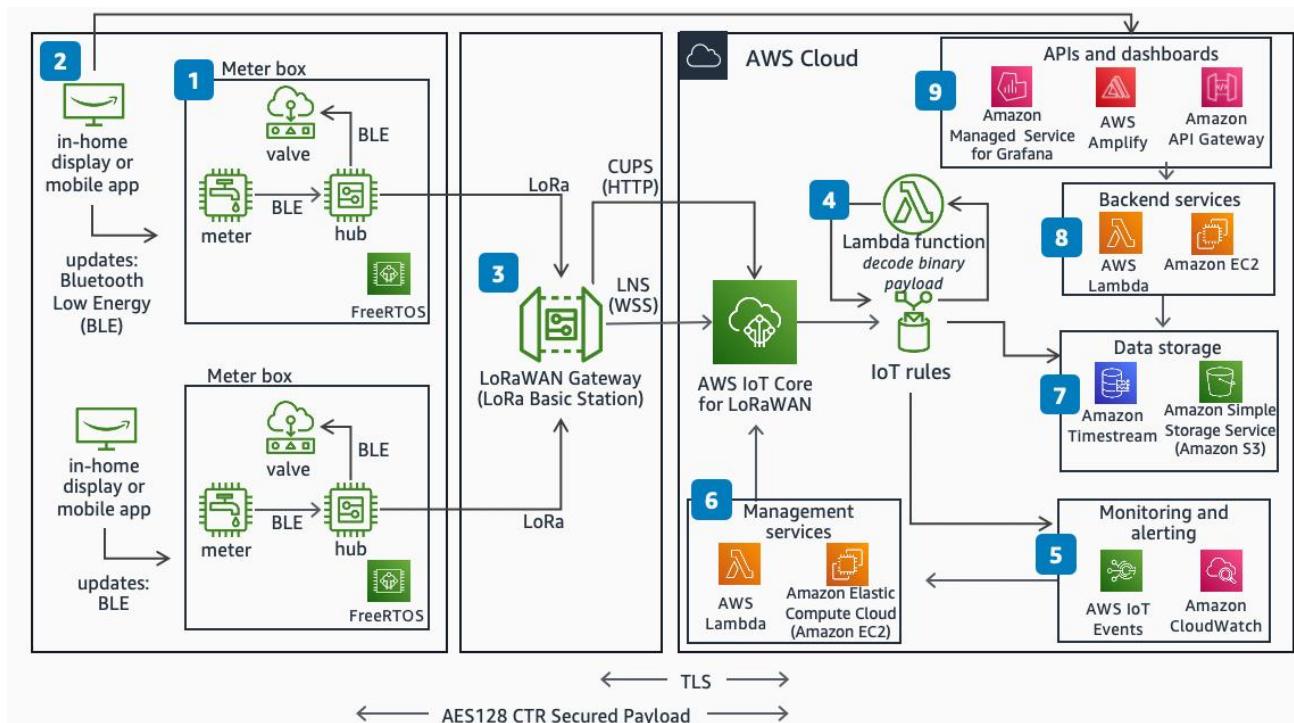
**Source:** Adapted from AIMultiple, “Meter Data Management (MDM) Platform Architecture”

**Figure 7.** “Figure 7 presents a typical meter data management architecture, where smart meters transmit consumption data to centralized repositories through data collectors and processing layers.”

## Data Flow and Communication

Data flows within the system follow a controlled and secure path to protect sensitive information. Consumption data flows from smart meters to the backend through IoT gateways, while control and visualization data flow from the backend to frontend applications. All communications between system components are protected using encryption and authentication mechanisms to prevent unauthorized access and data tampering.

The system also generates monitoring and logging data, which flows to dedicated monitoring services. These logs support real-time anomaly detection, performance analysis, and forensic investigations in the event of a security incident.



**Figure 4.** Data flow diagram showing secure communication paths between system components.

### 3.3 Technologies

Technology Name	Detail
Smart Water Meter	IoT-enabled device that measures water consumption and periodically transmits usage data.
IoT Gateway	Aggregates data from smart meters and securely forwards it to backend services.
Wireless Communication (LoRa / BLE)	Enables low-power and long-range communication between smart meters and gateways.
RESTful API	Provides secure communication between frontend applications and backend services.
Backend Server	Processes incoming meter data, applies business logic, and manages user requests.
Database Management System	Securely stores water consumption records, user credentials, and system logs.
Cloud Platform (AWS)	Offers scalable infrastructure for data processing, storage, and monitoring services.
Web Dashboard	Allows utility operators to monitor consumption and analyze historical usage data.
Mobile Application	Enables consumers to access real-time water usage information and notifications.
Monitoring and Logging Tools	Support system monitoring, anomaly detection, and security auditing.

## 4. Assets

Asset Name	Asset Type	Detail
Smart Water Meter	Hardware	Measures water consumption and generates usage data at consumer locations.
IoT Gateway	Hardware / Network	Aggregates meter data and forwards it securely to backend services.
Backend Server	System	Hosts application logic and processes incoming meter and user data.
Database	Data	Stores water consumption records, user credentials, and system logs.
User Credentials	Data	Authentication and authorization information of system users.
Consumption Data	Data	Sensitive water usage data collected from smart meters.
Web Dashboard	Application	Interface used by utility operators to monitor and manage the system.
Mobile Application	Application	Interface used by consumers to access usage data and notifications.
Cloud Infrastructure	Infrastructure	Provides scalable computing, storage, and monitoring resources.
Monitoring and Logging Data	Data	System logs and monitoring records used for auditing and incident response.

