algorithms

IMPACT FACTOR 2.1

CITESCORE 4.5

Article

A Decision Tree Regression Algorithm for Real-Time Trust Evaluation of Battlefield IoT Devices

Ioana Matei and Victor-Valeriu Patriciu

Special Issue

Algorithms for Cyber Defense: From Cryptography to Behavioral Analysis

Edited by

Dr. Paul A. Gagniuc

MDPI

https://doi.org/10.3390/a18100641

algorithms

MDPI

Article

A Decision Tree Regression Algorithm for Real-Time Trust Evaluation of Battlefield IoT Devices

Ioana Matei * and Victor-Valeriu Patriciu

Faculty of Information Systems and Cyber Security, Military Technical Academy "Ferdinand I", 050141 Bucharest, Romania; victor.patriciu@mta.ro

* Correspondence: ioana.matei@mta.ro; Tel.: +40-741562099

Abstract

This paper presents a novel gateway-centric architecture for context-aware trust evaluation in Internet of Battle Things (IoBT) environments. The system is structured across multiple layers, from embedded sensing devices equipped with internal modules for signal filtering, anomaly detection, and encryption, to high-level data processing in a secure cloud infrastructure. At its core, the gateway evaluates the trustworthiness of sensor nodes by computing reputation scores based on behavioral and contextual metrics. This design offers operational advantages, including reduced latency, autonomous decision-making in the absence of central command, and real-time responses in mission-critical scenarios. Our system integrates supervised learning, specifically Decision Tree Regression (DTR), to estimate reputation scores using features such as transmission success rate, packet loss, latency, battery level, and peer feedback. The results demonstrate that the proposed approach ensures secure, resilient, and scalable trust management in distributed battlefield networks, enabling informed and reliable decision-making under harsh and dynamic conditions.

Keywords: trust; reputation; supervised learning; context-aware security

Academic Editor: Paul A. Gagniuc

Received: 10 September 2025
Revised: 1 October 2025
Accepted: 7 October 2025
Published: 10 October 2025

Citation: Matei, I.; Patriciu, V.-V. A Decision Tree Regression Algorithm for Real-Time Trust Evaluation of Battlefield IoT Devices. *Algorithms* **2025**, *18*, 641. https://doi.org/10.3390/a18100641

1. Introduction

The Internet of Things (IoT) has become a transformative force in many domains, and its integration into military operations, increasingly referred to as the IoBT, is reshaping the way missions are planned and executed. By enabling the real-time monitoring of soldiers' physiological conditions and environmental factors, IoBT systems promise to enhance situational awareness, support informed decision-making, and improve the overall safety and effectiveness of combat operations. However, these opportunities are matched by equally significant challenges. The hostile nature of battlefield environments exposes networks to malicious interference, unreliable communications, and extreme resource constraints, making trust and reliability central issues in the deployment of such systems.

A key problem lies in how the trustworthiness of devices and communication nodes can be reliably assessed under such adverse conditions. Traditional approaches often rely solely on behavioral indicators such as packet loss or forwarding rates, which, although useful, may not fully capture the complexity of IoBT environments. There is a need for mechanisms that account not only for node behavior but also for contextual factors that can influence performance. Addressing this problem requires both a theoretical understanding of how trust can be quantified in distributed, adversarial systems and practical models that support secure and timely decision-making.

This study develops a trust evaluation framework that responds to these requirements by combining reputation-based mechanisms with supervised learning techniques. Specifically, a DTR algorithm is used to estimate the reputation scores of battlefield devices based on behavioral and contextual indicators. By doing so, the research aims to demonstrate that machine learning-driven approaches can enhance the reliability and resilience of IoBT networks. The model is designed to function in real time, enabling commanders to make operational adjustments, prioritize evacuations, and maintain readiness based on accurate trust assessments of devices and communication channels.

The findings demonstrate that the proposed framework enhances the precision of trust evaluation, improves the robustness of battlefield networks against malicious or compromised nodes, and reduces the risk of misinterpretations caused by environmental or operational stressors. The contribution of this work is therefore twofold: it advances the design of trust management systems for IoBT environments. It illustrates the benefits of incorporating context-sensitive machine learning into military communication networks.

The remainder of this article is organized as follows. Section 2 reviews the most relevant related work on trust and reputation models in IoT and IoBT. Section 3 presents the proposed materials and methods, including the operational scenario and the reputation estimation algorithm. Section 4 reports the experimental results obtained through progressive evaluation of the models. Section 5 provides a discussion that links the results to the layered IoBT architecture, highlights the impact of optimization, and examines the integration of physiological data into the trust framework. Finally, Section 6 concludes the paper, summarizes the main contributions, and outlines avenues for future research.

2. Related Work

Ensuring trust and security within IoT has been the subject of extensive research, particularly in mission-critical domains such as defense, healthcare, and industry. Reputation-based trust models have been among the most prominent strategies to address vulnerabilities in distributed networks, as they offer effective mechanisms for detecting malicious nodes and preserving communication reliability under constrained conditions.

Prior work has explored behavioral trust mechanisms, where node reliability is inferred from forwarding behavior, packet loss, or transmission accuracy. For example, the trust-aware Routing Protocol for Low-Power and Lossy Networks (RPL) proposed in [1] was able to mitigate blackhole and selective forwarding attacks by maintaining dependable communication paths. Similarly, the mobile code-based trust model in [2] dynamically monitored forwarding behavior to isolate compromised nodes, highlighting the importance of behavioral indicators in trust computation across decentralized IoT systems.

