Components of ensuring secure infrastructure for environmental monitoring systems using the LwM2M protocol

Kyrylo Vadurin[1,*,†], Andrii Perekrest[1,†], Dmytro Mamchur[1,†] and Serhii Vladov[2,†]

[1]Department of Computer Engineering and Electronics, Kremenchuk Mykhailo Ostrohradskyi National University, Universytetska Str., 20, Kremenchuk, 39600, Ukraine

[2]Kharkiv National University of Internal Affairs, L. Landau Avenue, 27, Kharkiv, 61080, Ukraine

Abstract

This research focuses on the security processes within the infrastructure of environmental monitoring systems employing the LwM2M protocol. The main objective is to develop a set of technical solutions aimed at securing the infrastructure of LwM2M-based environmental monitoring systems. This includes risk assessment methods, anomaly detection models, and adaptive access control algorithms. The developed solutions are designed to enhance data protection and ensure reliable system operation under resource constraints and dynamic threat conditions. The work involves the analysis of existing scientific, practical, and design solutions, as well as relevant hardware and software in the field of environmental monitoring system security using the LwM2M protocol. A concept, method, models, and algorithms are developed to achieve the research objective. The technical aspects of implementing the proposed concept are considered, including the synthesis of a list of potential user interaction capabilities, the development of a solution class diagram.

Keywords

LwM2M protocol, Internet of Things (IoT), environmental monitoring systems, information security, cybersecurity, risk assessment, anomaly detection, access control, secure bootstrapping, network traffic analysis

1. Introduction

Currently, there is a discernible trend towards the active implementation of Internet of Things (IoT) technologies across various domains, including environmental monitoring. This facilitates real-time data acquisition, enhances the celerity of responses to environmental threats, and refines natural resource management processes. The LwM2M protocol, designed for resource-constrained devices, is becoming increasingly prevalent for constructing such systems. However, the extensive utilization of IoT devices also introduces new challenges in the realm of information security.

The pertinence of the planned research stems from the necessity to ensure robust protection of data collected by environmental monitoring systems against unauthorized access, modification, or loss. Compromise of such data can lead to an erroneous assessment of the ecological situation, the adoption of ineffective managerial decisions, and, consequently, to detrimental impacts on the environment and public health. Considering the distributed nature of IoT systems and the limited resources of devices, traditional information protection methods may prove insufficiently effective.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.

†These authors contributed equally.

kir3337@gmail.com (K. Vadurin); pksg13@gmail.com (A. Perekrest); dgmamchur@gmail.com (D. Mamchur); serhii.vladov@univd.edu.ua (S. Vladov)

https://cee.kdu.edu.ua/en/content/vadurin-kyrylo-olehovych (K. Vadurin); https://cee.kdu.edu.ua/en/content/perekrest-andriy-leonidovych (A. Perekrest); https://cee.kdu.edu.ua/en/content/mamchur-dmytro-hryhorovych (D. Mamchur); https://klk.univd.edu.ua/uk/dir/1249 (S. Vladov)

0000-0001-7781-5783 (K. Vadurin); 0000-0002-7728-9020 (A. Perekrest); 0000-0002-2851-878X (D. Mamchur); 0000-0001-8009-5254 (S. Vladov)

Based on an analysis of works by other authors, it has been established that existing solutions often concentrate on discrete aspects of security, such as communication channel protection or device authentication. Nevertheless, to ensure comprehensive protection, it is imperative to consider all stages of the data lifecycle, from collection to storage and analysis, as well as to ensure the adaptability of the security system to evolving conditions and threats. Difficulties exist in integrating LwM2M with extant systems that utilize other protocols, and also in managing security within large-scale and heterogeneous IoT networks. Insufficient attention has been devoted to issues of information security risk assessment and the development of effective mitigation strategies, considering economic aspects.

The object of this work encompasses the processes of ensuring the security of the infrastructure for environmental monitoring systems that employ the LwM2M protocol. The subject of this work comprises the methods, models, and algorithms that allow for an enhancement of the data protection level and ensure the reliable functioning of environmental monitoring systems based on the LwM2M protocol. The aim of this work is to develop a comprehensive suite of technical solutions for ensuring a secure infrastructure for environmental monitoring systems based on the LwM2M protocol. This suite includes risk assessment methodologies, anomaly detection models, and adaptive access control algorithms, and is designed to elevate the level of data security and ensure the reliable operation of the system under conditions of limited resources and dynamic threats.

The principal unresolved tasks at present are:

- Development of a mathematical model for information security risk assessment for LwM2M-based environmental monitoring systems, enabling quantitative evaluation of potential threats and justification for the selection of effective protective measures.
- Development of a mathematical model for anomaly detection in environmental monitoring data using statistical methods and machine learning techniques, allowing for the identification of atypical parameter values that may indicate cyberattacks or device malfunctions.
- Development of an algorithm for dynamic access control to LwM2M device resources based on Attribute-Based Access Control (ABAC), facilitating flexible management of access rights depending on user roles, system state, and other contextual factors.
- Development of an algorithm for secure bootstrapping of LwM2M devices, ensuring the protected provisioning of credentials and configuration parameters on the device using mutual authentication and encryption.
- Development of an algorithm for detecting anomalies in LwM2M traffic, which analyzes network interaction characteristics (packet size, request frequency, operation types) to identify atypical behavior that may indicate cyberattacks or device malfunctions.

2. Analysis of the subject area and formulation of work tasks

2.1. Analysis of existing scientific and practical solutions

Ensuring a secure infrastructure for environmental monitoring systems (EMS), particularly those utilizing the Lightweight M2M (LwM2M) protocol, is crucial for environmental and public health due to their reliance on accurate and secure data [1]. Internet of Things (IoT) technologies enable real-time data collection, analysis, and forecasting in this domain [1]. LwM2M, designed for resource-constrained IoT devices, standardizes device and service management, facilitating environmental data collection (e.g., air quality, temperature) and remote device control through its client-server architecture [2, 3]. Interoperability is ensured via OMA LwM2M Registry Objects and Resources [3]. Security is a fundamental aspect of LwM2M and EMS, with the protocol offering secure communication through authentication methods (PSK, RPK, X.509 certificates), data encryption, and granular access control [3]. Secure bootstrapping provisions client credentials, and DTLS/TLS protocols are employed for secure data transmission [4, 5]. Despite these built-in security features, LwM2M and IoT devices remain susceptible to vulnerabilities, including difficulties in implementing and managing security at scale, inherent protocol or implementation weaknesses, network limitations affecting reliability, and

risks from incorrect configuration or integration [6, 1]. To enhance the security of LwM2M-based IoT infrastructure, best practices emphasize prioritizing security from the design phase, optimizing for low energy consumption, ensuring interoperability, planning for scalability, and continuous management through updates and monitoring [6, 4]. Utilizing reliable tools, platforms, and cloud services (e.g., Eclipse Wakaama, Leshan, AWS, Azure, Google Cloud) further strengthens security, alongside hardware security measures like HSMs and secure boot [7, 8, 9, 10, 11]. EMS also employ diverse technologies for data collection (sensors, satellite), transmission (ZigBee, LoRaWAN), and processing (edge/cloud computing, AI, blockchain) [10, 12, 13]. Despite these advancements, challenges persist in areas such as optimal sensor placement, mathematical modeling, LwM2M integration with existing systems, managing large heterogeneous IoT networks, and ensuring regulatory compliance [4, 11, 12].

2.2. Analysis of design solutions and software-hardware

Designing a secure infrastructure for EMS using the LwM2M protocol primarily adopts a client-server model, where EMS devices act as LwM2M clients and servers manage and collect data [6, 9]. This architecture standardizes interactions and simplifies device integration into a cohesive ecosystem [6, 14]. LwM2M offers standardized device management functions, including registration, bootstrapping, and data exchange [4, 6]. Its hierarchical data structure, utilizing Objects, Object Instances, and Resources, clearly defines device functionality and sensor data, while LwM2M gateways facilitate centralized management by integrating devices that do not natively support the protocol [7, 9].

Security is a paramount design consideration, leveraging LwM2M's inherent mechanisms such as authentication (PSK, RPK, X.509), communication encryption, and access control [1, 6]. Secure bootstrapping is essential for reliable device setup and credential distribution [2, 6]. The hardware components for EMS often include wireless microcontrollers with built-in security features like encryption acceleration, secure boot, and Trusted Execution Environments (TEE), exemplified by components from Microchip and NXP, ensuring device-level data confidentiality [11]. Wireless communication relies on standards like IEEE 802.15.4, Wi-Fi, and LPWAN technologies such as LoRaWAN [4, 11]. Software components encompass open-source LwM2M client (e.g., wakaama, Leshan) and server implementations (e.g., Leshan, SkyCase IoT Platform), embedded TLS/DTLS libraries (e.g., wolfSSL) for secure transport, and specialized tools for microcontroller software development and network security monitoring [4, 5, 11, 7]. The LwM2M protocol brings several security advantages to EMS. Its design prioritizes resource-constrained devices, enabling energy-efficient communication crucial for distributed sensor networks [6, 9]. LwM2M also provides standardized device lifecycle management, including remote firmware updates, status monitoring, and diagnostics, which are vital for maintaining security throughout a device's operational life [6, 9]. Its native security features—authentication, encryption, and access control—effectively safeguard data against unauthorized access and interception [6]. Furthermore, LwM2M simplifies development by standardizing data formats and streamlining complex authentication, allowing developers to concentrate on core system functionality while ensuring reliability and security [9]. This integration of LwM2M with appropriate hardware and software forms a robust foundation for scalable, flexible, and secure EMS [15].