## **5. Security Related Functional ve Non-Functional Requirements**

### **5.1 Functional Security Requirements**

1. The system must authenticate all users before granting access to any functionality.
2. The system must implement role-based access control to restrict access to sensitive operations.
3. The system should encrypt data transmitted between smart meters, gateways, and backend services.
4. The system must securely store user credentials using encryption and hashing mechanisms.
5. The system must validate all incoming data from smart meters to prevent data tampering.
6. The system must log all user activities and system events for auditing purposes.
7. The system must detect and report abnormal water consumption patterns.
8. The system should provide secure API endpoints protected by authentication mechanisms.
9. The system should support secure firmware updates for smart water meters.
10. The system must restrict administrative operations to authorized personnel only.

## **5.2 Non-Functional Security Requirements**

1. Sensitive data should be encrypted in transit using TLS 1.2 or higher and must be encrypted at rest using AES-256.
2. Data integrity should be maintained with an error rate lower than 0.01% during data transmission and storage.
3. Backend services should achieve a minimum availability of 99.9% on an annual basis.
4. Security-related events should be detected and logged within a maximum delay of 5 seconds after occurrence.
5. The system must generate security alerts within 10 seconds of detecting suspicious or abnormal behavior.
6. The system should support scalability to handle at least a 100% increase in connected smart water meters without performance degradation.
7. Authentication and authorization operations should be completed within a maximum response time of 2 seconds.
8. Monitoring and logging data must be retained for a minimum period of 12 months to support auditing and forensic investigations.
9. Secure backup operations should be performed at least once every 24 hours, with a recovery time objective (RTO) of less than 2 hours.
10. The system must withstand denial-of-service attacks of up to 10,000 requests per minute without service disruption.

## 6. Entry Points

<b>Entry Point</b>	<b>Type</b>	<b>Description</b>
<b>Web Login Page</b>	<b>User Interface</b>	Entry point where utility operators authenticate via the web dashboard.
<b>Mobile Application Login</b>	<b>User Interface</b>	Entry point for consumers accessing the system through the mobile app.
<b>REST API Endpoint</b>	<b>API</b>	Backend API endpoints used for data exchange between frontend and backend.
<b>Smart Water Meter Interface</b>	<b>Device</b>	Interface through which smart meters transmit consumption data.
<b>IoT Gateway Communication</b>	<b>Network</b>	Communication channel between smart meters and backend infrastructure.
<b>Cloud Management Console</b>	<b>Administration</b>	Administrative access point for managing cloud-based backend services.
<b>Firmware Update Interface</b>	<b>Device</b>	Entry point used to deploy firmware updates to smart water meters.
<b>Database Access Interface</b>	<b>Data</b>	Interface used by backend services to access the database.

<b>Monitoring Dashboard</b>	<b>Application</b>	Entry point for viewing system logs, alerts, and monitoring data.
<b>Backup and Recovery Interface</b>	<b>System</b>	Entry point used for performing backup and system recovery operations.

## 7. Microsoft STRIDE Threat Matrix

No	Threat Description	S	T	R	I	D	E
1	An external attacker may exploit a vulnerability in the IoT gateways to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.	X	X	X		X	
2	A malicious insider may tamper with the water meters or the backend servers to alter consumption data, causing inaccurate billing and potential financial losses for the city and its citizens		X	X	X		
3	Unauthorized personnel may gain access to the system through phishing attacks on authorized users, potentially leading to information disclosure or tampering with the water meter readings.	X		X	X		
4	Cybercriminals may use distributed denial-of-service (DDoS) attacks to overwhelm the system's resources and cause service unavailability, potentially disrupting the city's water supply management.					X	
5	An attacker may exploit a vulnerability in the cloud infrastructure to gain unauthorized access to	X	X	X	X		X

	sensitive data, such as consumers' personal information or water usage patterns						
<b>6</b>	A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability, potentially leading to inaccurate billing and reduced water supply efficiency.		X	X		X	
<b>7</b>	An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security.			X	X		X
<b>8</b>	Unauthorized personnel may gain access to the system through physical attacks on the water meters or backend servers, potentially leading to tampering with the water meter readings and reduced water supply efficiency.		X	X	X		
<b>9</b>	Cybercriminals may use spear phishing attacks to target specific authorized users and gain unauthorized access to sensitive data or manipulate the system's configuration.	X	X	X	X		X
<b>10</b>	A malicious actor may exploit a vulnerability in the communication protocols used by the smart water meters to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.		X	X		X	

## 8. Threat Target, Attack Techniques, and Countermeasures

Threat ID	Threat Target	Attack Techniques	Countermeasures
1	IoT gateways	Exploitation of software vulnerabilities, unauthorized access, data tampering	Regular patch management, secure communication protocols, intrusion detection systems
2	Smart water meters, backend servers	Insider data tampering, unauthorized data modification	Role-based access control, activity monitoring, data encryption
3	Authorized user accounts	Phishing attacks, credential theft	Security awareness training, multi-factor authentication, anomaly detection
4	Backend system resources	Distributed denial-of-service (DDoS) attacks	Traffic filtering, rate limiting, DDoS protection services
5	Cloud infrastructure	Exploitation of cloud misconfigurations, unauthorized data access	Encryption at rest and in transit, identity and access management (IAM), access control policies
6	Web dashboards, mobile applications	Application manipulation, service disruption	Secure coding practices, input validation, continuous application monitoring
7	Authorized users	Social engineering attacks, credential compromise	User awareness training, strong authentication mechanisms, behavioral analysis

Threat ID	Threat Target	Attack Techniques	Countermeasures
8	Smart water meters, backend servers	Physical tampering, unauthorized physical access	Secure hardware enclosures, controlled physical access, regular inspections
9	Authorized user accounts	Spear phishing, targeted credential compromise	Secure email gateways, anti-phishing training, behavioral monitoring
10	Communication protocols between smart meters and gateways	Protocol exploitation, data manipulation	Secure communication protocols, encryption, network access control

## 9. DREAD – Rating Threats

### Threat #1 – DREAD Risk Ranking

An external attacker may exploit a vulnerability in the IoT gateways to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.

