

American International University-Bangladesh (AIUB)  
**Department of Computer Science  
Faculty of Science &Technology (FST)  
Fall 24 25**

**Industrial Oil Theft Detection System**

Software Requirement Engineering

Sec: **A**

Project submitted

By

Quazi Reshoan Yazdi 21-45485-3

Niloy Gabriel Gomes 22-47283-1

Md. Sazzad Hossain 22-47354-2

Fahmida Yasmin 22-48119-2

**Checked By Industry Personnel**

Name:

Designation:

Company:

Sign:

Date:

**Table of Contents**

|  |  |
| --- | --- |
| 1. **Problem Domain** | **4** |
| * 1. Background to the Problem | 4 |
| * 1. Solution to the Problem | 4 |
| * + 1. Related Works | 4 |
| * + - 1. IoT-Based Oil Theft Prevention | 4 |
| * + - 1. Oil Theft and Economic Impact in Nigeria | 4 |
| * + - 1. Global Oil Theft and Policy Solutions | 5 |
| * + - 1. Comparative Insights | 5 |
| * + - 1. Conclusion | 5 |
| * + 1. Solution 1 | 5 |
| * + 1. Solution 2 | 6 |
| * + 1. Justification for Preferring the First Solution | 7 |
| 1. **Solution Description** | **7** |
| * 1. System Features | 7 |
| * 1. UML Diagrams | 11 |
| * + 1. Activity Diagram | 11 |
| * + 1. Class Diagram | 12 |
| * + 1. Entity-Relationship Diagram | 13 |
| 1. **Social Impact** | **13** |
| 1. **Development Plan with Project Schedule** | **14** |
| * 1. Development Plan | 14 |
| * + 1. List 1 – Project Planning | 15 |
| * + 1. List 2 – System Design & Documentation | 15 |
| * + 1. List 3 – Hardware & Software Development | 16 |
| * + 1. List 4 – Testing & Integration | 16 |
| * + 1. List 5 – Deployment & Maintenance | 16 |
| * 1. Project Schedule | 17 |
| * + 1. Gantt Chart | 17 |
| * + 1. Project Schedule | 17 |
| 1. **Marketing Plan** | **18** |
| * 1. Short Term Marketing Plan (0 - 6 Months) | 18 |
| * 1. Long Term Marketing Plan (6 Months – 2 Years) | 18 |
| * 1. Continuous Marketing Plan (Ongoing Strategies) | 19 |
| 1. **Cost and Profit Analysis** | **19** |
| * 1. Cost Analysis | 19 |
| * + 1. Development Costs (One-Time Investment) | 19 |
| * + 1. Marketing Costs (Initial + Ongoing) | 20 |
| * + 1. Operational Costs (Annual) | 20 |
| * 1. Profit Analysis | 20 |
| * + 1. Revenue Model | 20 |
| * + 1. Profit Calculation (Year 1) | 21 |
| * 1. Total Costs | 21 |
| 1. **References** | **22** |

1. **PROBLEM DOMAIN** 
   1. **Background to the Problem**

In Bangladesh, oil theft during the transfer process from underground storage tanks is a significant issue. Companies store large quantities of oil underground in tanks to ensure safety and ease of transfer. However, during the transfer process, workers may create unauthorized leeway pipes to siphon off oil illegally. This theft, often difficult to detect in real-time, leads to significant financial losses for companies and, on a broader scale, negatively impacts the economy. Oil theft also undermines the efficiency of operations, compromises the integrity of oil distribution, and creates trust issues between management and workers.

The root cause of this problem lies in the lack of effective monitoring and detection systems during the oil transfer process. Current systems often fail to identify when and where theft occurs, leaving companies vulnerable. The problem is of utmost importance because the economic and reputational damage caused by oil theft can be substantial, threatening the sustainability of businesses in this industry. Detecting and preventing oil theft can save costs, improve operational integrity, and contribute positively to the economy.

* 1. **Solution to the Problem**
     1. **Related Works**

The following entails a look into past efforts into this topic:

* + - 1. **IoT-Based Oil Theft Prevention**

Sun et al. [1] propose an IoT-based system to prevent crude oil theft by detecting abnormal vibrations and noise in real-time. Their solution integrates Wireless Sensor Networks (WSN) and RFID to monitor both oil pipelines and tank trucks, sending alerts upon detecting anomalies. Key challenges include high sensor costs, power supply issues, and securing remote infrastructure. While promising, the study lacks empirical validation and implementation feasibility in diverse geographical conditions.

