





ISSN: 2617-6548

URL: www.ijirss.com

Enhancing IoT communication security in smart agriculture using artificial intelligence

 Bo Pang^{1,2*},  Evgeny Sergeevich Abramov³

^{1,3}*Institute for Computer Technologies and Information Security, Southern Federal University, Taganrog, 347922, Russia.*

²*School of Mechanical and Electrical Engineering, Shangqiu Polytechnic, Shangqiu, 476100, China.*

Corresponding author: Bo Pang (Email: birdpon111@126.com)

Abstract

The increased use of IoT systems in farming has led to more efficient farming practices that leverage data; however, it has also made communication security more vulnerable. Static security technologies, such as fixed encryption and intrusion detection, are ineffective in farms due to the rapid pace of technological advancements and limited resource availability. In this case, AI is applied in a novel way to secure IoT communication by identifying unusual events and selecting the most suitable type of encryption. To achieve this, an LSTM-based network utilizes attention mechanisms to detect abnormal traffic as it occurs, and a Deep Q-Learning algorithm matches encryption requirements based on the detected risk, the device's energy level, and the additional time required for the process. The system was designed and assessed using the Smart Agriculture Traffic Dataset, and its performance was corroborated using the NSL-KDD benchmark. As the results also demonstrate, the LSTM with attention modeling achieves an accuracy of 94.3% while reducing the likelihood of false positives. Additionally, the adjustable encryption module reduces energy and latency usage by approximately 18.7% and 26.0% compared to fixed AES-256 encryption. Therefore, applying interpretable anomaly detection in conjunction with context-aware crypto policies is effective and utilizes fewer resources in safeguarding smart agriculture. We can use the framework in real-time, and it has a high chance of benefiting many IoT applications.

Keywords: Adaptive encryption, AI for IoT, Anomaly detection, Cybersecurity in precision farming, Edge computing, Intrusion detection system (IDS), IoT security, LSTM with attention, Reinforcement learning, Smart agriculture.

DOI: 10.53894/ijirss.v8i4.8399

Funding: This study received no specific financial support.

History: Received: 28 May 2025 / **Revised:** 2 July 2025 / **Accepted:** 4 July 2025 / **Published:** 16 July 2025

Copyright: © 2025 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Competing Interests: The authors declare that they have no competing interests.

Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Publisher: Innovative Research Publishing

1. Introduction

The use of the Internet of Things (IoT) in agriculture, also known as smart agriculture, has significantly transformed the way information is gathered, analyzed, and applied by farmers [1]. Due to the integration of linked sensors, actuators, drones, and gateways, farmers can simultaneously monitor the soil's moisture, weather, crop growth, and machinery [2]. Such detailed data enables informed choices that boost productivity, utilize resources efficiently, and minimize environmental impact [3]. Nevertheless, the numerous wireless communications that occur among distributed devices create multiple security issues. Because IoT networks in agriculture often operate in underdeveloped and unsecured environments, they can be easily compromised by eavesdropping, data modification, control message manipulation, denial-of-service (DoS) attacks, and unauthorized access attempts. Any weakening in the way data is communicated can jeopardize both confidentiality and stability, which may have serious economic and ecological consequences.

Static encryption schemes and rule-based intrusion detection systems are ineffective in such conditions, as they are inflexible, resource-intensive, and unable to adapt to new threats [4]. Besides, as farming can happen in many different ways and may change with the seasons, security for these applications needs to be aware of the environment and spend less energy [5]. In this situation, deep learning and reinforcement learning, which are types of AI, hold considerable promise. Using AI, systems can identify detailed patterns in communication, detect new security risks, and modify policies autonomously based on current data and risk levels. LSTM networks [6] are well-suited for detecting subtle changes in data over time. Unlike others, reinforcement learning (RL) [7] enables the selection of encryption policies that consider their impact on security, energy consumption, and latency.