2.3. Analysis of methods used in similar works

Securing environmental EMS, particularly those leveraging the LwM2M protocol, is a complex endeavor that integrates various technologies. Innovations such as IoT, sensor networks, artificial intelligence, modeling, and Geographic Information Systems (GIS) are crucial for effective environmental security monitoring and management [3]. The infrastructure of EMS typically features a multi-layered architecture, encompassing a physical layer with intelligent sensors and communication interfaces, an operating system abstraction layer, middleware, and an application layer [12]. Cloud storage, fortified with security measures, is widely used for data reliability, while GIS aids in managing and visualizing geographically referenced environmental data [11]. Hardware security mechanisms, including embedded security modules and TrustZone technology, are also being explored to enhance trust and

protect critical operations within these monitoring systems [11]. The LwM2M protocol, designed for resource-constrained devices, operates with an LwM2M client on the end device, an LwM2M Server for management, and an LwM2M Bootstrap Server for authentication and configuration [7, 9]. It standardizes data formats using concepts like objects, object instances, and resources, simplifying IoT solution development [9]. Originally based on CoAP over UDP with DTLS for security, later versions of LwM2M expanded to support CoAP over TCP/TLS, MQTT, and HTTP, alongside updates for TLS and DTLS 1.3 [5]. LwM2M implements security at both transport (DTLS for UDP or TLS for TCP) and application (optional OSCORE) levels, which can collectively provide end-to-end security [9]. It supports various client-server authentication modes, including Pre-Shared Key (PSK) and certificate mode, and incorporates key security mechanisms such as authentication, communication encryption, access control, and secure bootstrapping to protect data [6, 9]. Mandatory LwM2M objects like Security Object (/0), Server Object (/1), and Device Object (/3) manage credentials, secure communication, and device information [9].

Despite its built-in security features, LwM2M implementation in environmental monitoring faces challenges, including the complexity of managing security in large-scale deployments, network limitations affecting communication reliability, inherent protocol vulnerabilities requiring updates, and difficulties in integrating LwM2M with existing systems [6]. To address these, best practices recommend prioritizing security from a project's inception, which involves secure bootstrapping with mutual authentication and encryption, encrypting all device-server communication, and implementing detailed access control policies [6]. Additionally, optimizing for low energy consumption, carefully selecting appropriate tools and platforms—including reliable LwM2M client/server software, development frameworks, and cloud integration—is crucial [6]. Thorough testing, including environment simulation and security assessments, along with continuous management such as regular firmware updates, device status monitoring, and security policy reviews, are essential to maintain robust security against evolving threats [6].

2.4. Consolidated review of the subject area and identification of research gaps

Ensuring a secure infrastructure for EMS, particularly those utilizing the LwM2M protocol, is critically important due to their role in environmental and public health, relying heavily on data reliability and security. IoT technologies facilitate real-time data collection, analysis, and forecasting in this domain. The LwM2M protocol, designed for resource-constrained IoT devices, provides a standardized approach to device and service management, which is highly beneficial for EMS. Its client-server architecture, based on standardized Objects and Resources, ensures interoperability and simplifies device integration into a unified ecosystem, even allowing for LwM2M gateways to incorporate devices that do not directly support the protocol. Security is a paramount aspect of LwM2M and EMS. The LwM2M protocol incorporates a suite of built-in security mechanisms, including various authentication methods (PSK, RPK, X.509 certificates), communication encryption for data protection, detailed access control to resources, and a secure bootstrapping process for reliable device setup and credential distribution. Secure data transmission is achieved at the transport layer using DTLS and TLS protocols, and at the application layer via OSCORE. However, despite these features, vulnerabilities and challenges exist, such as the complexity of implementing and managing security in large-scale deployments, weaknesses in the protocol or its implementation requiring regular updates, network limitations affecting reliability, incorrect configuration, and difficulties in integrating LwM2M with existing systems that use other protocols. To achieve the necessary security level for LwM2M-based IoT infrastructure, adherence to best practices is crucial. This involves prioritizing security throughout the system lifecycle, including secure device bootstrapping, mandatory encryption of all communications, implementing granular access control policies, and optimizing device operation for energy efficiency. Thorough system testing and continuous management, including regular updates and monitoring, are also essential. Furthermore, leveraging reliable tools, platforms, cloud services, and hardware security measures like Hardware Security Modules (HSMs) and secure boot technologies significantly enhances protection. While various methods and technologies, such as sensors, AI, GIS, and blockchain, are employed in EMS, unresolved

challenges persist, including optimal spatial placement of monitoring stations, improving mathematical modeling, and managing security in large, heterogeneous IoT networks, alongside ensuring compliance with regulatory requirements.

3. Development of concept, method, models, and algorithms aimed at achieving the work's goal

3.1. Formalization of the solution concept

The concept for securing EMS, particularly those using the LwM2M protocol, is built upon a comprehensive approach. This approach integrates the protocol's built-in security mechanisms, cryptographic protection methods, best practices for device and data security, and advanced analytical methods for cyber threat detection and prevention. This comprehensive strategy is vital due to the critical importance of reliable and secure environmental monitoring data for public health and environmental preservation [3, 10, 11, 8]. The LwM2M protocol's application offers a standardized way to interact with resource-constrained IoT devices, providing consistent management and data collection [15]. The concept is defined by three fundamental principles. Firstly, security mechanisms must be integrated at every level of the EMS, from sensor devices to the management server, to ensure end-to-end data protection [6, 9]. This involves reinforcing LwM2M's authentication, encryption, and access control features throughout the system to address vulnerabilities across data processing and transmission stages [6, 9, 8]. Secondly, the concept advocates for adaptive protection methods that dynamically adjust security parameters based on current risk levels and available resources, optimizing energy consumption and computational power while maintaining necessary protection in diverse IoT environments [6]. Thirdly, the EMS must comply with regulatory requirements and industry standards for information security, particularly given the critical nature of environmental data, necessitating careful implementation of technical and organizational measures [16]. Structural elements crucial for implementing this concept include secure sensor devices, a secure LwM2M server, and a robust security monitoring and management system. Secure sensor devices should feature built-in hardware and software protection, such as encryption modules and secure boot, alongside LwM2M client implementations that support secure modes like DTLS/TLS and OSCORE [11, 9, 6]. The secure LwM2M server serves as a central hub, ensuring reliable device authentication, encrypted communications, strict access control, and secure data storage, while also managing device lifecycles including secure bootstrapping and firmware updates [6]. The security monitoring and management system provides intrusion detection, security event analysis, and incident response capabilities, tracking component security status and responding to anomalies [17, 18]. The concept's key formulations can be formalized through mathematical models and algorithms. A mathematical model for information security risk assessment evaluates potential threats, aiding in prioritizing security measures and allocating resources effectively [11, 6]. While not directly a security model, a mathematical model for optimizing sensor placement considers constraints like energy consumption and network bandwidth, indirectly influencing system availability and resilience [4, 6]. Furthermore, a mathematical model for anomaly detection in environmental monitoring data, utilizing statistical methods or machine learning, identifies atypical values that could indicate natural events or cyberattacks like data spoofing [3, 12, 11, 9]. Practical algorithms supporting this concept include a secure bootstrapping algorithm for reliable device connection and credential provisioning, a dynamic access control algorithm for flexible management of LwM2M resource rights (e.g., using ABAC), and an algorithm for detecting anomalies in LwM2M traffic to identify unusual network behavior indicative of cyber threats [6, 9, 11, 3, 12].