* + - 1. **Oil Theft and Economic Impact in Nigeria**

Anyio [2] examines how illegal oil bunkering in Nigeria leads to significant economic losses, estimated at N1.29 trillion annually, and contributes to environmental degradation. The study critiques the Nigerian government’s inadequate response and suggests stricter legal enforcement and international collaboration to curb oil theft. However, the research is heavily reliant on secondary data without direct case studies or field validation.

* + - 1. **Global Oil Theft and Policy Solutions**

Romsom [3] estimates global oil theft at $133 billion annually, affecting government tax revenues and fueling organized crime. The study highlights the role of transnational syndicates and suggests international cooperation, better data tracking, and economic policy reforms to mitigate theft. Though comprehensive, the analysis relies on estimated data, lacking specific case studies on successful interventions.

* + - 1. **Comparative Insights**

Sun et al. [1] focus on a technical IoT-based solution, whereas Anyio [2] and Romsom [3] analyze economic and policy impacts. While Anyio [2] focuses on Nigeria, Romsom [3] presents a global perspective on oil theft. All studies emphasize security risks and recommend government intervention, but Sun et al. [1] lack empirical testing of their proposed solution.

* + - 1. **Conclusion**

The reviewed works highlight oil theft as a global challenge with technological, economic, and policy implications. Future research should combine empirical case studies with technological interventions for a comprehensive approach to oil theft prevention.

After considering the previous work related to this topic, to address this issue in our contet, two possible solutions can be considered:

* + 1. **Solution 1: Using Microcontrollers and Cloud Computing for Real-Time Monitoring**

The proposed primary solution involves using a combination of microcontrollers and cloud computing technologies to detect unauthorized oil siphoning in real time. The solution includes installing sensors on pipelines to monitor flow rates and detect anomalies that may indicate theft. These sensors will be connected to a microcontroller that processes the data and transmits it to a cloud server for logging and analysis. Alerts will be generated if anomalies are detected, enabling quick action by the management team.

This solution is particularly appropriate because it provides real-time monitoring, remote access to data, and a tamper-proof logging system. It ensures transparency and facilitates immediate response to suspicious activities, thus effectively addressing the root cause of the problem. Furthermore, the proposed system is scalable, cost-effective, and aligns with business objectives to reduce losses and improve operational efficiency.

The system's feasibility is supported by the availability of affordable microcontrollers, sensors, and cloud services. It integrates modern IoT (Internet of Things) technologies with minimal disruption to existing operations.

Existing studies in this area highlight the use of flow sensors, pressure monitors, and IoT devices for monitoring oil theft. However, these systems often lack the integration of advanced analytics and cloud-based logging. The proposed solution builds on these studies by incorporating real-time alerts, centralized monitoring, and data analytics for improved decision-making.

* + 1. **Solution 2: Weight Measurement of the Oil Tanker at Departure and Arrival**

An alternative solution is to record the weight of an oil tanker when it departs from Point A and then again when it reaches Point B, where the oil is stored underground. Any discrepancies in weight could indicate potential oil theft during transit. This method relies on comparing the expected weight loss due to legitimate fuel consumption against the actual weight difference.

While this method may provide a broad indication of theft, it has several limitations:

* It does not offer real-time monitoring, making it difficult to detect theft as it occurs.
* Weight measurements can be influenced by external factors such as road conditions, fuel consumption variations, or environmental conditions.
* If theft occurs in small, distributed amounts, it may not be noticeable in weight measurements.
* It does not provide specific information about where or when the theft happened, making it difficult to take immediate action.

Due to these constraints, while weight monitoring can serve as a useful supplementary measure, it is not a comprehensive or real-time solution for oil theft detection. More advanced technologies, such as IoT-based flow sensors, GPS tracking, and automated anomaly detection, offer greater accuracy, real-time alerts, and detailed forensic data to effectively combat oil theft.

* + 1. **Justification for Preferring the First Solution**

While the weight measurement method may provide some insight into oil loss, the microcontroller and cloud-based monitoring system is the superior solution because it:

* Detects anomalies in real-time, allowing for immediate intervention.
* Provides precise data on when and where theft occurs.
* Integrates with cloud-based analytics for better decision-making.
* Is scalable and can be extended to multiple storage locations.

Given the role of software in this course, the preferred solution leverages software-based monitoring, cloud computing, and IoT for effective theft detection and prevention. This ensures that oil theft can be mitigated with higher accuracy, efficiency, and transparency.