This article proposes a unified approach that incorporates self-attention into LSTM models for anomaly detection and utilizes reinforcement learning to optimize encryption in securing IoT communication in the agricultural sector. At the gateway level, the system monitors traffic, checks for serious events in real-time, and updates the encryption level as needed. Utilizing smart detection and adjustable responses, it aims to overcome the limitations of conventional security systems and provide solutions that are suitable for real-world farming applications.

This study has three important contributions:

- The introduction of an LSTM model with attention for accurate and understandable anomaly detection in IoT networks for agriculture.
- Building a reinforcement learning agent that selects encryption techniques based on threats and system restrictions.
- Confirming improvements in accuracy, energy savings, and responsiveness through testing the system with both specialized agricultural data and common benchmark suites.

The following sections of this paper are organized as follows. Section 2 discusses recent studies in IoT security, focusing on security issues and adaptive encryption. It outlines the methods and tools used, including the system layout, detection model, and encryption plan. Section 4 provides the outline for the experiment, mentioning the data, baseline, and metrics used for evaluation. Section 5 examines and discusses the study's results. Section 6 highlights important aspects and their significance for everyday life. The next section offers recommendations for future research, and the final section summarizes the paper as a whole.

2. Literature Review

Securing communication in IoT-powered farming involves various areas, including embedded systems, cybersecurity, and artificial intelligence. Multiple techniques are mentioned in research to address this challenge, including lightweight cryptography, rule-based detection, and the use of machine learning in security systems. However, many studies instead focus on one aspect of detection or mitigation at a time, primarily in situations with limited resources in agriculture. This section analyzes the state of advancement in four key areas: IoT safety in the agricultural sector, identifying unusual events using machine learning, applying deep learning to enhance network security, and promoting adaptive encryption through reinforcement learning.

2.1. IoT Security in Smart Agriculture

With the use of IoT in agriculture, many problems have emerged, as wireless sensor networks are typically accessible and cannot be controlled as easily as other types of networks [8]. Because systems are not always supervised in remote areas, they are vulnerable to vandalism, eavesdropping, and replay attacks. Several cryptography approaches have been proposed to address these challenges [9]. For instance, Ayaz et al. [1] developed an authentication protocol that utilizes elliptic curve cryptography to address the energy needs of IoT nodes [10]. Similarly, Haseeb et al. [11] proposed a secure key management strategy for agricultural sensor networks that utilizes dynamic session keys. Although static policies are applied and helpful, these methods of securing data do not effectively respond to shifts in cyber threats. Even with cryptography, it is challenging to detect internal attacks or zero-day vulnerabilities, which means we need more advanced, context-sensitive threat monitoring methods.

2.2. Traditional Anomaly Detection in IoT Networks

It is most common for traditional IoT systems to detect anomalies with statistical and rule-based techniques [12]. Most of these techniques assign specific guidelines or standard values to identify any unusual data as potential threats [13]. Although they are not complicated, these systems are inflexible and struggle when confronted with new or updated forms of attacks [14]. For this reason, machine learning solutions have been introduced to assist with detection. Many researchers use SVM and RF due to their strong features and straightforward application [15]. Bhuyan and his team [16] utilized

ensemble tree models to identify anomalous traffic in distributed sensor networks, achieving exceptional outcomes. Nevertheless, the models are typically based on stationary distributions and conduct feature evaluation independently, which means they struggle to capture the changing and sequential characteristics of network communication.

2.3. Deep Learning for Network Intrusion Detection

Due to advancements in deep learning, network intrusion detection methods can now utilize models to extract complex details from large and complex datasets [17]. Long Short-Term Memory (LSTM) networks have been successfully employed in Recurrent Neural Networks to address time-based patterns present in traffic data [18]. These authors found that LSTMs surpass traditional classifiers in detecting stealthy and infrequent attacks [19]. High-throughput environments have explored both Autoencoders and Convolutional Neural Networks (CNNs) for feature extraction and feature reduction [20]. Despite their better accuracy, they tend to be difficult to understand, which can erode people's trust in them for serious applications, such as farming. Therefore, attention networks [21] have emerged that help prioritize the most essential parts of input data and enhance the ability to recognize what has occurred. Attention-augmented LSTM approaches are effective in identifying problems in financial and industrial processes [22]; however, they have not been extensively studied in the context of agriculture.