3.2. Planning the structural scheme of the solution

The structural scheme for a secure EMS solution using the LwM2M protocol is built on a comprehensive approach. This includes leveraging LwM2M's built-in security, cryptographic protection, best practices for device and data security, and integrating cyber threat detection and prevention methods. This

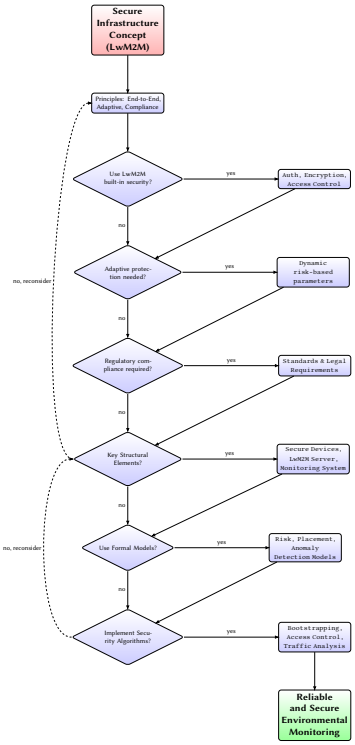

Figure 1: Flowchart illustrating the formalized solution concept for ensuring secure LwM2M-based environmental monitoring infrastructure.

approach is necessitated by the critical importance of reliable and secure environmental monitoring data for public health and environmental preservation [3, 10]. The solution concept integrates security mechanisms at every system level, employs adaptive protection methods, and ensures compliance with relevant regulatory documents and industry standards. Based on the analysis, the core structural elements include secure LwM2M-enabled sensor devices, a secure LwM2M server, and a dedicated security monitoring and management system [6, 7].

For sensor device implementation, the Espressif ESP32 WROOM 32E microcontroller was selected due to its accessibility, communication capabilities (Wi-Fi, Bluetooth), and sufficient resources for LwM2M client and cryptographic operations [11]. Integrated environmental sensors include those for air quality (MQ135), temperature/humidity (DHT22), and dust (PM2.5), chosen based on typical monitoring tasks [3, 10, 11]. While initial implementation uses ESP32, the concept acknowledges the value of microcontrollers with built-in hardware encryption accelerators and secure boot functions, such as Microchip PIC32CM5164LS60064 or NXP LPC55S3x, for enhanced data confidentiality and integrity [11]. Device communication with the server utilizes Wi-Fi, with CoAP/LwM2M protocols secured via DTLS for encrypted data transmission [6]. At the software level for sensor devices, open-source LwM2M client implementations like wakaama or Zephyr OS were chosen for their lightweight nature and suitability for resource-constrained environments [7, 9]. The wolfSSL library was integrated to provide optimized DTLS/TLS for secure transport layer communications in embedded systems [1, 11]. This software facilitates data collection from sensors, formats it according to the LwM2M object model, and securely transmits it to the LwM2M server using LwM2M security profiles (PSK, RPK, or certificates), aligning with the concept's emphasis on utilizing built-in protocol security mechanisms [6, 9]. For the LwM2M server, the Eclipse Foundation's open-source Leshan platform was selected, supporting all necessary LwM2M operations and security mechanisms (DTLS with PSK, RPK, X.509) [7, 9]. Data collected by the server is stored securely in either a relational (e.g., PostgreSQL) or document-oriented (e.g., MongoDB) database [12]. The security monitoring and management system is implemented as a separate Python-based module that interacts with the LwM2M server, analyzing security logs and detecting anomalies in environmental data and network traffic [3, 12]. This module integrates mathematical models for anomaly

detection, based on statistical methods or machine learning, and algorithms for detecting anomalies in LwM2M traffic to identify atypical behavior [3, 12]. Key algorithms like secure bootstrapping, which ensures protected provisioning of credentials using mutual authentication and encryption, and dynamic access control to LwM2M device resources, are implemented or supported on the server side [6, 9]. A mathematical model for information security risk assessment guides the selection of security measures, while a model for optimizing sensor placement informs system deployment to maximize coverage and minimize costs [11].

3.3. Collection and formalization of mathematical models of the solution

3.3.1. Mathematical model for information security risk assessment in LwM2M environmental monitoring systems

A mathematical model for assessing information security risks for LwM2M-based environmental monitoring systems is designed for the quantitative or qualitative evaluation of potential losses from the realization of information security threats and takes into account the cost of measures aimed at mitigating these risks. The model is based on the classical approach to risk assessment, which defines risk as a function of the probability of threat realization and the magnitude of potential impact. However, for the purposes of this work, the model is expanded by detailing the impact components and including the economic aspect – the cost of security measures.

The mathematical model is described by a set of components and equations that allow for the calculation of the risk level for the system or its individual components. The main components of the model are: the probability of threat realization, the impact of threat realization on confidentiality, integrity, and availability of data/system, and the cost of implementing and maintaining security measures.

The probability of threat realization (P_t) is determined for each identified threat t that is relevant to the LwM2M-based environmental monitoring system. This indicator reflects the frequency or likelihood that a specific threat will be successfully realized within a defined time period. The value of P_t can be determined based on statistical data, expert assessments, or analysis of system vulnerabilities and attacker activity. The probability takes values in the range from 0 to 1.

The impact of threat realization is assessed across three main aspects of information security: confidentiality ($I_{t,C}$), integrity ($I_{t,I}$), and availability ($I_{t,A}$). For each threat t, the degree of impact on each of these aspects is determined. Impact can be measured on quantitative (e.g., financial losses, downtime) or qualitative (e.g., low, medium, high) scales. For use in the mathematical model, qualitative assessments can be converted into numerical values, normalized to the range. For example, $I_{t,C}$, $I_{t,I}$, $I_{t,A}$ represent the normalized impact values of threat t on confidentiality, integrity, and availability, respectively.

The aggregate impact of threat t (I_t) can be calculated as a weighted sum of impacts on confidentiality, integrity, and availability. The equation used is:

$$I_t = w_C \cdot I_{t,C} + w_I \cdot I_{t,I} + w_A \cdot I_{t,A} \tag{1}$$

where w_C, w_I, w_A are weighting coefficients reflecting the relative importance of confidentiality, integrity, and availability for the specific environmental monitoring system. The sum of weighting coefficients usually equals 1 ($w_C + w_I + w_A = 1$). The values of the weighting coefficients are determined during the system security requirements analysis phase.

The risk associated with an individual threat t (Risk_t) is calculated as the product of the probability of realization of this threat and its aggregate impact. The formula for calculating the risk of an individual threat is:

$$\text{Risk}_t = P_t \cdot I_t = P_t \cdot (w_C \cdot I_{t,C} + w_I \cdot I_{t,I} + w_A \cdot I_{t,A}) \tag{2}$$

The total risk for the system (R) can be determined as the sum of risks of all identified relevant threats $t \in T$, where T is the set of all considered threats. The equation for calculating the total system risk is:

$$R = \sum_{t \in T} \text{Risk}_t = \sum_{t \in T} P_t \cdot (w_C \cdot I_{t,C} + w_I \cdot I_{t,I} + w_A \cdot I_{t,A}) \tag{3}$$

Table 1
Key Elements of the Structural Scheme for a Secure LwM2M Environmental Monitoring Solution

Structural Element / Process	Description & Purpose	Key Technologies / Implementations	Key Security Aspects / Features
1. Secure Sensor Devices	Collect environmental data; integrate hardware/software protection for end-to-end data security from the lowest level.	**Hardware:** ESP32 WROOM 32E (initial), MQ135, DHT22, PM2.5 sensors. (Alternatives: PIC32CM5164LS60064, NXP LPC55S3x for enhanced hardware security). **Communication:** Wi-Fi.	Hardware encryption accelerators (potential), secure boot (potential), CoAP/LwM2M over DTLS for secure data transmission channels.
	Software: Implement LwM2M client logic, data collection, formatting, and secure transmission.	LwM2M Client (wakaama or Zephyr OS), wolfSSL library.	Secure LwM2M profiles (PSK, RPK, certificates), DTLS/TLS for transport layer security, LwM2M object model for standardized data.
2. Secure LwM2M Server	Centralized device management, authentication, communication encryption, access control, and secure data storage.	Eclipse Leshan (open-source LwM2M server). **Deployment:** Standard server hardware or cloud. **Database:** PostgreSQL or MongoDB.	Supports all LwM2M operations, DTLS (with PSK, RPK, X.509 certificates), secure storage of collected data, centralized authentication and access control.
3. Security Monitoring & Management System	Intrusion detection, security event analysis, incident response capabilities, adaptive protection, continuous monitoring.	Separate module interacting with LwM2M server; Python development environment. Mathematical model for anomaly detection (statistical/ML), algorithm for LwM2M traffic anomaly detection.	Collection/analysis of security logs (server & devices), anomaly detection (environmental data & network traffic), incident notifications, implementation of adaptive protection methods. Continuous system status monitoring.
4. Secure Bootstrapping Process	Secure provisioning of credentials and configuration parameters to LwM2M devices.	LwM2M secure bootstrapping algorithms.	Mutual authentication and encryption during device provisioning.
5. Dynamic Access Control	Control access to LwM2M device resources dynamically.	Server-side LwM2M mechanisms, potentially ABAC.	Granular and policy-based access control to device resources.
6. Supporting Methodologies (Design/Planning)			
Information Security Risk Assessment	Justify the choice of specific security measures by considering threat probability and impact.	Mathematical model for risk assessment.	Informed decision-making for security measure selection during design.
Sensor Device Placement Optimization	Plan system deployment to maximize coverage and minimize costs.	Mathematical model for optimizing sensor placement.	Efficient and effective physical deployment of sensor network (planning stage).
Overall Security Concept	Comprehensive approach: built-in protocol security, cryptography, best practices, integration, adaptive protection, compliance.	Integrated across all levels of the system.	Ensures secure infrastructure for environmental monitoring systems using LwM2M.