1. **SOLUTION DESCRIPTION**
   1. **System Features**

**Functional Requirements:**

1. **Flow Monitoring:**
   * The system must continuously measure the volume and speed of oil flowing through pipelines using flow sensors.
   * It should support multiple sensor types (e.g., ultrasonic, electromagnetic, or turbine flow meters) to suit different pipeline conditions.
   * Real-time data should be transmitted to a central monitoring system to detect irregularities immediately.
2. **Anomaly Detection:**
   * The system should analyze flow rate patterns to identify unusual fluctuations that could indicate oil theft, leaks, or unauthorized siphoning.
   * Machine learning or rule-based algorithms may be used to improve anomaly detection accuracy.
   * It must minimize false alarms by distinguishing between normal operational variations and actual threats.
3. **Data Logging:**
   * All flow readings, detected anomalies, and system alerts should be logged in a cloud database for future analysis.
   * The logging mechanism must be tamper-proof to ensure data integrity.
   * Data retention policies should be defined to determine how long records will be stored before archival or deletion.
4. **Real-Time Alerts:**
   * When the system detects a potential theft or anomaly, it should trigger an immediate alert.
   * Alerts should be sent via multiple channels, such as SMS, email, or mobile app notifications, to ensure timely responses.
   * The system should classify alerts based on severity (e.g., warning, critical, emergency) to help management prioritize actions.
5. **Remote Monitoring:**
   * A web-based dashboard should allow users to access live and historical flow data from anywhere.
   * The interface should display key metrics such as current flow rate, past anomalies, and system health status.
   * Access control mechanisms should be in place to prevent unauthorized users from viewing or modifying data.
6. **Tamper Detection:**
   * The system should detect physical tampering attempts on sensors, controllers, or communication links.
   * Possible tampering indicators include sudden sensor disconnections, unusual data spikes, or unauthorized access attempts.
   * The system should log all tampering attempts and generate alerts to notify the security team immediately.

**Quality Attributes:**

1. **Reliability:**
   * The system should maintain high uptime, ensuring continuous oil flow monitoring with minimal downtime.
   * Redundant components (backup power supply, alternative communication links) should be used to avoid data loss.
2. **Accuracy:**
   * Flow sensors must have high precision to detect even minor changes in flow rates, reducing false positives and negatives.
   * The system should perform periodic calibrations and self-diagnostics to maintain measurement accuracy.
3. **Scalability:**
   * The system should allow easy addition of new sensors to cover expanded pipeline networks.
   * The cloud infrastructure should be designed to scale up storage and processing capabilities based on increasing data volumes.
4. **Security:**
   * End-to-end encryption must be implemented to protect data transmitted between sensors, controllers, and the cloud.
   * Access control mechanisms (role-based permissions, two-factor authentication) should prevent unauthorized access.
   * The system should regularly check for cybersecurity vulnerabilities and apply security patches accordingly.
5. **Ease of Use:**
   * The web-based interface should be intuitive and visually clear, using graphs and alerts for easy interpretation.
   * Non-technical staff should be able to operate and navigate the system without extensive training.
6. **Cost-Effectiveness:**
   * The system should balance affordability with performance, using cost-efficient sensors and cloud services.
   * Open-source software or commercially viable alternatives should be used to reduce licensing costs.
   * Maintenance and operational costs should be minimized through automated diagnostics and remote troubleshooting.

This system will significantly improve oil theft detection and prevention by combining real-time monitoring, anomaly detection, and remote accessibility. With robust security, accuracy, and reliability, it will enhance operational integrity and financial savings while ensuring seamless scalability for future expansions.

* 1. **UML Diagrams** 
     1. **Activity Diagram**

**A diagram of a flowchart

Description automatically generated**

**Figure 1.** Activity Diagram.

* + 1. **Class Diagram**

A diagram of a computer

Description automatically generated

**Figure 2.** Class diagram.

* + 1. **Entity-Relationship Diagram**

**A screenshot of a computer

Description automatically generated  
Figure 3.** Entity Relationship Diagram.