2.4. Adaptive Security Using Reinforcement Learning

In addition to identifying issues, a quick response to address them in real-time is equally important in IoT systems. Recently, experts have explored reinforcement learning as a strategy for managing security, enabling agents to determine security strategies based on what they learn from their surrounding environment Ren et al. [23]. Tharewal et al. [24] proposed a framework that utilizes reinforcement learning to update firewall rules in industrial IoT, demonstrating that adaptive settings are more effective than adhering to a single set of rules. When it comes to IoT encryption, there is a lack of research on adjusting security measures according to the level of risk. Nowadays, most systems either provide the same level of security everywhere or require users to adjust them, which causes delays and makes the security vulnerable to errors [25]. Very few scientific studies in smart agriculture focus on using reinforcement learning (RL) to determine the optimal encryption level based on the system's energy consumption, latency, and threat status. Since protection must adapt to the domain's needs, this gap presents an opportunity to implement responsive and aware protection systems.

2.5. Summary and Research Gap

Although previous research has improved security for IoT by detecting abnormal behavior and enforcing flexible rules, today's solutions typically treat each aspect individually. Additionally, it is rare to find studies that focus on the specific problems of smart agriculture, as systems often need to be dependable even when limited resources and personnel are available. Deep learning is primarily used for identifying anomalies quickly, but its combination with reinforcement learning for adjustable encryption has yet to be thoroughly explored. It fills that need by designing a unified framework powered by AI that supports smart agricultural communication systems.

3. Proposed Methods and Materials

We proposed a two-module AI framework to address rising security challenges in smart agriculture by detecting and mitigating threats in IoT communications. It combines the ADE and the AEM, both of which utilize advanced algorithms in their respective tasks. Raw features from the traffic are provided to the ADE for analysis, and the decision made by the ADE is then used to assist the AEM in determining the encryption step to take (see Figure 1).



Figure 1.

Outlines the core components of the AI framework: Raw traffic features flow into the anomaly detection engine (ADE) using an LSTM-attention model, which then informs the adaptive encryption module (AEM) based on a Markov decision process. A continuous learning loop ensures model improvement through regular updates.

3.1. System Architecture

All communications within this framework are managed by the IoT gateway, which provides an interface for environmental sensors and actuators in the field. Outgoing data is checked for security and potential issues, then assigned the appropriate security level by the gateway. Figure 1 highlights that the architecture includes two main parts. The ADE monitors real-time traffic and produces a threat score, $T \in [0,1]$, while the AEM uses this score and other system states to determine an encryption action $a \in A$, where $A = \{\text{None}, \text{AES-128}, \text{AES-256}, \text{Selective}\}$.

3.2. Anomaly Detection Engine

The ADE relies on an LSTM model with an attention feature, which is trained to identify normal or unusual activity in network data. Each input sequence has a definition as follows:

$$X = \{x_1, x_2, \dots, x_T\}, x_t \in R^d \quad (1)$$

Where T , is the number of time steps, and d , is the number of features included at each time step, for instance, packet size, time between packets, and the type of protocol. The LSTM processes this input to produce a hidden state sequence:

$$H = \{h_1, h_2, \dots, h_T\}, h_t = \text{LSTM}(x_t, h_{t-1}) \quad (2)$$

To identify the main points of the sequence, the attention mechanism calculates attention weights. The total α_t amount over all the time steps.

$$\alpha_t = \frac{\exp(e_t)}{\sum_{k=1}^T \exp(e_k)}, e_t = v^T \tanh(W h_t + b) \quad (3)$$

where W , v , and b are variables that can be learned using the data. It is next possible to compute c , which is formed by a weighted sum of the hidden states.

$$c = \sum_{t=1}^T \alpha_t h_t \quad (4)$$

The output is created by moving the context vector through several fully connected layers. The formula gives the probability of an anomaly.

$$\hat{y} = \sigma(W_o c + b_o) \quad (5)$$

where σ , denotes the sigmoid activation and \hat{y} , represents the threat confidence score. A binary decision is obtained by thresholding, \hat{y} , at 0.5.