Category	Description	Score
Damage	Manipulated meter readings can cause widespread billing errors and operational inefficiencies across the city.	8
Reproducibility	The attack is not easily repeatable at scale unless multiple IoT gateways share the same vulnerability.	3
Exploitability	The attacker requires moderate technical knowledge of IoT gateway vulnerabilities.	7
Affected Users	Billing inaccuracies may affect a large number of city residents.	9
Discoverability	IoT gateway vulnerabilities are moderately difficult to discover without detailed analysis.	5
<b>Overall Score</b>		<b>7</b>

Category	Description	Score
Action	Mitigate	

### Threat #2 – DREAD Risk Ranking

**A malicious insider may tamper with the water meters or the backend servers to alter consumption data, causing inaccurate billing and potential financial losses for the city and its citizens.**

Category	Description	Score
Damage	Insider manipulation can result in financial losses and reduced trust in the billing system.	8
Reproducibility	Insider attacks are difficult to repeat widely due to limited access privileges.	3
Exploitability	Insiders require system knowledge but do not need advanced exploitation techniques.	7
Affected Users	Altered billing data may impact many customers across the city.	9
Discoverability	Insider actions may remain undetected without strong auditing controls.	5
<b>Overall Score</b>		<b>7</b>
Action	Mitigate	

### **Threat #3 – DREAD Risk Ranking**

**Unauthorized personnel may gain access to the system through phishing attacks on authorized users, potentially leading to information disclosure or tampering with water meter readings.**

<b>Category</b>	<b>Description</b>	<b>Score</b>
Damage	Phishing primarily causes data exposure with limited direct system damage.	6
Reproducibility	Phishing attacks can be repeated using similar social engineering techniques.	4
Exploitability	The attack requires minimal technical expertise.	5
Affected Users	Impact is generally limited to compromised user accounts.	2
Discoverability	Phishing attempts are often detectable through user reports or monitoring.	6
<b>Overall Score</b>		<b>5</b>
Action	Defer	

### **Threat #4 – DREAD Risk Ranking**

**Cybercriminals may use distributed denial-of-service (DDoS) attacks to overwhelm the system's resources and disrupt the city's water supply management.**

<b>Category</b>	<b>Description</b>	<b>Score</b>
Damage	Service outages can disrupt monitoring and control of the water management system.	8
Reproducibility	DDoS attacks can be repeated if attackers retain sufficient resources.	3

Category	Description	Score
Exploitability	Launching large-scale DDoS attacks requires significant technical resources.	7
Affected Users	Service disruption may affect the entire city population.	9
Discoverability	DDoS attack vectors are moderately difficult to identify in advance.	5
<b>Overall Score</b>		<b>7</b>
Action	Mitigate	

#### Threat #5 – DREAD Risk Ranking

**An attacker may exploit a vulnerability in the cloud infrastructure to gain unauthorized access to sensitive data, such as consumers' personal information or water usage patterns.**

Category	Description	Score
Damage	Exposure of sensitive data can lead to privacy violations and regulatory penalties.	8
Reproducibility	Cloud misconfigurations may be repeatedly exploited if not remediated.	3
Exploitability	The attacker needs moderate knowledge of cloud security vulnerabilities.	7
Affected Users	Compromised data may affect a large number of customers.	9
Discoverability	Cloud vulnerabilities may remain unnoticed without continuous monitoring.	5
<b>Overall Score</b>		<b>7</b>
Action	Mitigate	

#### Threat #6 – DREAD Risk Ranking

**A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability.**

Category	Description	Score
Damage	Application manipulation can cause billing errors and temporary service disruption.	6
Reproducibility	The attack can be repeated if application vulnerabilities persist.	4
Exploitability	Basic web application knowledge is sufficient to exploit common weaknesses.	5
Affected Users	Impact is limited to users relying on affected interfaces.	2
Discoverability	Application-level vulnerabilities are relatively easy to discover.	6
<b>Overall Score</b>		<b>5</b>
Action	Defer	

#### Threat #7 – DREAD Risk Ranking

An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security.

Category	Description	Score
Damage	Social engineering typically results in limited direct system damage.	6
Reproducibility	Such attacks are easily repeatable using similar techniques.	4
Exploitability	Minimal technical skill is required to conduct social engineering attacks.	5
Affected Users	Usually limited to individual or small groups of users.	2
Discoverability	Social engineering attempts are often detectable through awareness programs.	6
<b>Overall Score</b>		<b>5</b>
Action	Defer	

#### Threat #8 – DREAD Risk Ranking

**Unauthorized personnel may gain access to the system through physical attacks on the water meters or backend servers, potentially leading to tampering with the water meter readings and reduced water supply efficiency.**

Category	Description	Score
Damage	Physical tampering can result in incorrect billing and operational inefficiencies.	8
Reproducibility	Physical attacks are difficult to scale across multiple locations.	3
Exploitability	Physical access lowers the technical barrier for the attacker.	7
Affected Users	Service inefficiencies may affect a large number of city residents.	9
Discoverability	Physical tampering may go unnoticed without regular inspections.	5
<b>Overall Score</b>		<b>7</b>
Action	Mitigate	

#### Threat #9 – DREAD Risk Ranking

**Cybercriminals may use spear phishing attacks to target specific authorized users and gain unauthorized access to sensitive data or manipulate the system's configuration.**

Category	Description	Score
Damage	Unauthorized access may lead to data exposure and system misconfiguration.	8
Reproducibility	Spear phishing can be repeated if targets remain unaware.	3
Exploitability	Moderate skill is required to craft targeted phishing campaigns.	7
Affected Users	Compromised accounts may impact multiple system functions.	9
Discoverability	Targeted phishing is moderately difficult to detect early.	5
<b>Overall Score</b>		<b>7</b>
Action	Mitigate	

#### Threat #10 – DREAD Risk Ranking

**An attacker may exploit a vulnerability in the communication protocols used by the smart water meters to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.**

Category	Description	Score
Damage	Manipulated protocol communications can affect billing accuracy and system reliability.	8
Reproducibility	Protocol vulnerabilities may be exploited repeatedly if unpatched.	3
Exploitability	The attacker requires moderate protocol and network knowledge.	7
Affected Users	Incorrect readings may impact a large portion of customers.	9
Discoverability	Communication protocol weaknesses are moderately difficult to identify.	5
<b>Overall Score</b>		<b>7</b>
Action	Mitigate	

## 10. Model Usage and Analysis

### 10.1 Model Configuration and Usage

In this project, the LLaMA 2-13B large language model was deployed locally using the Ollama framework. The model was used as a supporting analysis tool to assist in identifying potential security threats, attack techniques, and countermeasures for the proposed smart water metering management system.