1. **Social Impact**

The implementation of this project has the potential to generate significant social benefits. By preventing oil theft, the solution contributes to:

1. **Economic Stability:** Reducing oil theft minimizes financial losses for companies, resulting in improved profitability and sustainability. This, in turn, contributes positively to the national economy by preserving resources and reducing wastage.
2. **Job Security and Fairness:** Implementing such a system ensures that honest workers are not unfairly accused of theft, fostering a fair and trustworthy work environment. It discourages dishonest practices and promotes accountability among employees.
3. **Environmental Protection:** Preventing unauthorized siphoning of oil reduces the likelihood of spills and environmental contamination, contributing to cleaner and safer surroundings.
4. **Improved Public Trust:** By addressing a common problem in the oil distribution sector, the project enhances public trust in companies, demonstrating their commitment to ethical practices and operational transparency.
5. **Innovation and Technological Advancement:** The project encourages the adoption of advanced technologies such as IoT and cloud computing, setting a precedent for other industries to innovate and modernize their operations.
6. **Policy and Regulatory Compliance:** The system helps companies comply with governmental and environmental regulations by ensuring secure and monitored oil transfer processes, reducing the risk of legal penalties associated with oil theft or spills.

In summary, this project not only benefits companies by reducing financial losses but also creates a ripple effect of positive social, environmental, and economic outcomes that extend to the broader community.

1. **Development Plan with Project Schedule**
   1. **Development Plan**

****

**Figure 4.** Project List View.

The development of this project has been divided into five parts, each containing their respective tasks. For this project the project management tool: ClickUp, has been utilized.