Another research stream has explored trust-based Intrusion Detection Systems (IDS). In [3], a trust management IDS for low-power lossy networks demonstrated a 100% true positive rate in detecting routing attacks such as sinkhole and blackhole, reinforcing the potential of anomaly detection even in resource-constrained environments. Beyond deterministic evaluation, probabilistic trust approaches have been introduced. The Bayesian framework of [4] leveraged prior knowledge and behavioral updates to compute dynamic reputation scores, while RESFIT [5] combined reputation mechanisms with an application-layer firewall, optimizing computational load through gateway-centered oversight. These contributions underline the need for scalable and modular trust management systems.

Trust considerations have also expanded into domain-specific IoT applications. In healthcare, layered security frameworks [6] and real-time monitoring systems [7] have been proposed to protect sensitive data and ensure responsiveness. However, many of these solutions lack robust mechanisms for validating data sources or integrating automated trust assessment, leaving vulnerabilities unaddressed. Research in wireless sensor networks

(WSNs) has likewise emphasized the dual role of trust, as TEAHR [8] incorporated energy-aware hierarchical routing. At the same time, studies in [9,10] examined how adversaries exploit trust assumptions through Sybil, blackhole, and gray-hole attacks.

Recent surveys and proposals highlight a shift toward context-aware trust models. The extensive review in [11] classified trust approaches by metrics, architecture, and resilience, while [12] introduced a trust-aware routing protocol based on dynamically adapting Beta distributions. Similarly, the fog-based access control system in [13] demonstrated the value of incorporating contextual data for real-time decision-making.

In parallel, research on the IoBT emphasizes the specific challenges of military environments. A review of IoBT communication issues in [14] identified the need for resilient and adaptive networking, while the IoBT-OS framework in [15] aimed to optimize the sensing-to-decision cycle for tactical efficiency. Work in [16] further highlighted the multi-domain complexity of battlefield systems, stressing the importance of secure and integrated communication strategies.

Despite these advances, most existing approaches remain narrowly focused on behavioral trust indicators, often neglecting the physiological or contextual states of human operators. This omission is critical in IoBT environments, where factors such as stress, fatigue, or environmental pressure can influence system reliability and lead to unfair trust penalties. Addressing these gaps requires trust frameworks that integrate both behavioral and contextual data, enabling more resilient, fair, and adaptive trust evaluation for military operations. Despite these advances, most existing approaches remain narrowly focused on behavioral trust indicators, often neglecting the physiological or contextual states of human operators. This omission is critical in IoBT environments, where factors such as stress, fatigue, or environmental pressure can influence system reliability and lead to unfair trust penalties. Addressing these gaps requires trust frameworks that integrate both behavioral and contextual data, enabling more resilient, fair, and adaptive trust evaluation for military operations. In a previous study [17], we proposed a distributed communication framework for secure and efficient collaboration among multiple IoBT nodes, focusing on inter-node communication and trust propagation. Building on that foundation, the present work advances the state of the art by introducing a context-aware trust evaluation model that integrates both behavioral and physiological parameters into the reputation assessment process.

3. Materials and Methods

3.1. Proposed Scenario

In this study, we define a simulation-based battlefield scenario designed to evaluate the functionality and robustness of the proposed IoBT trust management system. The scenario reflects a realistic operational context in which military personnel are equipped with wearable sensing devices capable of continuous monitoring. We introduce a modular and layered design of an IoT device that incorporates sensing, processing, and communication functions. The node is designed to operate independently, collecting medical and environmental data, and preparing it for trust assessment within a multi-layer network infrastructure that includes trust management mechanisms. The node records various essential parameters, including military personnel's medical information and operational battlefield data. Continuous monitoring of vital signs, such as heart rate, blood pressure, and oxygen levels, is vital for safeguarding soldiers' health and facilitating swift medical interventions in cases of injury or fatigue. Moreover, the collection and analysis of tactical information, like environmental conditions and troop locations, support improved coordination and strategic decision-making. While the entire infrastructure plays a critical role in a trust management system, specific key components can significantly enhance the

reliability and performance of communication across the network. To better highlight these elements, the system will be analyzed at two distinct layers: the device level, which focuses on sensing, processing, and transmission; and the infrastructure level, which encompasses the broader trust and reputation mechanisms across the network.

The proposed IoBT device architecture is organized into multiple functional layers, each responsible for a distinct stage in the data acquisition, processing, and transmission pipeline. This modular design enables flexibility, fault isolation, and scalability, allowing the node to operate autonomously while contributing to the trust and reputation management processes at the network level. Figure 1 illustrates the high-level architecture of the node. At the base of the system lies the Multimodal Sensing Layer, which is responsible for collecting heterogeneous data from various physical sensors. This layer includes three major sensing domains, as follows:

- Physiological sensors, such as ECG, pulse oximeters, galvanic skin response sensors, and temperature probes, provide real-time insight into the soldier's health status.
- Environmental sensors, including temperature, humidity, barometric pressure, and gas/chemical detectors, help contextualize the physiological signals and assess external risk factors.
- Positioning and motion sensors, such as GPS modules, inertial measurement units (IMUs), and altimeters, offer situational awareness in terms of geolocation and movement dynamics.

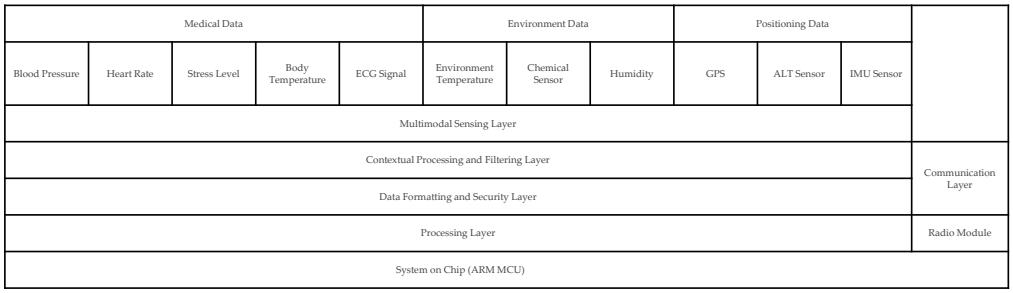

Figure 1. Modular IoBT device architecture showing sensing, processing, security, and communication layers for autonomous operation.