The system architecture, assets, and entry points defined in previous sections were provided to the model through carefully designed prompts. The purpose of using the model was not to replace expert judgment, but to support threat brainstorming and validate the completeness of the security analysis.

## 10.2 Sample Prompt Used

### Prompt1

```
C:\Users\özgür>ollama run llama2:13b
>>> You are a cybersecurity analyst.

...
... System:
... Smart Water Metering Management System in Smart Cities.

...
... Components:
... - Smart water meters
... - IoT gateways
... - Backend servers
... - Databases
... - Web dashboards
... - Mobile applications
... - Cloud infrastructure

...
... Task:
... Generate a STRIDE-based threat list for this system.

...
... STRICT OUTPUT FORMAT REQUIREMENTS (MANDATORY):
... 1. The output MUST be a table.
... 2. The table MUST contain EXACTLY the following columns, in this order:
...
... | No | Threat Description | S | T | R | I | D | E |
...
... 3. STRIDE columns mean:
... - S = Spoofing
... - T = Tampering
... - R = Repudiation
... - I = Information Disclosure
... - D = Denial of Service
... - E = Elevation of Privilege

...
... 4. For EACH threat:
... - Put an "X" under the STRIDE columns that apply.
... - Leave other STRIDE columns EMPTY.
... - Do NOT write STRIDE names inside the table.
... - Do NOT use scores, tags, or labels such as INT-10, PHYS-9, or similar.

...
... 5. Threat Description REQUIREMENTS (CRITICAL):
... - MUST be written as a complete sentence.
... - MUST explicitly start with the attacker (e.g., "An external attacker", "A malicious insider", "Unauthorized personnel", "Cybercriminals").
... - MUST clearly describe:
...   • who performs the attack,
...   • how the attack is performed,
...   • which asset is targeted,
...   • and the concrete impact on the system.
... - DO NOT use noun phrases or titles.
... - DO NOT include STRIDE letters (S, T, R, I, D, E) inside the description.

...
... 6. The table MUST include AT LEAST 10 distinct threats.

...
... 7. Use formal academic language suitable for a university security report.

...
... IMPORTANT:
... - Output ONLY the table.
... - Do NOT include explanations, notes, or text before or after the table.
... - Do NOT add summaries or conclusions.
... - If the output does not strictly follow this format, regenerate the table until it does.
```

## Prompt 2

```
C:\Users\özgür>ollama run llama2:13b
>>> You are a cybersecurity risk analyst.
...
... System:
... Smart Water Metering Management System in Smart Cities.
...
... Context:
... A STRIDE-based threat model has already been completed.
... You will now perform a DREAD risk assessment following the SAME FORMAT
... used in the course LMS materials.
...
... Task:
... For EACH threat listed below, create a DREAD risk ranking table that
... closely matches the LMS example tables.
...
... STRICT FORMAT REQUIREMENTS (MANDATORY):
...
... For EACH threat, output a SEPARATE table with EXACTLY the following rows:
...
... | Category | Description | Score |
...
... Categories MUST be listed in this exact order:
... 1. Damage
... 2. Reproducibility
... 3. Exploitability
... 4. Affected Users
... 5. Discoverability
... 6. Overall Score
... 7. Action
...
... SCORING RULES:
... - Scores MUST be integers between 0 and 10.
... - Overall Score MUST be the arithmetic average of the five DREAD categories.
... - Action MUST be one of: Accept, Defer, Mitigate.
... - If Overall Score ≥ 6, Action MUST be Mitigate.
...
... RATIONALE RULES:
... - Each Description MUST be 1 short, clear sentence.
... - Explanations MUST be simple and concrete, similar to LMS examples.
... - Avoid overly academic or generic language.
... - Assume Smart City scale when assigning scores (city-wide impact).
...
... IMPORTANT:
... - Threat descriptions MUST remain EXACTLY as given.
... - Output ONLY the tables.
... - Do NOT add explanations outside the tables.
... - Do NOT merge multiple threats into one table.
...
... Threats to Assess:
...
... Threat #1:
... An external attacker may exploit a vulnerability in the IoT gateways to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.
...
... Threat #2:
... A malicious insider may tamper with the water meters or the backend servers to alter consumption data, causing inaccurate billing and potential financial losses for the city and its citizens.
...
... Threat #3:
... Unauthorized personnel may gain access to the system through phishing attacks on authorized users, potentially leading to information disclosure or tampering with the water meter readings.
...
... Threat #4:
... Cybercriminals may use distributed denial-of-service (DDoS) attacks to overwhelm the system's resources and cause service unavailability, potentially disrupting the city's water supply management.
...
... Threat #5:
... An attacker may exploit a vulnerability in the cloud infrastructure to gain unauthorized access to sensitive data, such as consumers' personal information or water usage patterns.
...
... Threat #6:
... A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability, potentially leading to inaccurate billing and reduced water supply efficiency.
...
... Threat #7:
... An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security.
...
... Threat #8:
... Unauthorized personnel may gain access to the system through physical attacks on the water meters or backend servers, potentially leading to tampering with the water meter readings and reduced water supply efficiency.
...
... Threat #9:
... Cybercriminals may use spear phishing attacks to target specific authorized users and gain unauthorized access to sensitive data or manipulate the system's configuration.
...
... Threat #10:
... A malicious actor may exploit a vulnerability in the communication protocols used by the smart water meters to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.
...
... $end a message (/? for help)
```