This indicator R represents an integral assessment of the system's information security level before the implementation of additional security measures (initial risk).

The cost of implementing and maintaining security measures (C_m) is an important component of the model, used to evaluate the effectiveness and economic feasibility of various risk mitigation strategies. For each security measure m, its cost is determined, which may include expenses for purchasing equipment/software, installation, configuration, personnel training, as well as ongoing costs for maintenance and support over a certain period. The cost C_m is measured in financial units.

The implementation of a security measure m or a set of measures M (where M is a subset of the set of all possible measures S) leads to a change in the probabilities of threat realization and/or their impact. The probability of threat t realization after implementing measures M is denoted as $P_t^{(M)}$, and the impact as $I_{t,C}^{(M)}$, $I_{t,I}^{(M)}$, $I_{t,A}^{(M)}$. Typically, it is expected that $P_t^{(M)} \leq P_t$ and $I_{t,CIA}^{(M)} \leq I_{t,CIA}$.

The residual risk for the system after implementing a set of measures M ($R^{(M)}$) is calculated similarly to the total risk, but using probability and impact indicators that account for the effect of these measures:

$$R^{(M)} = \sum_{t \in T} P_t^{(M)} \cdot (w_C \cdot I_{t,C}^{(M)} + w_I \cdot I_{t,I}^{(M)} + w_A \cdot I_{t,A}^{(M)}) \tag{4}$$

The total cost of implementing and supporting a set of measures M ($C(M)$) is the sum of the costs of individual measures in this set:

$$C(M) = \sum_{m \in M} C_m \tag{5}$$

The mathematical model allows for evaluating different security provision scenarios by comparing the initial risk ($R^{(0)}$), residual risk ($R^{(M)}$) after implementing various sets of measures M, and the corresponding cost $C(M)$. The effectiveness of measures can be assessed by analyzing the risk reduction ($\Delta R^{(M)} = R^{(0)} - R^{(M)}$) relative to the costs $C(M)$. This allows for determining the most economically effective risk mitigation strategies for LwM2M-based environmental monitoring systems.

3.3.2. Mathematical model for optimal placement of environmental monitoring sensor devices

Applying this model to LwM2M-based environmental monitoring systems requires specification of threats characteristic of IoT devices and the LwM2M protocol (e.g., unauthorized access to sensor data, data spoofing, DDoS attacks on the management server, device compromise), assessment of their realization probabilities under system operation conditions, determination of the impact of these threats on monitoring data and system functioning, and calculation of the cost of specific security measures (e.g., implementation of LwM2M authentication and authorization mechanisms, data encryption, network segmentation, security monitoring).

The formulation of the sensor placement optimization problem involves defining a set of potential locations for installing devices within the territory subject to monitoring. Each potential location is associated with certain characteristics, such as installation cost, availability of power sources, or specifics of wireless signal propagation. The monitoring territory can be discretized into a set of target points or areas for which coverage and data collection with the required accuracy must be ensured. Sensor devices that can be used in the system include various types of sensors for measuring environmental parameters, such as air quality, pollution levels, temperature, and humidity [10], as well as sensors for monitoring the condition of equipment affecting the environment [6, 11].

The mathematical model can be formulated as an integer linear programming problem or its extension. Let I be the set of potential placement locations and J be the set of target monitoring points. Binary decision variables $x_i \in \{0, 1\}$ are defined for each potential location $i \in I$, where $x_i = 1$ if a sensor device is installed at location i, and $x_i = 0$ otherwise.

The objective function of the model is multi-objective, aimed at maximizing coverage and minimizing costs. This can be realized by minimizing costs subject to achieving a required level of coverage, or maximizing coverage within a given budget and technical constraints. Let us consider the option of

minimizing total deployment and operation costs. The costs associated with location i are denoted as c_i. The total costs are defined as $\sum_{i \in I} c_i x_i$.

The model constraints include:

1. Constraints on territory coverage and measurement accuracy: Each sensor placed at location i can provide coverage for a certain subset of target points $J_i \subseteq J$. Coverage of point $j \in J$ is considered ensured if at least one deployed sensor can cover it. A binary parameter $a_{ij} \in \{0, 1\}$ is introduced, where $a_{ij} = 1$ if a sensor at location i can cover point j with the required accuracy, and $a_{ij} = 0$ otherwise. Measurement accuracy depends on the sensor type, distance to the monitoring object, and signal propagation conditions [11]. The constraint may require that each target point $j \in J$ is covered: $\sum_{i \in I} a_{ij} x_i \geq 1$ for all $j \in J$. Alternatively, achieving a certain minimum percentage or area of covered territory may be required.
2. Constraints on energy consumption: Sensor devices operate on limited energy sources, especially in remote or wireless deployments [12]. The energy consumption of a sensor at location i over a certain period is denoted as e_i. This consumption depends on the sensor's operating mode, frequency of measurements, and data transmission. The total energy consumption of all deployed sensors must not exceed the total available energy budget of the system E_{max}: $\sum_{i \in I} e_i x_i \leq E_{\text{max}}$.
3. Constraints on network bandwidth: Data collected by sensors are transmitted through a communication network, which may have limited bandwidth [11]. In a system using the LwM2M protocol, sensors can connect to gateways or base stations that aggregate data before transmitting it to a central platform [12]. Let K be the set of gateways, and b_i be the average bandwidth required for data transmission from a sensor at location i. If sensor i connects to gateway k, this can be represented by a binary variable $y_{ik} \in \{0, 1\}$. Then, the total bandwidth arriving at gateway k must not exceed its maximum capacity $B_{\text{cap},k}$: $\sum_{i \in I} b_i y_{ik} \leq B_{\text{cap},k}$ for all $k \in K$. It must also be ensured that if a sensor is deployed, it connects to one gateway: $\sum_{k \in K} y_{ik} = x_i$ for all $i \in I$.

Thus, the mathematical model can be formulated as: Minimize $\sum_{i \in I} c_i x_i$ Subject to:

$$\sum_{i \in I} a_{ij} x_i \geq 1 \quad \forall j \in J \tag{6}$$

$$\sum_{i \in I} e_i x_i \leq E_{\text{max}} \tag{7}$$

$$\sum_{i \in I} b_i y_{ik} \leq B_{\text{cap},k} \quad \forall k \in K \tag{8}$$

$$\sum_{k \in K} y_{ik} = x_i \quad \forall i \in I \tag{9}$$

$$x_i \in \{0, 1\} \quad \forall i \in I \tag{10}$$

$$y_{ik} \in \{0, 1\} \quad \forall i \in I, k \in K \tag{11}$$

This model allows for determining the optimal set of locations for placing sensor devices, considering the given constraints and objectives. The result of solving the model is the determination of the set of locations i for which $x_i = 1$. Such optimized placement forms the basis for further deployment of the physical layer of the environmental monitoring system, where devices managed by the LwM2M protocol will collect and transmit data, ensuring effective monitoring and analysis of the environmental state [10, 11]. The application of LwM2M for managing these devices allows for remote configuration, status monitoring, and data collection, which is important for operating a distributed sensor network [6]. The developed model contributes to creating a more efficient, reliable, and resource-saving infrastructure for environmental monitoring.

3.3.3. Mathematical model for anomaly detection in environmental monitoring data

Effective functioning of environmental monitoring systems necessitates not only reliable data transmission but also the ability to promptly detect atypical situations arising from natural events, man-made

incidents, or malicious actions like cyberattacks on sensor infrastructure. In the context of intelligent monitoring systems, as highlighted by [4], modern data analysis methods are crucial. To identify atypical environmental parameter values, a mathematical model for anomaly detection in environmental monitoring data is being developed, utilizing statistical methods, machine learning, or a combination thereof. This model analyzes multidimensional time series data from various sensors (e.g., temperature, humidity, air pollution) to automatically detect deviations from the "normal" data behavior, signaling potential problems. The input data, $\mathbf{X}_t = (p_{1,t}, p_{2,t}, \ldots, p_{N,t})$, represents the measurements of N different environmental parameters at time t, collected from the physical layer of the monitoring system [12]. The core idea is to define a "normal" behavioral profile based on historical data and identify observations that significantly deviate from it.