Data collected from the sensors is passed to the Contextual Processing Layer, which is tasked with filtering, normalization, and initial validation. This layer performs local computations to reduce raw signal noise and eliminate artifacts that could arise from harsh environmental or physiological conditions.

A lightweight anomaly detection mechanism is integrated within this layer, enabling the identification of sensor readings that deviate from expected patterns. These algorithms do not perform trust evaluation in the formal sense but rather ensure that data forwarded to the next stage is clean and internally consistent. Once processed, the data enters the Data Formatting and Security Layer, where it is structured, encapsulated, and secured for transmission. This layer adds essential metadata such as: Node identifier, Timestamp, Sensor source identifiers, Optional data quality flags, or anomaly markers.

Given the military nature of the communication context, the device-level architecture must include a layer for managing communication security. In order to ensure data confidentiality, integrity, and authenticity in contested environments, encryption schemes such as AES-128 and elliptic-curve cryptography (ECC) are recommended due to their efficiency and suitability for resource-constrained embedded systems. These methods are in alignment with established security standards, including NIST SP 800-38D for AES-GCM modes of operation and NIST SP 800-56A for elliptic curve key establishment. Incorporating such standards at the device level ensures interoperability, robustness, and compliance

with coalition force requirements. This pre-transmission formatting plays a critical role in maintaining data integrity across the trust chain of the IoBT network.

At the processor level, commands are executed by an ARM microcontroller (System on Chip). This microcontroller includes support for multiple communication protocols (e.g., BLE, Wi-Fi, LoRa) and is responsible for ensuring connectivity under variable radio conditions. The radio processing and transmission modules shown in Figure 1 manage communication with the gateway node or other devices in the network. Thus, to ensure operational efficiency and responsiveness in dynamic battlefield conditions, the communication layer must implement adaptive transmission mechanisms. The node is required to dynamically select the most suitable communication protocol and adjust transmission power based on contextual factors such as node proximity, environmental interference, and network congestion. Additionally, a priority queuing system should be integrated to manage data flow intelligently, ensuring that critical alerts or validated high-importance data are transmitted with higher precedence over routine monitoring packets. This approach enhances bandwidth utilization and ensures timely delivery of mission-critical information.

Building on the individual node architecture, the complete IoBT system integrates these nodes into a multi-layer network that enables secure, reliable, and context-aware communication across the battlefield. While each node performs local sensing and preliminary processing, the broader system coordinates data collection, trust evaluation, and decision-making at higher levels of the infrastructure.

The IoBT architecture, as described in Figure 2, is designed to ensure reliable, secure, and context-aware communication across heterogeneous nodes deployed in contested military environments. The system is structured in layers, from embedded sensing on the individual soldier to centralized processing at the command level. Each component plays a vital role in enabling data flow, facilitating reputation-based trust assessments, and providing mission-critical decision support. At the edge of the system, each soldier is equipped with a set of onboard embedded sensors that capture relevant data in real-time. These include physiological indicators (e.g., heart rate, temperature, ECG), environmental parameters (e.g., humidity, chemical exposure), and equipment status. Each sensor is interfaced with a local processing unit, responsible for preliminary processing, anomaly detection, and data encapsulation. Intra-sensor communication is achieved using low-power radio protocols, such as LoRa, ZigBee, or Bluetooth Low Energy (BLE), which are selected for their efficiency and reliability in short-range transmission under high-mobility conditions. Sensor data from individual soldiers is relayed to a nearby Device/Concentrator, a lightweight forwarding unit that collects and transmits the unaltered data upstream. Typically, the concentrator is co-located with the equipment of a commanding officer, functioning as a local gateway device. Communication from field devices to the gateway utilizes sub-1GHz transmission technologies, ensuring extended range and robustness in obstructed environments. At this level, real-time data visualization may be enabled for the commanding officer. In contrast, critical data (e.g., medical alerts) can be securely forwarded to designated personnel, such as medics or field support units. To maintain persistent connectivity in mobile and dispersed deployment scenarios, the architecture integrates Unmanned Aerial Vehicles (UAVs) as data relays. These airborne platforms facilitate multi-hop transmission between field-level nodes and higher infrastructure layers, effectively extending the communication range and providing redundancy in the event of ground-level disruption. UAVs act solely as transparent relay agents, enabling communication continuity without modifying or interpreting the transmitted data. Their mobility ensures line-of-sight links and dynamic adaptation to the tactical topology. The next critical stage in the data pipeline is Radio Gateway, which transforms the radio-based stream into IP-compatible data packets, enabling secure routing over existing tactical or satellite networks.

This gateway forms the transition point between constrained battlefield communication protocols and broader networked infrastructures.

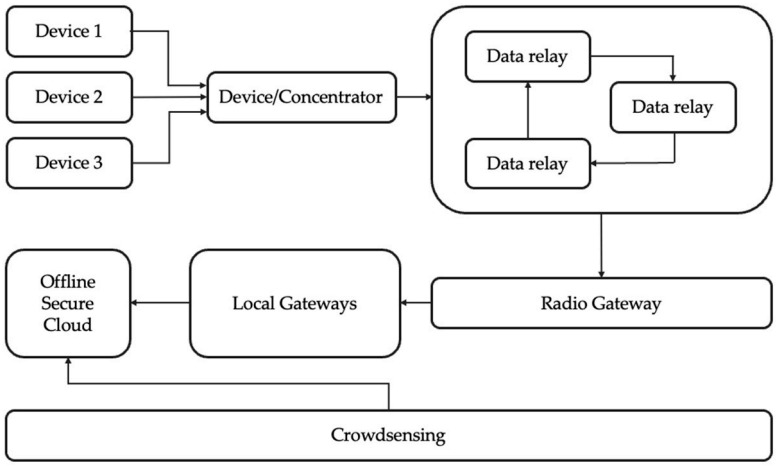

Figure 2. High-Level IoBT System Architecture Demonstrating Layered Trust Management and Secure Data Flow from Edge Devices to Command Infrastructure.