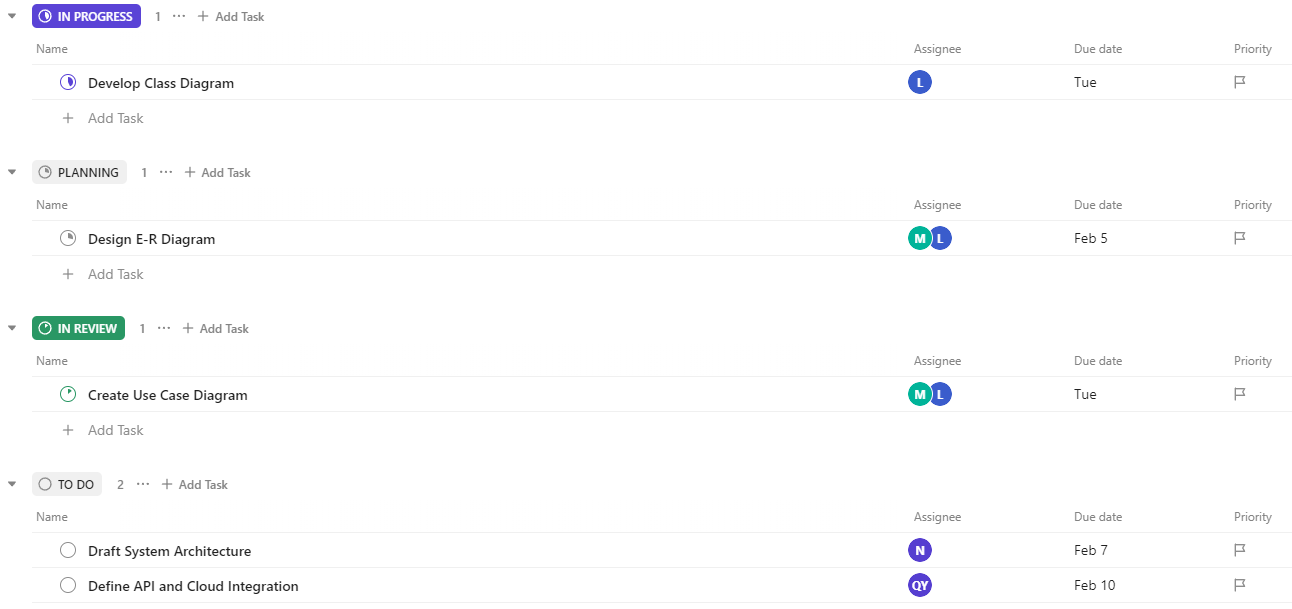
* + 1. **List 1- Project Planning:**

**A screenshot of a computer

Description generated with very high confidence**

**Figure 5.** Project Planning Tasks.

* + 1. **List 2- System Design & Documentation:**

****

**Figure 6.** System Design & Documentation Tasks.

* + 1. **List 3- Hardware & Software Development:**

**A white background with black lines

Description generated with high confidence**

**Figure 7.** Hardware & Software Development Tasks.

* + 1. **List 4- Testing & Integration:**

**A white paper with black lines

Description generated with high confidence**

**Figure 8.** Testing & Integration Tasks.

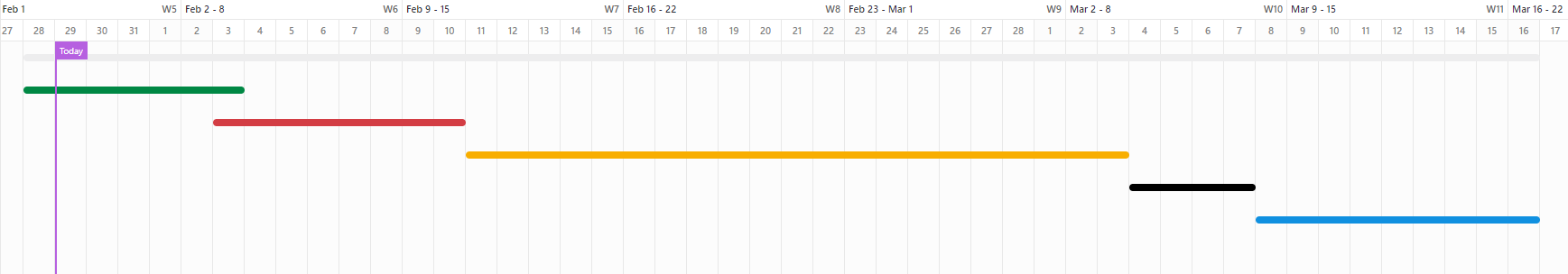
* + 1. **List 5- Deployment & Maintenance:**

**A white background with black lines

Description generated with high confidence**

**Figure 9.** Deployment & Maintenance Tasks.

* 1. **Project Schedule**
     1. **Gantt Chart**

****

**Figure 10.** Gantt Chart of all Lists.

* + 1. **Task Status**

**A pie chart with text on it

Description generated with high confidence**

**Figure 11**. Project Workload.

1. **Marketing Plan**
   1. **Short Term Marketing Plan (0 - 6 Months)**

In the initial phase, the primary objective is to generate awareness and attract early adopters. This will be achieved through branding, digital marketing, direct outreach, and promotional offers.

* Branding & Messaging: Establish a strong brand identity with a professional logo, website, and an explainer video that clearly demonstrates how the system works.
* Digital Marketing: Launch an SEO-optimized website and run LinkedIn Ads targeting oil and gas company executives, logistics managers, and fuel storage facilities.
* Direct Outreach & Networking: Email marketing campaigns will be conducted to introduce the product to potential clients. Additionally, participation in trade fairs, security expos, and industry conferences will help showcase the solution to a broader audience.
* Early Adopter Deals: Offering pilot programs and free demonstrations will encourage companies to test the system, increasing confidence in its effectiveness.

By leveraging these strategies, the goal is to secure the first set of clients and establish credibility in the industry.

* 1. **Long Term Marketing Plan (6 Months – 2 Years)**

Once initial traction is gained, the focus will shift towards expansion, partnerships, and brand authority. This phase ensures long-term sustainability and growth.

* Industry Partnerships: Collaborations with IoT security firms and oil distribution companies will help integrate the system with existing monitoring infrastructures. Partnering with insurance firms to offer discounts on theft prevention policies can also drive adoption.
* Content Marketing & Thought Leadership: Regular publishing of case studies, whitepapers, and blog articles on oil theft prevention will position IOTDS as an industry leader.
* Government & Regulatory Compliance: Engaging with government agencies and regulatory bodies can help establish IOTDS as a standard security requirement for oil storage and transfer processes.
* Franchise & Reseller Network: Establishing a network of authorized distributors and offering a subscription model for software updates will create recurring revenue and expand market reach.

By executing these strategies, IOTDS will move from being a new product to a market leader in the oil theft detection industry.

* 1. **Continuous Marketing Plan (Ongoing Strategies)**

To maintain growth and ensure customer satisfaction, continuous marketing strategies will be implemented. These include customer engagement, product innovation, public relations, and referral programs.

* Customer Engagement & Support: Providing 24/7 customer support, periodic training sessions, and a customer loyalty program will help retain clients.
* Continuous Product Innovation: Collecting user feedback to improve the system, integrating AI-based theft detection, and developing a mobile app for remote monitoring will enhance user experience.
* Community & Public Relations: Hosting webinars, industry discussions, and press releases will keep IOTDS relevant in the market and build trust with stakeholders.
* Referral & Affiliate Programs: Encouraging satisfied clients to refer new customers and partnering with security consultants and oil industry experts will boost credibility and sales.

By focusing on continuous improvements and maintaining strong customer relationships, IOTDS will ensure long-term success and industry recognition.