The mathematical model can employ statistical methods, machine learning, or a combination. Statistical methods often assume specific data distributions. A simple approach involves analyzing each parameter separately, where an anomaly is detected if the current value $p_{i,t}$ deviates from the mean μ_i by more than a certain multiple of the standard deviation σ_i, i.e., $|p_{i,t} - \mu_i| > k \cdot \sigma_i$. More complex statistical methods, such as multivariate analysis, can use the Mahalanobis distance $D_M(\mathbf{X}_t)$ to measure the deviation of an observation vector $\mathbf{X}_t$ from the mean vector $\boldsymbol{\mu}$ of the "normal" data's multivariate distribution, considering their covariance matrix $\boldsymbol{\Sigma}$. The formula is $D_M(\mathbf{X}_t) = \sqrt{(\mathbf{X}_t - \boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1} (\mathbf{X}_t - \boldsymbol{\mu})}$. A high $D_M(\mathbf{X}_t)$ value indicates a low probability within the "normal" distribution, signaling an anomaly.

Machine learning methods offer more flexible anomaly detection, particularly for complex or unknown data distributions. Given the rarity of anomalies and potential lack of labeled data, unsupervised learning methods are commonly applied. These include clustering, where anomalies appear as isolated points or small clusters, and density estimation methods like Local Outlier Factor (LOF). Another effective approach is using data reconstruction methods such as Autoencoders, trained on "normal" data to compress and reconstruct representations. A significantly larger reconstruction error for anomalous data indicates abnormality, with detection occurring if this error exceeds a threshold. If sufficient labeled anomaly examples are available, supervised learning methods, like classification algorithms (e.g., Support Vector Machines, neural networks), can be used to distinguish "normal" from "anomalous" states. Combined approaches can leverage the strengths of both statistical and machine learning methods, for instance, by using statistical indicators as features for machine learning models or confirming machine learning detections with statistical tests.

When developing anomaly detection models for environmental monitoring data, it is crucial to consider the specifics of time series, including temporal dependencies, seasonality, and trends, ensuring the model adapts or accounts for these changes. The correlation between different measured parameters also highlights the importance of multivariate analysis. Additionally, the model must address data quality issues such as missing values, noise, or sensor drift, which can mimic or mask anomalies. The model's output typically identifies time points or periods of anomalous parameter values, providing a binary flag, an anomaly score, or indicating contributing parameters. This detection serves as a signal for further analysis and interpretation, as atypical values could be caused by environmental events, equipment malfunctions, or cyberattacks aimed at data falsification, often requiring additional information and expert analysis to distinguish between these scenarios.

3.4. Synthesis of methods and algorithms of the solution

3.4.1. Algorithm for secure bootstrapping of an LwM2M device

For constructing secure infrastructures for environmental monitoring systems, where the collection and transmission of sensitive data from numerous devices are critically important, ensuring security at all stages of the device lifecycle assumes paramount significance. A fundamental stage is the LwM2M device bootstrapping process, which establishes trust and configures parameters for a secure connection with the management server. This process is designed to prevent unauthorized access and compromise of configuration data, ensuring foundational security for sensitive environmental data. The LwM2M device bootstrapping process provides devices with essential configuration information, enabling a

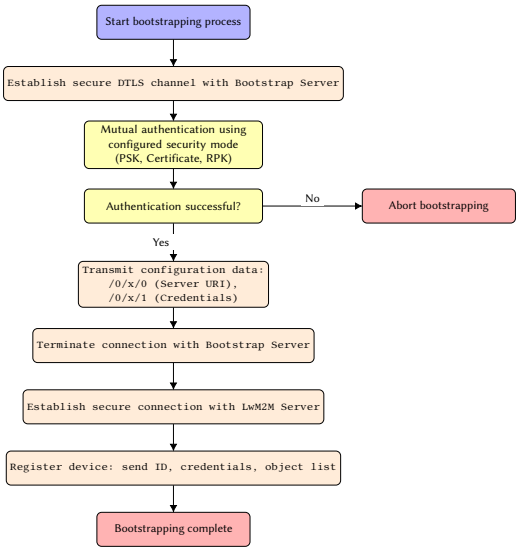

Figure 2: Flowchart of the secure LwM2M device bootstrapping algorithm.

secure connection to an LwM2M Server [9]. Instead of connecting directly to the main LwM2M Server, the device initially communicates with a specialized Bootstrap Server [12]. This dedicated server provides initial configuration parameters and security credentials, typically including the address of the subsequent LwM2M Server and the necessary security credentials for establishing a secure connection with it [9].

To ensure security during this bootstrapping phase, methods of mutual authentication and encryption are employed [4, 6]. Mutual authentication verifies the legitimacy of both the device and the Bootstrap Server before any confidential information exchange. The LwM2M standard supports various security modes, including Pre-Shared Key (PSK) mode, which uses a pre-distributed secret key for symmetric encryption and authentication, and Certificate mode, which relies on asymmetric cryptography with public keys and X.509 certificates for authentication and encryption [9]. Support for Raw Public Key and Public Key Infrastructure (PKI) deployment is also available [12]. The bootstrapping procedure typically begins with the device establishing a secure communication channel, often using the DTLS (Datagram Transport Layer Security) protocol, with its known Bootstrap Server [12]. DTLS ensures data confidentiality and integrity at the transport layer, protecting transmitted configuration. Within this secure channel, mutual authentication occurs using the chosen security mode. Upon successful authentication, the Bootstrap Server transmits critical configuration parameters, such as the LwM2M Server URI and associated security credentials [9]. The LwM2M Server can later initiate new bootstrap requests to update device credentials or server addresses, enabling dynamic security management throughout the device's lifecycle [9]. After bootstrapping, the device disconnects from the Bootstrap Server and uses the obtained credentials to establish a secure connection with the main LwM2M Server, preceding its registration process [9].

3.4.2. Algorithm for dynamic access control to LwM2M device resources

In research on securing environmental monitoring systems (EMS) using the LwM2M protocol, access control mechanisms are paramount. While LwM2M offers basic access control, its flexibility can be limited for complex EMS scenarios where access rights may depend on context beyond simple user or device identification, such as user role, system state, time, or data from other sensors [6, 10]. To address this, a dynamic access control algorithm for LwM2M device resources has been developed, founded on ABAC principles. This allows for defining access rights based on attributes of the subject, object, action, and environment, offering a higher degree of granularity and dynamism than traditional models like Role-Based Access Control (RBAC). The algorithm's functioning involves several key stages,

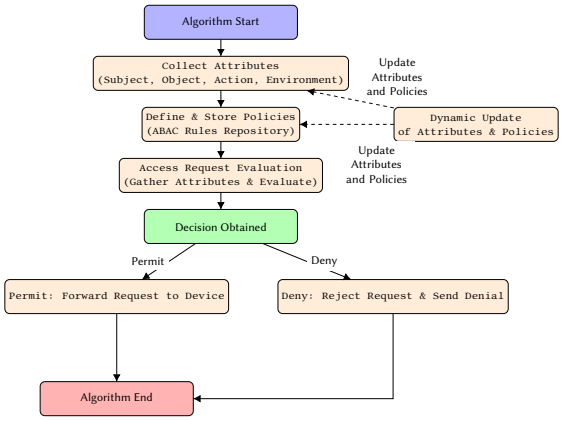

Figure 3: Flowchart of the ABAC algorithm for LwM2M device resources.

starting with attribute collection. For an LwM2M EMS, subject attributes might include roles (e.g., "system administrator"), object attributes relate to the LwM2M resource (e.g., "temperature" type, sensor location), and action attributes correspond to LwM2M operations like Read or Write [8].

Environment attributes encompass contextual factors such as time, device state (e.g., "normal operation"), or data from other monitoring devices [10]. The second stage involves defining and storing access policies as rules linking these attributes to permissions or denials. For instance, a policy might permit "monitoring engineers" to "Read" "temperature" data during "normal operation" within "working hours." These policies are centrally stored, typically on the LwM2M server or a dedicated security management component. The third stage is access request evaluation. When a subject requests an action on an LwM2M resource, the access control system intercepts it. It collects all relevant attributes (subject, object, action, and environment) and passes them to a policy evaluation engine. This engine analyzes defined access policies against the collected attributes to yield a "Permit" or "Deny" decision. The fourth stage is decision enforcement: if "Permit," the requested action is executed on the LwM2M device; if "Deny," the request is rejected, and the subject receives an access denial message. A crucial aspect of this algorithm is its support for dynamism. Since environment attributes, device states, or user roles can change, the algorithm includes mechanisms for updating attribute information. This allows the access control system to react promptly to context changes; for example, if an EMS device enters maintenance mode, the system can automatically restrict access to certain resources for all users except maintenance personnel. Implementing this algorithm within an LwM2M EMS infrastructure requires integrating attribute collection components, a policy store, a policy evaluation engine, and a policy enforcement point, usually located on the LwM2M server, with communications between components secured by LwM2M's authentication and encryption mechanisms [6].