Once within the network domain, the data is forwarded to computational gateways, nodes with significantly higher processing power. These gateways serve as local trust engines, performing reputation scoring based on behavioral analysis, cross-sensor correlation, and anomaly tracking.

Gateways maintain a distributed trust ledger, periodically synchronized with central systems. The reputation values computed at this layer influence both data prioritization and network routing decisions, improving resilience against compromised or malfunctioning nodes.

At the top of the architecture resides the command-level infrastructure, which integrates high-performance computing capabilities and serves as the ultimate decision-making authority. Within this tier, all collected and relayed data is aggregated, processed at scale, and stored in a secure centralized database.

A key function of this level is to maintain and manage a historical ledger of node behavior and trust scores. Each node in the network is continuously evaluated based on its data consistency, communication reliability, and alignment with expected behavioral profiles. These trust scores are not only stored but also periodically updated using batch processing or upon specific events that indicate a significant change in behavior. The trust ledger enables system-wide data integrity verification, supports retrospective forensic analysis, and can guide dynamic policy enforcement, such as isolating untrusted nodes or prioritizing critical messages from high-trust sources. Furthermore, this layer ensures operational traceability, offering decision-makers a clear overview of network health and the reputational standing of all participating entities. In contrast to the core network, the main architecture enables opportunistic data integration through a crowdsensing layer, which aggregates information from auxiliary or external sources (e.g., civilian infrastructure or allied devices). While such data is initially untrusted, it can be filtered and fused with validated inputs to enhance contextual awareness under defined operational policies.

3.2. Reputation Estimation Algorithm

In the context of reputation-based security for IoT networks, the evaluation and classification of node behavior play a critical role. This section proposes the use of a supervised learning approach, specifically, DTR, to estimate the reputation score of each IoT node based on a series of behavioral and contextual indicators. The reputation score

is modeled as a continuous value that reflects the node's trustworthiness, allowing the system to make dynamic security decisions such as permitting, limiting, or blocking network access.

The features utilized for training the regression model consist of following metrics:

- transmission success rate (TSR): the proportion of successfully transmitted packets in the simulation. TSR indicates the reliability of the node in forwarding data;
- packet loss (PL): fraction of lost packets during simulation runs, identifying unreliable or faulty nodes;
- latency (L): time between data generation and reception, reflecting responsiveness under various simulated conditions;
- battery level (B): simulated remaining energy of the node, accounting for operational constraints;
- feedback from users or peers (FB): modeled evaluations from neighboring nodes or operators within the simulation, capturing behavioral context;
- reputation score (RS): the output of the regression model.

Through learning on labeled data, the DTR model can capture complex non-linear relationships among these variables and the resulting reputation score.

The choice of DTR is motivated by its high interpretability, low computational complexity, and robustness in handling heterogeneous data types (e.g., numerical, categorical). Unlike more complex algorithms such as neural networks or support vector machines, DTRs are well-suited for deployment on resource-constrained gateway devices, which are commonly found in IoBT environments. Furthermore, the model provides a clear understanding of the decision-making process and supports feature importance analysis, enabling system administrators to better understand the factors influencing trust within the network. Compared to traditional threshold-based or statistical models, the use of supervised machine learning allows for adaptive, data-driven reputation assessment that can evolve over time in a military environment. This capability is especially important in dynamic ecosystems, where nodes, such as soldiers, field equipment, and mobile gateways, operate under constantly changing conditions, including mobility, environmental variability, and network disruptions. Leveraging contextual data from heterogeneous sensors across the device, gateway, and cloud layers, the system can adjust trust scores in real time, enabling more accurate and resilient decision-making in mission-critical scenarios.

In our scenario, the gateway plays a central role in evaluating the trust level of nodes contributing sensor data across a distributed military IoT network. Performing reputation computation at the gateway level offers several operational advantages, particularly in mission-critical military scenarios. First, it significantly reduces latency, enabling trust-based decisions to be made locally and in real-time. This is crucial in tactical environments where delays can compromise mission outcomes. Additionally, local computation enhances system autonomy. Gateway nodes can continue to assess trustworthiness even if connectivity to the central command infrastructure is temporarily lost.

Another essential benefit is reduced exposure of sensitive data. By processing and aggregating information locally, the system minimizes the volume of raw physiological and behavioral data transmitted over the network, thereby enhancing data privacy and reducing communication overhead. These mobile devices operate in an ad hoc manner and do not establish a pre-existing trust relationship with the gateway. To determine the reliability of the data received, the gateway utilizes a DTR algorithm, as illustrated in Algorithm 1, which calculates a reputation score for each IoBT device. This diagram shows the proposed algorithm for evaluating the reputation of IoT nodes.

The process begins by collecting behavioral data for each node in the network, including successful transmissions, lost packets, feedback, battery level, and latency.

For each node, a feature vector is constructed and fed into the trained regression model. The model predicts a reputation score, and this score is compared to a predefined threshold.

If the reputation is below the threshold, the node is considered unsafe, and security rules (such as blocking or filtering traffic) are applied.

If the reputation is acceptable, the node is considered trustworthy and is allowed access to the network.

The model can be updated over time through online learning to adapt to behavioral changes in the nodes. This mechanism supports real-time decision-making in a secure and autonomous IoT architecture.