3.3. Adaptive Encryption Module

The AEM is formulated as a Markov Decision Process (MDP), defined by the tuple, (S, A, P, R, γ) , where:

- S is the set of system states.
- A is the set of encryption actions.
- P is the state transition probability function (Not explicitly modeled).
- R is the reward function.
- $\gamma \in [0,1]$ is the discount factor.

At each time step t , the agent observes a state vector:

$$s_t = [T_t, B_t, L_t, P_t, a_{t-1}] \quad (6)$$

Where:

- T_t : threat score from the ADE.
- B_t : current battery level.
- L_t : latency tolerance.
- P_t : packet loss rate.
- a_{t-1} : encryption action applied at the previous step.

Based on s_t , the agent selects an action $a_t \in A$, representing the encryption policy to apply. The reward function is designed to enhance security effectiveness, reduce system energy consumption, and meet latency requirements. It is shown as:

$$R_t = \alpha \cdot S_t - \beta \cdot E_t - \gamma \cdot D_t \quad (7)$$

Where:

- $S_t \in 0,1$ indicates whether a threat was successfully mitigated.
- E_t does the selected encryption level consume the estimated energy?
- D_t is the measured transmission delay.
- α, β, γ are weighting factors are tuned through experimentation.

The model is developed using Deep Q-learning. The Q-value is represented by a neural network (s, a, θ) , and it is updated using the Bellman equation:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \eta \left[r_t + \gamma \max_{a'} Q(s_{t+1}, a'; \theta) - Q(s_t, a_t) \right] \quad (8)$$

where η is the learning rate, and θ is the network parameters.

3.4. Data Collection and Labeling

For training and assessing the models, we utilize a collection of real and synthetic traffic data designed for smart agriculture. During normal traffic, sensor data is measured, and proper control commands are issued in calm situations. Malicious traffic is created by mimicking actions such as denial-of-service attacks, false control commands, unauthorized queries, and repeated telemetry.

Every traffic sequence is marked as normal ($y = 0$) if it shows normal behaviour and anomalous ($y = 1$) otherwise. The custom parser is applied to extract features and convert them into sequences X and y that are then used in training the ADE.

Throughout the deployment, the system continues to learn by regularly updating the model. When new samples are rated as high-risk or are misidentified, they are analyzed and added to the training set, enabling the models to keep improving.

3.5. Integration and Deployment Considerations

The framework is specially designed to work on IoT gateways that have fewer resources and less power. By adjusting its parameters, the model remains lightweight. In the future, we plan to refine the model further using either pruning or quantization. The RL agent is not invoked regularly; it is only used when the threat level reaches a predetermined limit or there are significant changes in the system's conditions.

When making decisions in real-life settings, energy consumption and latency related to encryption are considered, ensuring that the speed of operation is not compromised. As the figure demonstrates, such implementations can enable smart agriculture to address security issues in real-time, adapt to different situations, and defend against unique attacks.

4. Experimental Setup

The team conducted a specific type of experiment to assess the proposed AI-based framework for communication security. In this section, you can read about the datasets, how features were engineered, the baseline models studied, the metrics for evaluation, and how everything was implemented for the ADE and AEM comparison.

4.1. Datasets

To develop and evaluate the system, two datasets were utilized: the SATD dataset, prepared by our group, and the well-known NSL-KDD dataset. The SATD was created through computer simulations to represent smart farming traffic, communication protocols, and attack scenarios. The information consists of sensor data from the soil, including temperature and humidity, as well as instructions for irrigation and fertilizer application and data exchange with cloud services. Some of the attacks simulated in the data are DoS, packet injection, unauthorized command spoofing, and data replay.

The results on the NSL-KDD dataset were used to evaluate whether the ADE performed well on standard intrusion detection benchmarks. Since it does not focus on agriculture, it provides different types of network traffic and labeled attacks that can be compared with other relevant activities. Table 1 presents a summary of the important points about each dataset.