3.4.3. Algorithm for anomaly detection in LwM2M traffic based on network interaction characteristics

Ensuring security and operational reliability is paramount in rapidly developing IoT applications like environmental monitoring systems, where sensitive data collection and transmission from numerous devices are critical. The LwM2M protocol standardizes IoT device management, but LwM2M-based systems remain vulnerable to cyberattacks and malfunctions that can distort data or cause system failure [6, 17]. To effectively counter these threats, timely detection of atypical behavior is crucial. This work focuses on an algorithm for detecting anomalies in LwM2M traffic, which analyzes network interaction characteristics and employs machine learning methods. The LwM2M protocol, based on an Object/Instance/Resource (O/I/R) model, facilitates device interaction via operations like Read, Write, and Execute, primarily using UDP with a DTLS security layer [6]. Anomaly detection in LwM2M traffic involves collecting and processing data reflecting network interaction specifics, particularly packet size, request frequency, and operation types. These parameters can be obtained through passive network

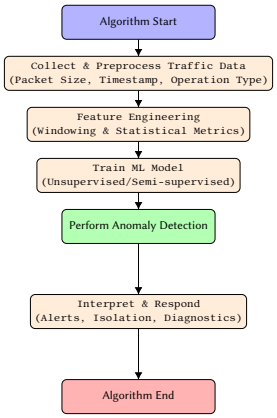

Figure 4: Flowchart of the machine learning-based algorithm for LwM2M traffic anomaly detection.

monitoring or by collecting metrics directly from the LwM2M server [9]. Atypically large or small packet sizes can signal anomalies like data exfiltration or malicious data formats. Deviations in request frequency, such as a sharp increase (DoS attempt) or unexpected cessation (malfunction/compromise), are strong indicators of anomalous behavior, as are changes in expected Observe notification frequencies [17]. Additionally, atypical sequences or ratios of operation types (e.g., excessive Write operations on usually read-only resources) can suggest unauthorized access attempts or manipulation, even with LwM2M's built-in access control [6, 8, 9].

The algorithm utilizes machine learning to analyze these traffic characteristics, identifying deviations from normal behavior through several stages. First, LwM2M network traffic data is collected and preprocessed, extracting relevant characteristics like packet size, timestamps, and LwM2M operation types [17]. Second, feature engineering aggregates raw traffic data over specific time windows, calculating statistical indicators such as average packet size, total packets, and frequency/distribution of each operation type to form a multidimensional feature vector [9]. Third, a machine learning model is trained, typically using unsupervised or semi-supervised learning methods (e.g., Isolation Forest, One-Class SVM, Autoencoders) on normal traffic data to learn patterns and define boundaries between typical and atypical behavior. Finally, direct anomaly detection occurs as new, real-time feature vectors are fed into the trained model, which calculates an "anomaly score" or classifies the behavior as "normal" or "anomalous." A high anomaly score or "anomalous" classification signals a potentially dangerous situation or failure. Anomalous traffic patterns are then compared against known attack scenarios (e.g., DDoS, scanning, unauthorized access) or failure types (e.g., sensor malfunction, software error). Upon detection, appropriate response measures are initiated, which may include generating alerts, automatically blocking/isolating compromised devices, enhancing monitoring, or initiating device diagnostic procedures, leveraging LwM2M's capabilities for monitoring and diagnostics [6, 17].

3.5. Synopsis of conceptual and methodological developments

It was established that the implementation of this concept requires a comprehensive approach, encompassing security provision at every level of the system – from sensor devices to the server infrastructure. This entails the use of adaptive protection methods that consider the limited resources of devices and the dynamic nature of threats, as well as ensuring the system's compliance with the requirements of regulatory documents and industry standards in information security.

To implement the formulated concept, key structural elements were identified, including secure sensor devices with LwM2M support, a secure LwM2M server, and a security monitoring and management system. A software-hardware configuration that can be used to build these elements was described, including the selection of microcontrollers, sensors, LwM2M client and server implementations, as well as the integration of libraries for cryptographic protection and the development of modules for security analysis. Justification for the choice of specific technologies and components was provided, considering

security requirements and resource constraints of IoT devices.

For the purpose of formalizing key security aspects and optimizing system functionality, a series of mathematical models were developed. A mathematical model for information security risk assessment was presented, enabling quantitative evaluation of potential threats considering their probability of realization, impact on data confidentiality, integrity, and availability, as well as the cost of security measures. This model serves as a tool for substantiating and prioritizing protection measures. A mathematical model for optimizing sensor device placement was considered, which, although not directly a security model, accounts for constraints on energy consumption and network bandwidth, indirectly affecting system availability and resilience. A mathematical model for detecting anomalies in environmental monitoring data was developed, utilizing statistical methods and machine learning techniques to identify atypical parameter values that may indicate either environmental events or cyberattacks.

Based on the developed models and structural elements, algorithms ensuring the implementation of key security functions were presented. An algorithm for secure bootstrapping of LwM2M devices was described, guaranteeing protected provisioning of credentials and configuration parameters using mutual authentication and encryption. An algorithm for dynamic access control to LwM2M device resources was developed, based on ABAC principles, providing flexible and granular management of access rights depending on context. An algorithm for detecting anomalies in LwM2M traffic was presented, which analyzes network interaction characteristics (packet size, request frequency, operation types) using machine learning methods to identify atypical behavior that may indicate cyberattacks or malfunctions.

4. Technical aspects of implementing the concept proposed in the work

4.1. Synthesis of a list of potential user interaction capabilities with the solution

The solution for a secure LwM2M-based environmental monitoring system provides users with functional capabilities through its software components, primarily the LwM2M server and the security monitoring and management system. This enables effective use of environmental data, device management, and overall system security. Users can view current sensor readings in near real-time, leveraging LwM2M's Read and Observe operations [17]. Sensor devices, acting as LwM2M clients, collect environmental parameters, represented as resources within LwM2M objects [11, 17]. The LwM2M server establishes secure connections via DTLS/TLS and sends Read requests or initiates Observe sessions to receive updates, with end-to-end communication encryption and access control ensuring security [6, 9, 17]. Beyond current data, users can access historical monitoring data stored securely in a database [12]. The security monitoring and management system provides access to this archival data, allowing users to query information for specific periods, devices, or sensor types, enabling analysis of environmental parameter dynamics and trend identification. The reliability of this historical data is maintained through cryptographic protection and data integrity mechanisms applied during collection, transmission, and storage [12]. Furthermore, the system allows for changing device configuration parameters via LwM2M's Write operations, including adjusting measurement periods, trigger thresholds, operating modes, or firmware updates [1, 6, 16, 17]. All such operations are subject to rigorous access control, potentially using a dynamic access control algorithm that considers user, device, and contextual attributes, with DTLS/TLS encryption securing command transmission [6].

An important function is managing user access rights, crucial for protecting sensitive environmental data and infrastructure from unauthorized interference. Users with administrative privileges can define access permissions for other users or groups to specific system functions, device data, or configuration changes. This is implemented using granular access control models like ABAC, with policies stored and enforced on the LwM2M server and security management system [9]. The security monitoring and management system also enables users to view and analyze security event logs, which record

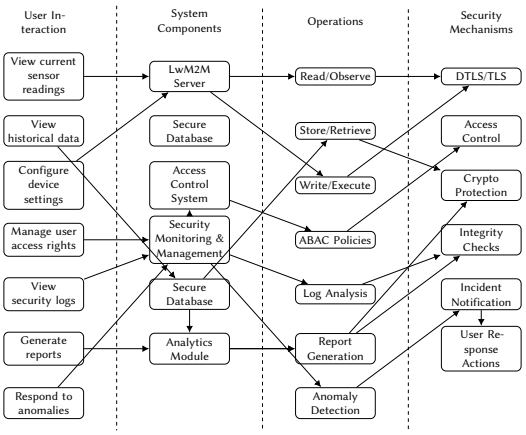

Figure 5: Mapping of potential user interaction capabilities to system components, operations, and security mechanisms within the LwM2M environmental monitoring solution.

device connection attempts, authentication results, operations performed, communication errors, and events detected by the anomaly detection system [10, 11]. The integrated algorithm for detecting anomalies in LwM2M traffic enhances this process by identifying atypical network behavior that simple log review might miss [11]. Finally, the system provides capabilities for generating reports on the monitoring system's state, encompassing data statistics, device operability, detected anomalies, and security incidents [10, 11]. This provides summarized information vital for managerial decisions and regulatory compliance. Crucially, the system supports responding to detected anomalies and security incidents, utilizing mathematical models for anomaly detection in data and traffic [11]. Upon detecting an anomaly (e.g., failed authentication, atypical traffic, sharp sensor deviation), the system can automatically notify the user [13]. Users can then initiate response actions through the interface, such as remote device diagnostics, configuration changes, temporary device blocking, or launching predefined cyber incident response procedures, including automatically adjusting measurement periods when pollutant standards are exceeded [10, 13].