Each gateway maintains a local database containing the reputation scores of mobile devices that have submitted data. These scores are updated exclusively through the decision tree-based algorithm.

Algorithm 1. DTR-based algorithm for evaluating the reputation of IoBT devices

```
Data: Current observation for each IoBT node
Result: Reputation score for each node
foreach Node N_i in the network do
    Collect data: successful_transmissions, lost_packets, feedback, battery, latency;
    Build the feature vector X_i
    Apply the Decision Tree Regression model:
        Ri <- DTR.predict(X_i)
    if R_i < threshold then
        Mark node N_i as unsafe
        Apply security rules (e.g., block, packet filtering)
    else
        Allow access and use data transmitted by Ni
    Update the model if needed (online learning)
```

To train the supervised learning model, a data simulator was built to meet the specific requirements of the proposed scenario. Each instance in the dataset represents a virtual node, described by a feature vector comprising the metrics: TSR, PL, B, L, and FB. The simulator computes a reputation score (R) for each instance using a weighted formula:

$$R = 0.4 \times TSR - 0.3 \times PL + 0.2 \times B + 0.0005 \times L + 0.1 \times FB + \text{Gaussian Noise} \quad (1)$$

The weights were assigned based on the presumed impact of each parameter on node trustworthiness:

- TSR (Transmission Success Rate) is the most influential positive factor. A higher TSR indicates reliable data delivery, contributing strongly to a higher reputation score.
- PL (Packet Loss) is a major negative indicator. Frequent packet loss reduces confidence in the node's communication reliability and is penalized accordingly.
- B (Battery Level) reflects the device's battery sustainability. Nodes with sufficient energy are considered more stable and thus more trustworthy.
- L (Latency) is included with a small negative weight. Although high latency may not always indicate malicious behavior, consistent delays can hinder performance and reliability.
- FB (Feedback) introduces a social or collaborative dimension to trust. Positive feedback from peers incrementally improves the reputation of the node.

To enhance realism, Gaussian Noise was added to the computed reputation score. This stochastic component introduces natural variability, mimicking fluctuations that would occur due to hardware imprecision, environmental interference, or transient performance anomalies. Including noise prevents overfitting during model training and improves the generalizability of the regression model when applied to real-world or previously unseen data.

4. Results

A diverse and balanced dataset was generated to train the AI model in a controlled and efficient manner. Before training the machine learning model, we ensured a clean, well-understood, and properly formatted dataset. In this regard, initial preparation and exploratory analysis of the dataset were performed before building and training the machine learning model. This step played a crucial role in verifying the quality of synthetic data and in gaining a deeper understanding of its structure.

Figure 3, created through Python 3.13.4 scripting for data analysis and visualization, illustrates the distribution of reputation scores in this synthetic training dataset. The bell-shaped (approximately normal) distribution indicates that most IoT nodes have moderate reputation scores, while relatively few nodes exhibit very low or very high scores. This balanced distribution supports effective regression model training by preventing class imbalance and ensuring broad coverage of target values. The absence of anomalies in the histogram also indicates that the data generator produced a consistent and reliable dataset suitable for supervised learning tasks.

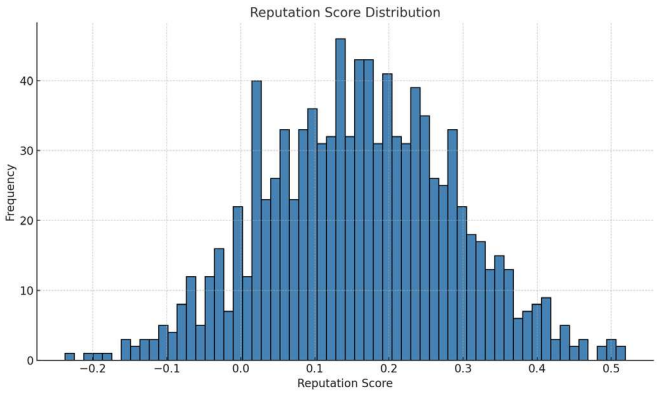

Figure 3. Analysis of Reputation Score Distribution in the Training Dataset.

Moreover, to complement this analysis, a correlation matrix was generated and visualized as a heatmap to examine the linear relationships between variables (see Figure 4). The results show that the transmission success rate (r = 0.59), battery level, and feedback (r = 0.38 each) are positively correlated with reputation, indicating that reliable communication, energy autonomy, and positive peer evaluations enhance the perceived trustworthiness of a node. Conversely, latency (r = −0.56) and packet loss (r = −0.30) are negatively associated with reputation. Importantly, some input features, such as TSR and battery level, are largely uncorrelated (r = 0.01), which ensures that each contributes distinct, non-redundant information to the model. These findings support the inclusion of all five behavioral features in the supervised learning process.

To assess the predictive performance of the supervised learning model, two key metrics are employed: the coefficient of determination (R^2) and the mean squared error (MSE). R^2 measures the proportion of variance in the actual reputation scores that is captured by the model, indicating how well the predictions align with the ground truth. MSE quantifies the average squared difference between the predicted and actual values, providing an estimate

of the model's error magnitude. R^2 values close to 1 indicate a strong agreement between the predicted and actual reputation scores, demonstrating that the model captures most of the variance in the data. MSE values close to 0 indicate minimal prediction errors and high model accuracy. Together, these metrics allow for a robust evaluation of the model's accuracy and reliability, ensuring that the estimated reputation scores accurately reflect the behavior and trustworthiness of IoBT nodes.