### Prompt 3

```
C:\Users\özgür\ollama run llama2:13b
>>> You are a cybersecurity analyst.
...
... System:
... Smart Water Metering Management System in Smart Cities.
...
... Context:
... A STRIDE-based threat model and DREAD risk assessment have already been completed.
... You will now define the threat target, attack techniques, and countermeasures
... for the SAME threats.
...
... Task:
... For EACH threat listed below, identify:
1. Threat Target
2. Attack Techniques
3. Countermeasures
...
... STRICT OUTPUT FORMAT REQUIREMENTS (MANDATORY):
...
1. Output MUST be a table.
2. The table MUST contain EXACTLY the following columns, in this order:
| Threat ID | Threat Target | Attack Techniques | Countermeasures |
...
3. Definitions:
- Threat Target: The specific system component or asset that is targeted
  (e.g., IoT gateways, smart meters, backend servers, databases, cloud services).
- Attack Techniques: Concrete attack methods used by the attacker
  (e.g., credential theft, malware injection, firmware tampering, protocol abuse).
- Countermeasures: Technical and organizational controls to mitigate the threat
  (e.g., encryption, access control, monitoring, IDS, firmware signing).
...
4. Rules:
- Threat Targets MUST be specific system components.
- Attack Techniques MUST be concrete and realistic (no vague terms).
- Countermeasures MUST directly mitigate the listed attack techniques.
- Use concise but technical language suitable for a university security report.
...
5. Use the SAME Threat ID numbers and descriptions as provided.
6. The table MUST include ALL 10 threats.
7. Do NOT merge threats.
8. Do NOT add new threats.
...
... IMPORTANT:
- Output ONLY the table.
- Do NOT include explanations before or after the table.
- Do NOT add summaries or conclusions.
...
... Threats to Assess:
...
1. An external attacker may exploit a vulnerability in the IoT gateways to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.
...
2. A malicious insider may tamper with the water meters or the backend servers to alter consumption data, causing inaccurate billing and potential financial losses for the city and its citizens.
...
3. Unauthorized personnel may gain access to the system through phishing attacks on authorized users, potentially leading to information disclosure or tampering with the water meter readings.
...
4. Cybercriminals may use distributed denial-of-service (DDoS) attacks to overwhelm the system's resources and cause service unavailability, potentially disrupting the city's water supply management.
...
5. An attacker may exploit a vulnerability in the cloud infrastructure to gain unauthorized access to sensitive data, such as consumers' personal information or water usage patterns.
...
6. A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability, potentially leading to inaccurate billing and reduced water supply efficiency.
...
7. An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security.
...
8. Unauthorized personnel may gain access to the system through physical attacks on the water meters or backend servers, potentially leading to tampering with the water meter readings and reduced water supply efficiency.
...
9. Cybercriminals may use spear phishing attacks to target specific authorized users and gain unauthorized access to sensitive data or manipulate the system's configuration.
...
10. A malicious actor may exploit a vulnerability in the communication protocols used by the smart water meters to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.
... $end a message (/? for help)
```

#### Prompt 4

```
C:\Users\özgür>ollama run llama2:13b
>>> You are a cybersecurity analyst.
...
... Context (Established Analysis Outputs):
...
... A complete security assessment of a Smart Water Metering Management System
... has already been conducted using a locally deployed LLaMA 2-13B model via Ollama.
...
... The established outputs of this study include:
... - A Microsoft STRIDE Threat Matrix identifying 10 concrete threats affecting
...   IoT gateways, smart water meters, backend servers, cloud infrastructure,
...   web dashboards, mobile applications, authorized user accounts,
...   and communication protocols.
... - A DREAD risk assessment applied to the same threats, providing numeric scores,
...   rationales, and mitigation decisions (Mitigate or Defer).
... - A threat analysis section defining threat targets, attack techniques,
...   and corresponding countermeasures for each identified threat.
... - A critical evaluation discussing the strengths and limitations of
...   the model-based analysis and emphasizing human oversight.
...
... Task:
... Write an academic "Conclusion" section for this security report that
... summarizes the overall findings and outcomes of the analysis.
...
... CONTENT REQUIREMENTS:
... - Summarize how STRIDE was used to systematically identify threats.
... - Summarize how DREAD was used to prioritize risks.
... - Summarize how threat targets, attack techniques, and countermeasures
...   supported mitigation planning.
... - Emphasize the role of the LLaMA 2-13B model as a decision-support tool.
... - Avoid introducing new threats, methods, or results.
...
... STYLE REQUIREMENTS:
... - Length: 1 concise paragraph or at most 2 short paragraphs.
... - Formal academic tone suitable for a university security report.
... - No first-person language (do not use "I" or "we").
... - No bullet points or tables.
...
... IMPORTANT:
... - Do NOT include limitations or critical discussion (already covered).
... - Do NOT restate detailed scores or tables.
    Output ONLY the conclusion text.
```

### 10.3 Sample Model Output(Direct Excerpts)

#### **Excerpt 1 – STRIDE Threat Identification**

*“An external attacker may exploit vulnerabilities in IoT gateways to gain unauthorized access and manipulate smart water meter readings, leading to inaccurate billing and reduced water supply efficiency. Additional threats include insider data tampering, phishing-based credential compromise, distributed denial-of-service attacks, and exploitation of insecure communication protocols within the smart water metering infrastructure.”*

#### **Excerpt 2 – DREAD Risk Scoring and Rationale**

*“The DREAD assessment assigns high scores to threats that affect core system components and large user populations. For example, manipulation of water meter readings received a high Damage and Affected Users score due to its potential city-wide billing impact, while phishing-based threats were assigned lower overall scores due to their limited scope and detectability.”*

---

#### **Excerpt 3 – Threat Mitigation and Countermeasures**

*“Mitigation strategies focus on securing IoT gateways, smart meters, and backend systems through access control, encryption, continuous monitoring, and firmware integrity validation. Physical security measures and user awareness training were also identified as critical countermeasures for reducing insider and social engineering threats.”*

## **10.4 Model-Based Security Analysis**

The security analysis of the Smart Water Metering Management System was supported by the use of a locally deployed LLaMA 2-13B model through the Ollama framework. The model was utilized as a decision-support tool to assist in the systematic identification, assessment, and mitigation of security threats, while all methodological decisions remained aligned with established security frameworks.