4.2. Development of a class diagram for the solution

The proposed solution for a secure LwM2M-based environmental monitoring system is built upon a layered architecture of interconnected software classes, each dedicated to a specific functional or security aspect. This design ensures comprehensive data protection and efficient device management. A central component on the end-device side is the LwM2MClient class, which handles the LwM2M client functionality directly on the sensor device. Its responsibilities include device registration, collecting and transmitting environmental data according to the LwM2M object model, and executing commands received from the LwM2M server, while also monitoring device resource status. Conversely, the LwM2MServer class represents the central management and data collection node. It manages connected devices, including their registration, bootstrapping, and de-registration processes. This class is responsible for processing requests from LwM2M clients (e.g., read, write, execute, observe) and securely storing collected environmental monitoring data. Crucially, the LwM2MServer class plays a vital role in security by controlling client authentication and authorization, ensuring the secure interaction between devices and the central platform. Overall system security management is handled by the SecurityManager class, which coordinates and implements security mechanisms at a system-wide level. Its functions include managing encryption keys, configuring authentication and authorization policies, monitoring security events, and coordinating responses to cyberattacks. The SecurityManager interacts with other system components, especially the LwM2MServer, to enforce defined security policies. For complex access control, the AccessControlPolicyManager class implements dynamic access control based on ABAC principles. This allows for granular access rights defined by contextual attributes like user role, resource type, and time, with the AccessControlPolicyManager evaluating

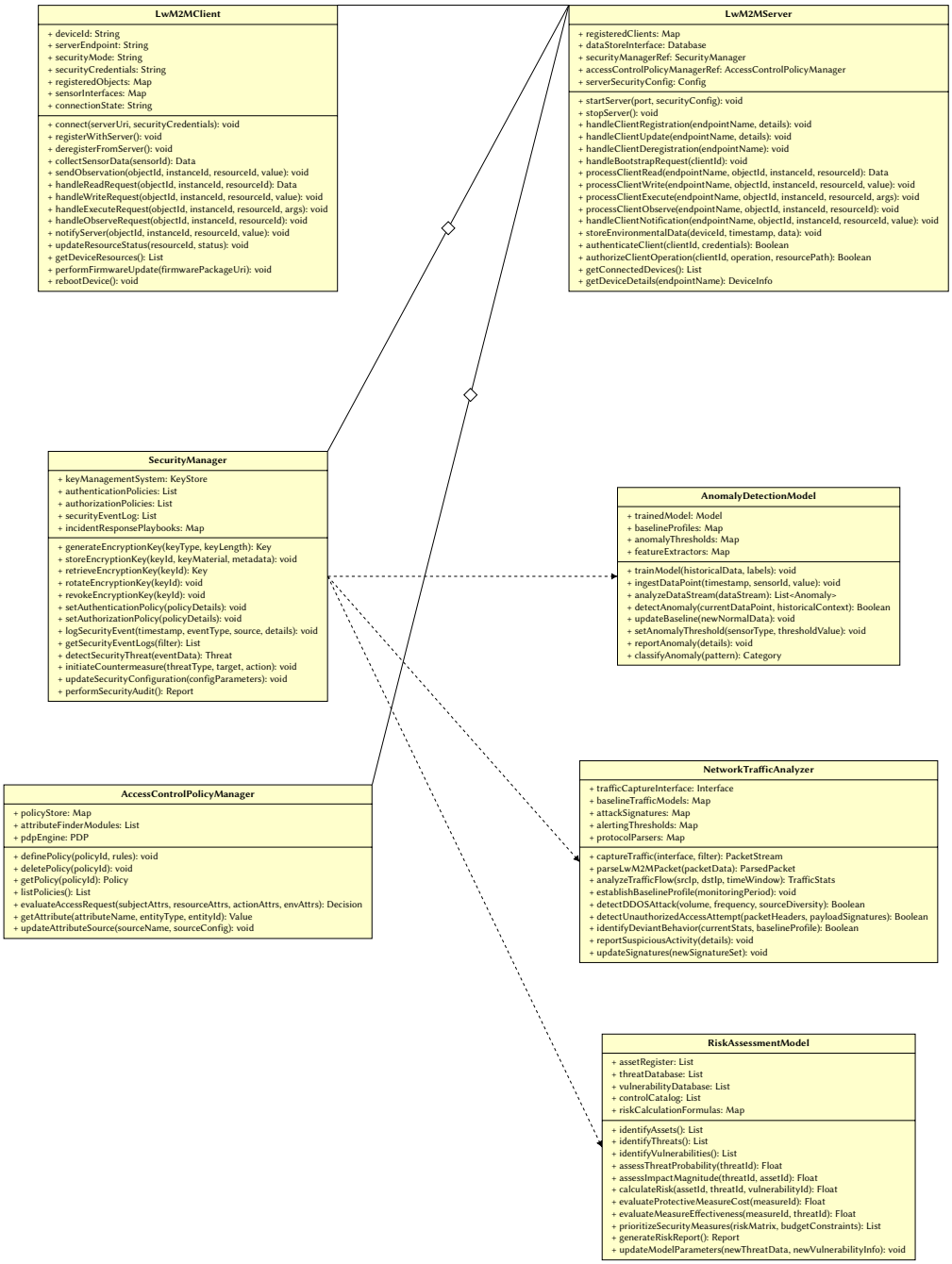

Figure 6: Class diagram illustrating the software architecture for the secure LwM2M environmental monitoring solution.

requests and enforcing decisions through, for example, the LwM2MServer. For analytical processing and problem detection, the architecture includes classes implementing mathematical models. The RiskAssessmentModel class quantifies potential information security threats, considering probability, impact, and protection costs, aiding in prioritizing security measures. The AnomalyDetectionModel class analyzes sensor data using statistical and machine learning methods to identify deviations from normal environmental behavior, which could indicate real events or cyberattacks. Complementing this, the NetworkTrafficAnalyzer class monitors LwM2M network traffic for anomalies in characteristics like packet size and request frequency, detecting potential unauthorized access or DDoS attacks. Together, these classes form a cohesive and secure infrastructure for effective environmental monitoring, with secure client-server interactions and integrated analytical and security management functions.

5. Plans for further work and practical implementation

Subsequent research endeavors will concentrate on the extensive validation and empirical testing of the developed conceptual framework and its constituent elements. A pivotal direction for further work involves the practical implementation of the proposed structural scheme and the software architecture articulated through the detailed class diagram, transitioning from theoretical constructs to operational prototypes. The mathematical models for risk assessment, sensor placement optimization, and anomaly detection necessitate refinement through application to real-world environmental monitoring data. Building upon advancements in forecasting information systems for environmental monitoring [19] and information-analytical systems for processing air pollution data [20], future efforts will aim to integrate these analytical capabilities to enhance the predictive accuracy and utility of our security models. The practical efficacy of the developed algorithms will be rigorously tested, drawing from experiences in developing systems for municipal-level air quality data collection, such as those involving Vaisala stations [21], and for intellectual analysis within industrial enterprises [22].

Significant attention will be directed towards addressing unresolved challenges, including the optimization of sensor network deployment and the secure integration with heterogeneous existing monitoring systems and databases, such as those developed for storing atmospheric air quality indicators for utility companies [23]. Future work will also explore secure pathways for incorporating data from corporate IoT networks used in environmental research [24, 25]. The development of secure and reliable automated reporting mechanisms, for instance, on the exceedance of established atmospheric air marker standards [26], will be pursued within the secure LwM2M framework.

Future investigations must also thoroughly evaluate the performance characteristics of the implemented security mechanisms, particularly under conditions of constrained device resources and varying network loads. The adaptation and extension of the proposed security solutions to other Internet of Things application domains exhibiting similar constraints and security requirements represent a valuable avenue for continued research. Further studies will focus on the scalability of the system, examining its capacity to accommodate an increasing number of devices and data streams without degradation in performance or security posture. The developed algorithms for secure bootstrapping, dynamic access control, and LwM2M traffic anomaly detection will undergo iterative refinement based on empirical data gathered from experimental setups and pilot deployments.

There is a recognized need for the development of intuitive user interfaces for the security monitoring and management system, facilitating effective interaction for operators and administrators. Comprehensive field trials of the complete integrated system are planned to assess its robustness, usability, and effectiveness in realistic environmental monitoring scenarios. Ongoing research will explore the integration of emerging security technologies, such as advanced cryptographic primitives and distributed ledger technologies for enhanced data integrity and auditability. Finally, a thorough investigation into the economic viability and cost-benefit analysis of implementing the comprehensive suite of security measures will be undertaken to provide practical guidance for deployment decisions.

6. Conclusions

The conducted research has culminated in the development of a comprehensive suite of technical solutions meticulously designed to ensure a secure infrastructure for environmental monitoring systems predicated on the LwM2M protocol. A significant achievement of this work is the formulation of an integrated security concept that addresses the multifaceted challenges inherent in protecting distributed IoT systems, from the sensor device level through to data management and analysis.