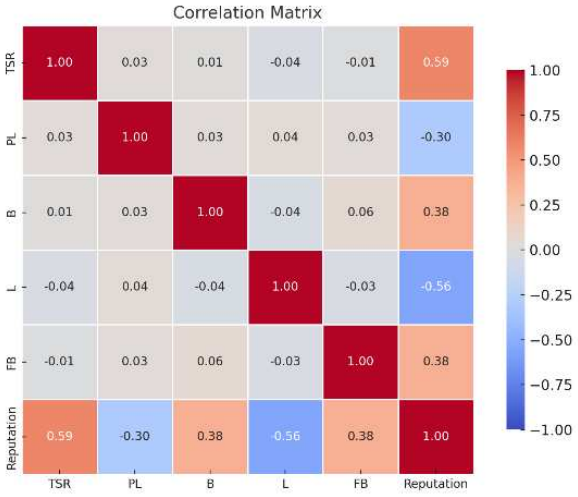

Figure 4. Correlation Analysis of Behavioral Trust Indicators and Reputation Scores.

To evaluate the predictive performance of our model, a scatter plot (see Figure 5) was used to compare the predicted reputation scores with the ground truth values. The red dashed line in the figure represents the ideal diagonal, where the predicted and actual values are equal. The close alignment of points along the diagonal, representing perfect agreement, demonstrates that the model generalizes well to unseen data. In addition, the scatter plot highlights that most predicted values closely overlap with the ground truth along the main diagonal, with only minimal deviations observed. This absence of significant outliers indicates that the model not only generalizes well but also maintains robustness against random variations in the dataset. This visual observation is supported by strong performance metrics: a coefficient of determination (R^2) of 0.9765 and a mean squared error (MSE) of 0.00042. The high R^2 score indicates that the model captures most of the variance in the data, while the low MSE confirms that prediction errors are minimal. The compact clustering of points around the diagonal further confirms the model's stability and suitability for real-time trust estimation in IoBT environments. Together, these results validate the model's reliability in estimating reputation scores, reinforcing its role within the broader trust-based architecture.

Following dataset preprocessing and exploratory analysis, a decision tree regression model was trained to evaluate its ability to learn the mapping between node features (TSR, PL, FB, B, L) and the generated reputation scores. The pipeline included dataset loading, train-test splitting, standard normalization, and model training. Evaluation on the test set yielded an MSE of 0.003 and an R^2 score of 0.807, indicating that the model explains approximately 81% of the variance in reputation scores. To further interpret model behavior, a scatter plot (see Figure 6) was generated. It shows that the model predicts mid-range reputation values with higher accuracy, while deviations are more pronounced at the extremes of the distribution. The diagonal trend in the scatter plot confirms that predictions are generally well-aligned with ground truth values, with only minor dispersion, the red dashed line indicates a perfect match between predicted and actual reputation scores. This demonstrates that the model effectively captures the core relationships between features and reputation scores, even if some non-linearities at extreme values remain challenging.

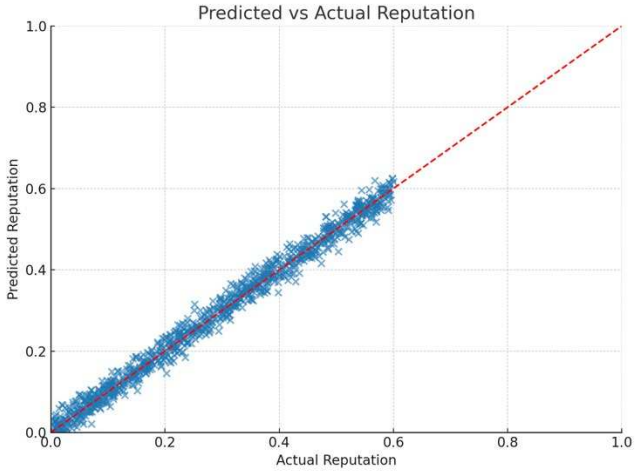

Figure 5. Comparison of Predicted and Actual Reputation Scores for IoBT Nodes Using Linear Regression Model.

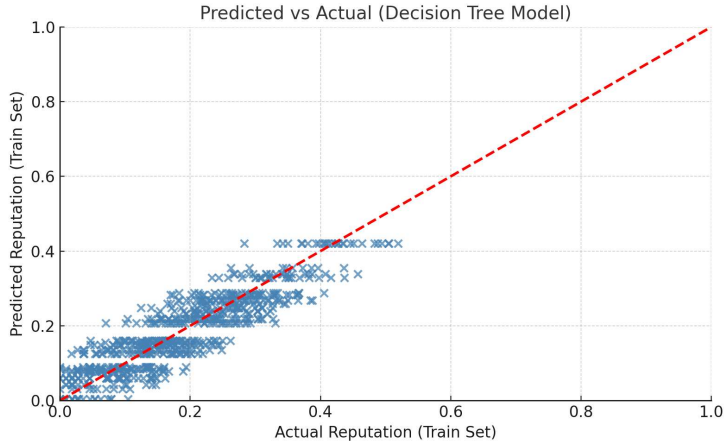

Figure 6. DTR: Evaluation of Model Performance on Training Dataset for Reputation Estimation.

The decision tree regression model achieved lower performance (MSE = 0.003, R^2 = 0.807) compared to the earlier linear regression results (MSE ≈ 0.0004, R^2 ≈ 0.976). This discrepancy is largely due to the inherently linear structure of the synthetic dataset, which aligns better with the assumptions of linear regression. Additionally, the use of default hyperparameters likely limited the performance of the tree, and the train-test evaluation method provided a more realistic measure of generalization. These observations highlighted the need for model optimization, which was subsequently addressed using GridSearchCV. Thus, to enhance the predictive performance of the DTR, a systematic hyperparameter tuning process was conducted using GridSearchCV with 5-fold cross-validation. The optimization targeted key parameters controlling model complexity and generalization:

- max_depth
- min_samples_split
- min_samples_leaf.