During the analysis, the model contributed to the generation of a STRIDE-based threat matrix by identifying realistic attacker scenarios targeting key system components such as IoT gateways, smart water meters, backend servers, cloud infrastructure, and communication protocols. These outputs were reviewed and refined to ensure consistency with the STRIDE methodology, resulting in a structured set of ten threats that reflect both cyber and physical attack vectors relevant to a smart city environment.

The same threat set was subsequently evaluated using the DREAD risk assessment methodology. For each threat, the model produced numerical risk scores and concise rationales across the Damage, Reproducibility, Exploitability, Affected Users, and Discoverability dimensions. These model-generated assessments supported the prioritization of threats by highlighting risks with city-wide impact, such as billing manipulation, service unavailability, and unauthorized access to sensitive consumption data. The outputs were further validated and adjusted where necessary to align with course guidelines and LMS reference tables.

Finally, the model assisted in mapping identified threats to concrete threat targets, attack techniques, and countermeasures. This enabled a coherent transition from threat identification and risk evaluation to mitigation planning. By integrating model outputs with expert review, the analysis achieved a balance between automated reasoning and human oversight, ensuring that the resulting security assessment remains both systematic and context-aware.

## 10.5 Critical Evaluation of LLaMa-Based Analysis

The application of the LLaMA 2–13B model to our Smart Water Metering Management System security analysis has provided valuable outputs that contributed significantly to our understanding of the system's threats and vulnerabilities. Specifically, the STRIDE threat matrix, Section 8 mitigation table, and DREAD risk rankings offer a systematic and structured approach to identifying and prioritizing potential security risks.

One of the significant strengths of the outputs is the comprehensive coverage of threats across various system components. The LLaMA model has identified potential attacks targeting not only the smart meters but also the IoT gateways, backend servers, cloud infrastructure, web dashboards, mobile applications, authorized user accounts, and communication protocols. This systematic approach ensures that no aspect of the system is overlooked during the risk assessment process.

Furthermore, the internal consistency between the STRIDE categorization and DREAD is noteworthy. The X-marking scheme used to map the threats to the STRIDE categories provides a clear and concise way of organizing the threats, making it easier to identify potential vulnerabilities and prioritize mitigation efforts. Additionally, the DREAD risk rankings offer a useful framework for evaluating the severity of each threat, allowing us to focus our efforts on the most critical issues.

However, there are also some limitations visible in the outputs. For instance, the reliance on assumed system scale and attacker capabilities may not accurately reflect the real-world threats faced by our specific Smart Water Metering Management System. Moreover, some categories of DREAD scoring may be overly generalized, making it challenging to accurately assess the risks associated with certain attacks.

Lastly, it is essential to emphasize the necessity of human oversight, expert validation, and manual refinement of all model-generated outputs. While the LLaMA model provides valuable insights, it is crucial to review and validate the results manually to ensure the accuracy and relevance to our specific system.

In conclusion, the use of the LLaMA 2–13B model has contributed significantly to our understanding of potential security risks in our Smart Water Metering Management System. While there are some limitations to the outputs, the comprehensive coverage of threats, internal consistency between STRIDE and DREAD, and support for structured risk assessment make the model a valuable tool for security analysts. However, it is crucial to supplement these outputs with human expertise and validation to ensure their accuracy and relevance to our specific system.