The analysis of the subject area unequivocally confirmed the critical relevance of robust security measures for environmental monitoring and underscored the specific vulnerabilities associated with LwM2M-based deployments, which the present work systematically addresses. The proposed structural scheme provides a coherent framework for organizing the necessary hardware and software components, thereby facilitating a structured approach to system design and implementation.

A core contribution of this research lies in the development and formalization of specific mathematical models tailored to the security requirements of LwM2M environmental monitoring systems. These include a quantitative model for information security risk assessment, a model for optimizing the physical placement of sensor devices considering operational constraints, and a sophisticated model for detecting anomalies within the collected environmental data streams using statistical and machine learning methodologies. Furthermore, a set of novel algorithms has been synthesized to address critical security functionalities: an algorithm for secure LwM2M device bootstrapping ensures the protected provisioning of credentials; an algorithm for dynamic, attribute-based access control enables fine-grained and context-aware authorization; and an algorithm for LwM2M traffic anomaly detection identifies suspicious network behavior indicative of potential cyberattacks or device malfunctions. These components collectively enhance data protection, ensure the reliability of monitoring operations, and support adaptive security management under conditions of limited device resources and dynamic threat landscapes. The detailed class diagram offers a concrete blueprint for the software realization of the proposed system, outlining the interrelationships and responsibilities of key software modules.

The investigation into potential user interaction capabilities further illustrates the practical utility and operational relevance of the developed solution. In essence, this work establishes a robust theoretical and methodological foundation for the engineering of secure, reliable, and efficient LwM2M-based environmental monitoring systems, contributing significantly to the advancement of secure IoT applications.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] A. Hammad, S. Abd, R. Ahmed, Detecting cyber threats in iot networks: A machine learning approach, International Journal of Computing and Digital Systems 17 (2024) 1–25. doi:10.12785/ijcds/1571020041.

[2] S. Raza, P. Misra, Z. He, T. Voigt, Lightweight m2m (lwm2m): A new kid on the block for iot device management and bootstrapping, IEEE Communications Standards Magazine 1 (2017) 42–47.

[3] M. A. Naeem, B. An, K. H. Kim, Security and privacy in lwm2m based iot systems: A survey and research challenges, Journal of Network and Computer Applications 168 (2020) 102745.

[4] R. Dvorak, L. Jabloncik, M. Mikulasek, M. Štůsek, P. Masek, R. Mozny, A. Ometov, P. Mlynek, P. Cika, J. Hosek, Lwm2m for cellular iot: Protocol implementation and performance evaluation, 2023, pp. 212–218. doi:10.1109/ICUMT61075.2023.10333286.

[5] S. Rao, D. Chendanda, C. Deshpande, V. Lakkundi, Implementing lwm2m in constrained iot devices, 2015. doi:10.1109/ICWISE.2015.7380353.

[6] S. Bakhare, D. S. W. Mohod, A review on real-time network traffic monitoring and anomaly detection system : A comprehensive study with user-friendly interface and historical analysis capabilities, International Journal of Scientific Research in Science, Engineering and Technology 11 (2024) 23–41. doi:10.32628/IJSRSET.

[7] C. Gilbert, M. Gilbert, Ai-driven threat detection in the internet of things (iot), exploring opportunities and vulnerabilities, International Journal of Research Publication and Reviews 5 (2024) 219–236. doi:10.2139/ssrn.5259702.

[8] A. Abidin, E. Marquet, J. Moeyersons, X. Limani, E. Pohle, M. Van Kenhove, J. M. Marquez-Barja, N. Slamnik-Krieštorac, B. Volckaert, Mozaik: An end-to-end secure data sharing platform, in: Data Economy (DE '23), ACM, 2023. URL: https://www.mdpi.com/2076-3417/15/2/499.

[9] M. Clark, L. Rajabion, A strategic approach to iot security by working towards a secure iot future, International Journal of Hyperconnectivity and the Internet of Things 7 (2023) 1–18. doi:10.4018/IJHIoT.317088.

[10] B. W. Kilgour, K. R. Munkittrick, C. B. Portt, T. J. Arciszewski, G. C. Sbeglia, An adaptive environmental effects monitoring framework for assessing the influences of liquid effluents on benthos, water, and sediments in aquatic receiving environments, Integrated Environmental Assessment and Management 14 (2018) 552–566.

[11] C. C. Uzondu, A. C. Lele, Challenges and strategies in securing smart environmental applications: A comprehensive review of cybersecurity measures, Computer Science IT Research Journal 5 (2024) 1695–1720. URL: https://www.fepbl.com/index.php/csitrj/article/download/1353/1585.

[12] S. Channivally, Blockchain in Internet of Things (IOT) Security, Ph.D. thesis, 2023. doi:10.13140/RG.2.2.18730.59841.

[13] A. Aluwala, Ai-driven anomaly detection in network monitoring techniques and tools, Journal of Artificial Intelligence Cloud Computing (2024) 1–6. doi:10.47363/JAICC/2024(3)310.

[14] T. Alam, Blockchain-based big data integrity service framework for iot devices data processing in smart cities, SSRN Electronic Journal 19 (2021). doi:10.2139/ssrn.3869042.

[15] S. Rao, D. Chendanda, C. Deshpande, V. Lakkundi, Implementing lwm2m in constrained iot devices, 2015. doi:10.1109/ICWISE.2015.7380353.

[16] U. Zafer, J. Pomeroy, Blockchain-powered iot security: Ensuring data integrity and device trustworthiness, 2025. doi:10.13140/RG.2.2.15756.22404.

[17] M. Al-Hawawreh, E. Al-Masri, A comprehensive analyses of intrusion detection system for iot environment, International Journal of Interactive Mobile Technologies (iJIM) 16 (2022) 4–20. This paper reviews IDS for IoT, covering detection, analysis, and response aspects.

[18] A. Cook, L. Maglaras, R. Smith, H. Janicke, Managing incident response in industrial internet of things, International Journal of Internet Technology and Secured Transactions 8 (2016). doi:10.1504/IJITST.2018.10014544.

[19] K. Vadurin, A. Perekrest, V. Bakharev, V. Shendryk, Y. Parfenenko, S. Shendryk, Towards digitalization for air pollution detection: Forecasting information system of the environmental monitoring, Sustainability 17 (2025). URL: https://www.mdpi.com/2071-1050/17/9/3760.

[20] A. Zavalieiev, K. Vadurin, A. Perekrest, V. Bakharev, Information and analytical system for collecting, processing and analyzing data on air pollution, Automation of technological and business processes 16 (2024) 72–82. doi:10.15673/atbp.v16i1.2774.

[21] K. O. Vadurin, A. L. Perekrest, V. S. Bakharev, A. I. Deriienko, A. V. Ivashchenko, S. A. Shkarupa, Information system for collecting and accumulating municipal-level atmospheric air quality data from vaisala stations, Infocommunication and Computer Technologies 2 (2024) 38–49. doi:10.36994/2788-5518-2023-02-06-04.

[22] A. Perekrest, D. Mamchur, A. Zavaleev, K. Vadurin, V. Malolitko, V. Bakharev, Web-based technology of intellectual analysis of environmental data of an industrial enterprise, in: 2023 IEEE 5th International Conference on Modern Electrical and Energy System (MEES), 2023, pp. 1–7. doi:10.1109/MEES61502.2023.10402523.

[23] A. Perekrest, V. Bakharev, K. Vadurin, A. Deriyenko, A. Ivashchenko, S. Shkarupa, Development of a database for storing atmospheric air quality indicators from the research stations of a utility company, Problems of informatization and management 3 (2023). URL: https://tech.sn-tnu.edu.ua/index.php/tech/article/view/18018. doi:10.18372/2073-4751.75.18018.

[24] A. Korostelov, M. Guchenko, A. Perekrest, A. Samoilov, K. Vadurin, Analytical calculations of the corporate network based on the internet of things technologies of the environmental research enterprise, «Scientific Notes of Taurida National V. I. Vernadsky University. Series: Technical Sciences» 34 (2023) 73. doi:10.32782/2663-5941/2023.5/23.

[25] A. Korostelov, M. Guchenko, A. Perekrest, A. Nikitina, K. Vadurin, Model of a corporate network based on internet of things technologies for an environmental research enterprise, Control, Navigation and Communication Systems 3 (2023) 111–114. doi:10.26906/SUNZ.2023.3.111.

[26] K. O. Vadurin, A. L. Perekrest, V. S. Bakharev, Development of a method of automatic reporting on the number of exceedances of the established standards of atmospheric air markers, INFOCOMMUNICATION AND COMPUTER TECHNOLOGIES 2 (2024) 50–59. URL: https://visn-icct.uu.edu.ua/index.php/icct/article/view/139. doi:10.36994/2788-5518-2023-02-06-05.