The best configuration

- max_depth = 10
- min_samples_leaf = 2
- min_samples_split = 2

resulted in improved performance, with an R^2 of 0.827 on validation folds, 0.831 on the test set, and a consistent MSE of 0.003. These results demonstrate the effectiveness of

the tuning process in refining model accuracy and enhancing its ability to approximate reputation scores reliably.

To evaluate the generalization capability of the model in realistic conditions, a final test was conducted using a newly generated dataset independent of the training data. The model achieved an R^2 score of 0.836 and an MSE of 0.003, indicating strong predictive performance on unseen inputs. As shown in Figure 7, the alignment of predicted values with actual scores confirms the robustness of our model. These results validate the applicability of the model in real-time reputation assessment scenarios within IoT networks, demonstrating both accuracy and reliability beyond the training environment.

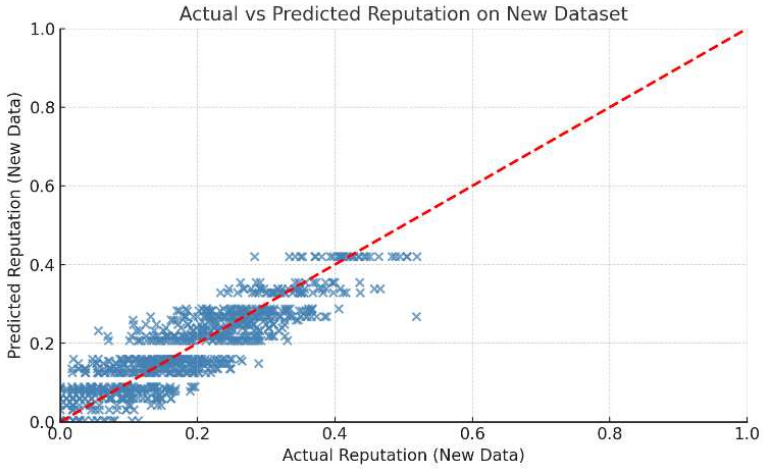

Figure 7. DTR: Evaluation of Model Performance on an Independent Test Dataset.

This final evaluation demonstrates that the model not only fits the training data but also generalizes well to new inputs, validating its use in a real-time IoT reputation assessment system.

5. Discussions

The layered IoBT architecture, from device-level sensing to gateway-based trust evaluation and command-level aggregation, provides a robust foundation for real-time, context-aware decision-making. This modular design ensures that reputation scores computed at the edge or gateway can be reliably integrated into higher-level command infrastructure, supporting secure routing, anomaly detection, and adaptive responses. By linking the performance of the supervised learning model to the system's architecture, the results demonstrate how both the computational framework and the hierarchical design contribute to resilient and informed trust evaluation across the network.

Throughout the development process, the model's performance was carefully monitored at each stage, enabling meaningful comparisons between the baseline, intermediate, and optimized versions. Table 1 summarizes the key metrics (R^2 score and MSE) across all main stages of the pipeline. The linear regression model trained during the exploration phase achieved very high accuracy, likely benefiting from the synthetic nature and internal consistency of the dataset. However, linear models may lack the flexibility to model non-linear interactions that exist in real-world IoBT systems.

The transition to a decision tree regressor resulted in a slight decrease in the R^2 score, due to the model's increased variance and sensitivity to unoptimized splits. However, the introduction of hyperparameter tuning through GridSearchCV significantly improved generalization, especially when evaluated on the unseen test set. Moreover, the final stage confirmed that the optimized model retained its predictive capability on new data, achieving an R^2 score of 0.836 and a low MSE of 0.003. This consistent performance suggests

that the decision tree model, when properly tuned, offers a robust approach for real-time reputation estimation in IoT environments. This progressive improvement highlights the importance of not only model selection but also data preprocessing, scaling, and hyperparameter optimization in achieving a balance between accuracy and generalizability.

Table 1. Performance comparison across implementation stages.

Stage	R^2	MSE
Initial linear regression	0.976	0.0004
Unoptimized decision tree	0.807	0.003
GridSearchCV optimized model	0.831	0.003
Final evaluation on new data	0.836	0.003

In operational contexts, reputation scores derived from behavioral metrics alone may fail to capture the full situational reality of a node, especially in high-stress environments. The integration of physiological data enables the trust model to adapt its decisions based not only on performance indicators, but also on the physical condition of the operator of the node. For instance, a sudden drop in communication quality might otherwise trigger security mechanisms such as access restriction or data filtering. However, when the system detects concurrent physiological stress, such as elevated heart rate, abnormal body temperature, or irregular ECG readings, the reputational penalty is proportionally mitigated. This ensures that decisions remain context-aware and aligned, avoiding the unfair penalization of nodes whose degraded behavior may stem from legitimate physiological strain rather than malicious intent. By incorporating this adjustment, the trust evaluation framework enables fairer, more resilient, and human-centric decision-making in military-grade IoT networks.

6. Conclusions

This study presents a context-aware trust evaluation framework for IoT nodes operating in dynamic and mission-critical environments. Leveraging supervised learning, specifically Decision Tree Regression, we developed a robust model capable of estimating node reputation scores based on behavioral metrics, including transmission success rate, packet loss, latency, battery level, and peer feedback. The model demonstrated strong predictive performance across multiple validation stages, with optimization techniques such as GridSearchCV further enhancing its generalizability. To address limitations in traditional trust models that overlook the operational context, we introduced a physiological adjustment mechanism using a Medical Stress Index (MSI). This approach integrates vital signs, heart rate, body temperature, blood pressure, ECG signal, and stress level into a dynamic penalty system that modulates reputation scores based on the node operator's physical state. The adjusted model preserved predictive accuracy while introducing greater resilience and fairness, particularly in sensitive scenarios. The scientific questions regarding the influence of behavioral and physiological parameters on node trustworthiness were successfully addressed, confirming that context-aware metrics improve both reliability and decision-making in IoBT networks. The comparative analysis confirms that the trust framework performs consistently on new data and benefits from contextual integration. This architecture offers a scalable, modular, and responsible solution for secure, real-time decision-making in battlefield IoT environments, where adaptability and situational awareness are paramount. Implementation challenges included generating a realistic and balanced synthetic dataset, ensuring model generalization across nodes, and integrating physiological adjustments without compromising computational efficiency. Future work could explore deployment in real battlefield environments, inclusion of additional

behavioral and environmental features, and development of fully autonomous adaptive trust mechanisms to further enhance situational awareness and operational security. Additionally, enhancing system security against deliberate trust manipulation and adversarial attacks represents a key direction for future research, ensuring that the trust evaluation framework remains robust under malicious or unforeseen conditions.