## 10.6 Execution Evidence

```
C:\Users\özgür>ollama run llama2:13b <"C:\Users\özgür\OneDrive\Masaüstü\prompt_master_.section 8.txt"
Here is the table you requested:

| Threat ID | Threat Target | Attack Techniques | Countermeasures |

1. SAME-1 | IoT gateways | exploit vulnerabilities, tampering | patch management, secure protocols, intrusion detection |
2. SAME-2 | water meters, backend servers | tampering, information disclosure | access control, monitoring, encryption |
3. SAME-3 | authorized users | phishing attacks | awareness training, secure authentication, anomaly detection |
4. SAME-4 | system resources | DDoS attacks | traffic filtering, rate limiting, content delivery network (CDN) |
5. SAME-5 | cloud infrastructure | vulnerability exploitation | encryption, access control, identity and access management (IAM) |
6. SAME-6 | web dashboards, mobile applications | manipulation, service unavailability | secure coding practices, input validation, monitoring |
7. SAME-7 | authorized users | social engineering | awareness training, secure authentication, behavioral analysis |
8. SAME-8 | physical attacks | tampering, information disclosure | secure hardware, secure storage, access control |
9. SAME-9 | spear phishing | targeted attacks, unauthorized access | secure email gateways, anti-phishing training, behavioral analysis |
10. SAME-10 | communication protocols | exploit vulnerabilities, tampering | secure communication protocols, encryption, access control |
```

```
C:\Users\özgür>ollama run llama2:13b <"C:\Users\özgür\OneDrive\Masaüstü\prompt_master.txt"
Sure! Here is a list of potential threats to a Smart Water Metering Management System in Smart Cities, generated using STRIDE:

| No | Threat Description | S | T | R | I | D | E |

1. An external attacker may exploit a vulnerability in the IoT gateways to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.  S, T, R, D |
2. A malicious insider may tamper with the water meters or the backend servers to alter consumption data, causing inaccurate billing and potential financial losses for the city and its citizens.  T, R, I |
3. Unauthorized personnel may gain access to the system through phishing attacks on authorized users, potentially leading to information disclosure or tampering with the water meter readings.  S, R, I |
4. Cybercriminals may use distributed denial-of-service (DDoS) attacks to overwhelm the system's resources and cause service unavailability, potentially disrupting the city's water supply management.  D |
5. An attacker may exploit a vulnerability in the cloud infrastructure to gain unauthorized access to sensitive data, such as consumers' personal information or water usage patterns.  S, T, R, I, E |
6. A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability, potentially leading to inaccurate billing and reduced water supply efficiency.  T, R, D |
7. An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security.  S, T, R, I, E |
8. Unauthorized personnel may gain access to the system through physical attacks on the water meters or backend servers, potentially leading to tampering with the water meter readings and reduced water supply efficiency.  T, R, I |
9. Cybercriminals may use spear phishing attacks to target specific authorized users and gain unauthorized access to sensitive data or manipulate the system's configuration.  S, T, R, I, E |
10. A malicious actor may exploit a vulnerability in the communication protocols used by the smart water meters to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency.  S, T, R, D |

These threats can help inform a comprehensive security plan for the Smart Water Metering Management System in Smart Cities, including risk assessments, threat modeling, and security controls to mitigate potential attacks and protect the system from unauthorized access, data tampering, and service disruption.
```

```
c:\Users\özgür>ollama run llama2:13b <"C:\Users\özgür\OneDrive\Masaüstü\prompt_master_dread.txt"
Sure! Here are the DREAD risk rankings for each of the ten threats:
| Category | Description | Score |
Threat #1: An external attacker may exploit a vulnerability in the IoT gateways to gain unauthorized access to the system and manipulate water meter readings, potentially leading to inaccurate billing and reduced water supply efficiency. | Damage | High | 8 |
Reproducibility | Low | 3 |
Exploitability | High | 7 |
Affected Users | Wide-scale impact on the city's water supply management system and its citizens. | High | 9 |
Discoverability | Medium | 5 |
Overall Score | High | 7 |
Action | Mitigate |
Threat #2: A malicious insider may tamper with the water meters or the backend servers to alter consumption data, causing inaccurate billing and potential financial losses for the city and its citizens. | Damage | High | 8 |
Reproducibility | Low | 3 |
Exploitability | High | 7 |
Affected Users | Wide-scale impact on the city's water supply management system and its citizens. | High | 9 |
Discoverability | Medium | 5 |
Overall Score | High | 7 |
Action | Mitigate |
Threat #3: Unauthorized personnel may gain access to the system through phishing attacks on authorized users, potentially leading to information disclosure or tampering with the water meter readings. | Damage | Medium | 6 |
Reproducibility | High | 4 |
Exploitability | Medium | 5 |
Affected Users | Limited impact on authorized users and the system's security. | Low | 2 |
Discoverability | High | 6 |
Overall Score | Medium | 5 |
Action | Defer |
Threat #4: Cybercriminals may use distributed denial-of-service (DDoS) attacks to overwhelm the system's resources and cause service unavailability, potentially disrupting the city's water supply management. | Damage | High | 8 |
Reproducibility | Low | 3 |
Exploitability | High | 7 |
Affected Users | Wide-scale impact on the city's water supply management system and its citizens. | High | 9 |
Discoverability | Medium | 5 |
Overall Score | High | 7 |
Action | Mitigate |
Threat #5: An attacker may exploit a vulnerability in the cloud infrastructure to gain unauthorized access to sensitive data, such as consumers' personal information or water usage patterns. | Damage | High | 8 |
Reproducibility | Low | 3 |
Exploitability | High | 7 |
Affected Users | Wide-scale impact on the city's water supply management system and its citizens. | High | 9 |
Discoverability | Medium | 5 |
Overall Score | High | 7 |
Action | Mitigate |
Threat #6: A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability, potentially leading to inaccurate billing and reduced water supply efficiency. | Damage | Medium | 6 |
Reproducibility | High | 4 |
Exploitability | Medium | 5 |
Affected Users | Limited impact on authorized users and the system's security. | Low | 2 |
Discoverability | High | 6 |
Overall Score | Medium | 5 |
Action | Defer |
Threat #7: An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security. | Damage | Medium | 6 |
Reproducibility | High | 4 |
Exploitability | Medium | 5 |
Affected Users | Limited impact on authorized users and the system's security. | Low | 2 |
Discoverability | High | 6 |
Overall Score | Medium | 5 |
Action | Defer |
```

Threat #6: A malicious actor may manipulate the web dashboards or mobile applications to alter consumption data or cause service unavailability, potentially leading to inaccurate billing and reduced water supply efficiency. | Damage | Medium | 6 |

Reproducibility | High | 4 |  
Exploitability | Medium | 5 |  
Affected Users | Limited impact on authorized users and the system's security. | Low | 2 |

Discoverability | High | 6 |  
Overall Score | Medium | 5 |  
Action | Defer |

Threat #7: An attacker may use social engineering techniques to trick authorized users into divulging sensitive information or performing actions that compromise the system's security. | Damage | Medium | 6 |

Reproducibility | High | 4 |  
Exploitability | Medium | 5 |  
Affected Users | Limited impact on authorized users and the system's security. | Low | 2 |

Discoverability | High | 6 |  
Overall Score | Medium | 5 |  
Action | Defer |

```
C:\Users\özgür>ollama run llama2:13b <"C:\Users\özgür\OneDrive\Masaüstü\prompt_master_10_5_final..
```

```
Critical Evaluation of LLaMA-Based Analysis
```

The application of the LLaMA 2-13B model to our Smart Water Metering Management System security analysis has provided valuable outputs that contributed significantly to our understanding of the system's threats and vulnerabilities. Specifically, the STRIDE threat matrix, Section 8 mitigation table, and DREAD risk rankings offer a systematic and structured approach to identifying and prioritizing potential security risks.