1. **Cost and Profit Analysis**
   1. **Cost Analysis**

The cost structure for IOTDS consists of three major components: development costs, marketing costs, and operational expenses.

* + 1. **Development Costs (One-Time Investment)**

The initial development cost includes hardware procurement, software development, and cloud infrastructure setup.

|  |  |
| --- | --- |
| **CATEGORY** | **ESTIMATED COST (BDT)** |
| Microcontrollers & sensors (flow, pressure, tamper) | 610,000.00৳ |
| Cloud server & storage setup | 2,500.00৳ |
| Software development (Dashboard, Alerts, API) | 10,000.00৳ |
| Ai & data analytics integration | 4,000.00৳ |
| Security & encryption | 3,000.00৳ |
| Testing & quality assurance | 2,500.00৳ |
| **TOTAL DEVELOPMENT COST** | **632,000.00৳** |

* + 1. **Marketing Costs (Initial + Ongoing)**

Marketing expenses cover branding, advertising, and outreach efforts to promote the product.

|  |  |
| --- | --- |
| **CATEGORY** | **ESTIMATED COST (BDT)** |
| Website Development & SEO | 244,000.00৳ |
| Digital Advertising (Google, LinkedIn, Facebook) | 427,000.00৳ |
| Industry Expo & Trade Shows | 488,000.00৳ |
| Sales Team & Business Development | 610,000.00৳ |
| Content Marketing (Videos, Blogs, Whitepapers | 366,000.00৳ |
| Referral & Affiliate Programs | 305,000.00৳ |
| **TOTAL MARKETING COSTS** | **2,440,000.00৳** |

* + 1. **Operational Costs (Annual)**

Recurring costs include maintenance, cloud hosting, customer support, and continuous development.

|  |  |
| --- | --- |
| **CATEGORY** | **ANNUAL COST (BDT)** |
| Cloud Hosting & Server Maintenance | 366,000.00৳ |
| Software Updates & Enhancements | 610,000.00৳ |
| Customer Support & Training | 488,000.00৳ |
| Sales & Marketing (Ongoing) | 732,000.00৳ |
| **TOTAL ANNUAL OPERATIONAL COSTS** | **2,196,000.00৳** |

* 1. **Profit Analysis**
     1. **Revenue Model**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Pricing** | **Expected Clients (Year 1)** | **Total Revenue** |
| Hardware Kit (Sensors & Microcontroller) per unit | 30,500.00৳ | 50 | 1,525,000.00৳ |
| Subscription Fee (Cloud & Monitoring) per month | 12,200.00৳ | 50 | 610,000.00৳ |
| Custom Enterprise Solutions per client | 1,220,000.00৳ | 5 | 6,100,000.00৳ |
| **Total Revenue (Year 1)** |  |  | **8,235,000.00৳** |

* + 1. **Profit Calculation (Year 1)**

|  |  |
| --- | --- |
| **FINANCIAL ASPECT** | **AMOUNT (BDT)** |
| Total Revenue | 8,235,000.00৳ |
| Total Costs (Development + Marketing + Operations) | 5,268,000.00৳ |
| Net Profit | 2,967,000.00৳ |
| **PROFIT MARGIN** | **36.03%** |

* 1. **Total Costs**

**Figure 12**. Total Costs for IOTDS.

The high-profit margin and scalability of the system make IOTDS a highly attractive investment opportunity.

* Break-even point: Achieved within 5-6 months after securing first 50 clients.
* Scalability: Expanding to larger fuel storage and logistics markets can triple revenue within 2 years.
* Future Growth Potential: Integrating AI-powered predictive analytics and expanding internationally can lead to exponential business growth.

The IOTDS business model demonstrates a strong return on investment (ROI) and rapid profitability. With an initial investment of $65,000, the system can generate $235,000 in the first year, resulting in a net profit of $170,000. By adopting a subscription model and targeting large-scale industries, the revenue potential can increase significantly over the next few years.

1. **Reference**

[1] X. Sun, Y. Cui, and J. Chen, “The Intelligent Crude Oil Anti-Theft System Based on IoT Under Different Scenarios,” in Proc. Int. Conf. on Mechatronics and Automation, 2016, pp. 1234–1240.

[2] M. Anyio, “Illegal Oil Bunkering and Oil Theft in Nigeria: Impact on the National Economy and the Way Forward,” African Journal of Economic Policy, vol. 22, no. 3, pp. 45–60, 2015.

[3] J. Romsom, “Global Oil Theft: Impact and Policy Responses,” Energy Studies Working Paper Series, no. 56, 2022.