Author Contributions: Conceptualization, I.M. and V.-V.P.; methodology, I.M. and V.-V.P.; software, I.M.; validation, I.M. and V.-V.P.; formal analysis, I.M.; investigation, I.M.; resources, I.M. and V.-V.P.; data curation, I.M.; writing—original draft preparation, I.M.; writing—review and editing, I.M. and V.-V.P.; visualization, I.M.; supervision, V.-V.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original data presented in the study are openly available in GitHub at https://github.com/ioanamat/IOBT-generated-data (accessed on 10 September 2025).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Airehrour, D.; Gutiérrez, J.A.; Ray, S.K. A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks. *Aust. J. Telecommun. Digit. Econ.* **2017**, *5*, 50–59. [CrossRef]
2. Tariq, N.; Asim, M.; Maamar, Z.; Farooqi, M.; Faci, N.; Baker, T. A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT. *J. Parallel Distrib. Comput.* **2019**, *134*, 153–166. [CrossRef]
3. El-Sisi, A.; Youssef, A. A trust-management-based intrusion detection system for routing protocol attacks in Internet of Things. *Int. J. Comput. Inf.* **2020**, *10*, 45–59.
4. Bica, I.; Chifor, B.; Arseni, S.; Matei, I. Reputation-Based Security Framework for Internet of Things. In *Innovative Security Solutions for Information Technology and Communications*; Simion, E., Géraud-Stewart, R., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 213–226.
5. Arseni, S.-C.; Chifor, B.-C.; Coca, M.; Medvei, M.; Bica, I.; Matei, I. RESFIT: A reputation and security monitoring platform for IoT applications. *Electronics* **2021**, *10*, 1840. [CrossRef]
6. Bica, I.; Chifor, B.-C.; Arseni, S.; Matei, I. Multi-layer IoT security framework for ambient intelligence environments. *Sensors* **2019**, *19*, 4038. [CrossRef] [PubMed]
7. Cișmaș, A.G.; Cișmaș, I.; Popescu, G.D.; Popescu, N. Proposed system for multi-node communication. *J. Control Eng. Appl. Inform.* **2024**, *26*, 45–52. [CrossRef]
8. Vikas, W.C.; Sagar, B.B.; Manjul, M. Trusted Energy-Aware Hierarchical Routing (TEAHR) for wireless sensor networks. *Sensors* **2025**, *25*, 2519. [CrossRef] [PubMed]
9. Smith, S.E.; Jones, L.Q. An adaptive approach to detecting black and grey hole attacks in ad hoc networks. In Proceedings of the IEEE International Conference on Advanced Information Networking and Applications, Perth, Australia, 25–28 March 2008; pp. 775–780.
10. Osathanunkul, K.; Zhang, N. A countermeasure to black hole attacks in mobile ad hoc networks. In Proceedings of the 2011 International Conference on Networking, Sensing and Control, Delft, The Netherlands, 11–13 April 2011; pp. 508–513.
11. Aaqib, M.; Ali, A.; Chen, L.; Nibouche, O. IoT trust and reputation: A survey and taxonomy. *J. Cloud Comput.* **2023**, *12*, 42. [CrossRef]
12. Singh, J.; Dhurandher, S.K.; Woungang, I.; Chao, H.-C. Context-Aware Trust and Reputation Routing Protocol for Opportunistic IoT Networks. *Sensors* **2024**, *24*, 7650. [CrossRef] [PubMed]
13. Kalaria, A.; Thakkar, A.; Patel, D.; Prajapati, R. Context-aware access control in fog-enabled IoT using machine learning. *Future Gener. Comput. Syst.* **2024**, *149*, 192–205.
14. Kufakunesu, R.; Myburgh, H.; De Freitas, A. The Internet of Battle Things: A survey on communication challenges and recent solutions. *Discov. Internet Things* **2025**, *5*, 3. [CrossRef]
15. Liu, D.; Abdelzaher, T.; Wang, T.; Hu, Y.; Li, J.; Liu, S.; Caesar, M.; Kalasapura, D.; Bhattacharyya, J.; Srour, N.; et al. IoBT-OS: Optimizing the sensing-to-decision loop for the Internet of Battlefield Things. In Proceedings of the International Conference on Computer Communications and Networks (ICCCN 2022), Honolulu, HI, USA, 25–28 July 2022; pp. 1–10.

16. Russell, S.; Abdelzaher, T.; Suri, N. Multi-domain effects and the Internet of Battlefield Things. In Proceedings of the MILCOM 2019—IEEE Military Communications Conference, Norfolk, VA, USA, 12–14 November 2019; pp. 724–730.
17. Cișmaș, I.; Cișmaș, A.G. Hardware parameters for trust mechanisms in MIoT. In *Advances in Digital Health and Medical Bioengineering. EHB 2023. IFMBE Proceedings, vol. 109*; Costin, H.N., Magjarević, R., Petroiu, G.G., Eds.; Springer: Cham, Switzerland, 2024; pp. 224–230.