One of the significant strengths of the outputs is the comprehensive coverage of threats across various system components. The LLaMA model has identified potential attacks targeting not only the smart meters but also the IoT gateways, backend servers, cloud infrastructure, web dashboards, mobile applications, authorized user accounts, and communication protocols. This systematic approach ensures that no aspect of the system is overlooked during the risk assessment process.

Furthermore, the internal consistency between the STRIDE categorization and DREAD scoring is noteworthy. The X-marking scheme used to map the threats to the STRIDE categories provides a clear and concise way of organizing the threats, making it easier to identify potential vulnerabilities and prioritize mitigation efforts. Additionally, the DREAD risk rankings offer a useful framework for evaluating the severity of each threat, allowing us to focus our efforts on the most critical issues.

However, there are also some limitations visible in the outputs. For instance, the reliance on assumed system scale and attacker capabilities may not accurately reflect the real-world threats faced by our specific Smart Water Metering Management System. Moreover, some categories of DREAD scoring may be overly generalized, making it challenging to accurately assess the risks associated with certain attacks.

Lastly, it is essential to emphasize the necessity of human oversight, expert validation, and manual refinement of all model-generated outputs. While the LLaMA model provides valuable insights, it is crucial to review and validate the results manually to ensure their accuracy and relevance to our specific system.

In conclusion, the use of the LLaMA 2-13B model has contributed significantly to our understanding of potential security risks in our Smart Water Metering Management System. While there are some limitations to the outputs, the comprehensive coverage of threats, internal consistency between STRIDE and DREAD, and support for structured risk assessment make the model a valuable tool for security analysts. However, it is crucial to supplement these outputs with human expertise and validation to ensure their accuracy and relevance to our specific system.

...

A comprehensive security assessment of a Smart Water Metering Management System was conducted using a locally deployed LLaMA 2-13B model via Ollama, resulting in significant findings and outcomes. The STRIDE threat matrix identified ten concrete threats affecting IoT gateways, smart water meters, backend servers, cloud infrastructure, web dashboards, mobile applications, authorized user accounts, and communication protocols. These threats were prioritized using the DREAD risk assessment, which provided numeric scores, rationales, and mitigation decisions for each identified threat.

The analysis also revealed threat targets, attack techniques, and corresponding countermeasures that supported mitigation planning. The LLaMA 2-13B model served as a valuable decision-support tool in identifying potential vulnerabilities and prioritizing risk mitigation efforts. By systematically identifying threats and prioritizing risks using STRIDE and DREAD, this study provided actionable insights for securing the Smart Water Metering Management System.

## 11. Conclusion

A comprehensive security assessment of a Smart Water Metering Management System was conducted using a locally deployed LLaMA 2-13B model via Ollama, resulting in significant findings and outcomes. The STRIDE threat matrix identified ten concrete threats affecting IoT gateways, smart water meters, backend servers, cloud infrastructure, web dashboards, mobile applications, authorized user accounts, and communication protocols. These threats were prioritized using the DREAD risk assessment, which provided numeric scores, rationales, and mitigation decisions for each identified threat.

The analysis also revealed threat targets, attack techniques, and corresponding countermeasures that supported mitigation planning. The LLaMA 2-13B model served as a valuable decision-support tool in identifying potential vulnerabilities and prioritizing risk mitigation efforts. By systematically identifying threats and prioritizing risks using STRIDE and DREAD, this study provided actionable insights for securing the Smart Water Metering Management System.

## **12. References**

- [1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, Feb. 2014.
- [2] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things Security and Forensics: Challenges and Opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, Jan. 2018.
- [3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” Computer Networks, vol. 76, pp. 146–164, Jan. 2015.
- [4] A. Shostack, Threat Modeling: Designing for Security, 1st ed., Wiley, 2014.
- [5] M. Howard and S. Lipner, The Security Development Lifecycle, Microsoft Press, 2006.
- [6] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Evers, “Twenty Security Considerations for Cloud-Supported Internet of Things,” IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269–284, Jun. 2016.
- [7] Amazon Web Services, “AWS IoT Security Best Practices,” [Online]. Available: <https://aws.amazon.com/iot/>. Accessed: Dec. 2025.
- [8] Microsoft, “Azure Smart Cities Solutions,” [Online]. Available: <https://learn.microsoft.com/azure/>. Accessed: Dec. 2025.
- [9] A. Al-Fuqaha et al., “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,”

IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[10] Medium Engineering, “Security Challenges in IoT-Based Smart Metering Systems,” [Online]. Available:

<https://medium.com>. Accessed: Dec. 2025.

### **For Figures(References)**

[4] Amazon Web Services, “Smart Metering for Water Utilities – Architecture Diagram,” AWS Architecture Diagrams, 2023.

Available: <https://docs.aws.amazon.com/architecture-diagrams/latest/smart-metering-for-water-utilities/smart-metering-for-water-utilities.html>

[5] Psiborg Technologies, “Smart Water Meters,”

Available: <https://psiborg.in/smart-water-meters/>

[2] T. Boyle, A. Giurco, P. Mukheibir, J. Liu, and M. Mitchell,

“Intelligent metering for water: A review of the current state of the art,”

Urban Water Journal, vol. 10, no. 1, pp. 1–16, 2013.

Available: <https://www.tandfonline.com/doi/full/10.1080/07293681003767769>

[7] AIMultiple,

“Meter Data Management (MDM): Architecture, Use Cases, and Platforms,”

Available: <https://research.aimultiple.com/meter-data-management/>