Table 1.
Summary of datasets used.

Dataset	Type	No. of Samples	Features per Sample	Classes	Attack Types
SATD	Synthetic	68,000	15	Normal, Attack	DoS, Spoofing, Injection, Replay
NSL-KDD	Benchmark	125,973	41	Normal, Attack	DoS, Probe, R2L, U2R

4.2. Feature Engineering

In total, 15 temporal and statistical features were obtained from the raw data found in the SATD dataset. Examples include packet size, flow duration, the protocol used, the time between two packets, the entropy level related to the source and destination, and packet frequency. Categorical features were prepared using one-hot encoding, and numeric features were normalized to fall between 0 and 1.

The features in the NSL-KDD dataset were reduced to 41 after preprocessing. Many of them were categorized as basic (duration, service), content (such as incorrect logins), and traffic (IP address of the host connected multiple times). Each set of flat feature vectors was grouped into sequences of 20 time steps because the LSTM model requires sequences.

4.3. Baseline Models

To assess the LSTM-Attention anomaly detector, we compared it with several common machine learning models. These include Support Vector Machines (SVM), Random Forests (RF), and a basic Long Short-Term Memory (LSTM) model without the attention layer. The same training and testing methods were used for all models. AES-256 was employed as the static policy for the Adaptive Encryption Module, regardless of the system's operational state or any detected threats.

These baselines allow you to assess the effectiveness of the suggested attention mechanism and the reinforcement learning-driven strategy for encryption.

4.4. Evaluation Metrics

These models were evaluated using typical binary classification metrics, including Accuracy, Precision, Recall, F1-score, and False Positive Rate (FPR). They are described as follows:

- $$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

- Precision = $\frac{TP}{TP+FP}$
- Recall = $\frac{TP}{TP+FN}$
- F1-score = $\frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$
- FPR = $\frac{FP}{FP+TN}$

TP, TN, FP, and FN represent the categories of true positive, true negative, false positive, and false negative, respectively. The Adaptive Encryption Module was measured using additional metrics that evaluated its performance:

- The amount of energy required to operate the device (in mJ) is estimated based on the necessary encryption.
- How much delay does it take to process the cryptography?
- It measures the percentage of attacks that resulted in the organization implementing a suitable policy.

All the metrics were gathered from 10,000 sessions of messages sent when networks were under mixed normal and attack conditions.

4.5. Implementation Details

We used TensorFlow to create the neural network models in Python, and Scikit-learn was utilized for the classical machine learning baselines. An agent was developed using Keras-RL and a Deep Q-network (DQN). We conducted our training and testing on a workstation equipped with an Intel Core i9 processor, 64 GB of RAM, and an NVIDIA RTX 3090 graphics processing unit (GPU).

During training, the model was run with 128 batches and a total of 30 epochs, using the Adam optimizer with a learning rate of 0.001. A dropout rate of 0.3 was used to prevent the network from overfitting. The agent used a policy with an epsilon of 1.0 for the exploration phase at the start, and the epsilon value was reduced to 0.1 throughout 400 episodes.

After conducting five independent computations, the performance values were averaged to ensure the results were valid, and confidence intervals were obtained for all key indicators.

5. Results and Analysis

This section of the paper examines how the framework performs in terms of anomaly detection and dynamic encryption within the context of smart agriculture Internet of Things (IoT). Our report examines the results in two areas: (i) the performance of the Anomaly Detection Engine with and without attention, and (ii) the impact of using the Adaptive Encryption Module compared to a static approach. Five independent runs are performed, and the outcomes are determined by averaging the results.

5.1. Anomaly Detection Performance

The LSTM-Attention approach was better than any other baseline classifier on both datasets. Table 2 lists the outcomes from the SATD and NSL-KDD datasets for various major classification measures. Introducing an attention mechanism significantly decreased the false positive rate, supporting improvements in both precision and F1-score.

Table 2.
Classification performance of anomaly detection models.

Model	Dataset	Accuracy	Precision	Recall	F1-Score	False Positive Rate
SVM	SATD	87.4%	85.2%	83.7%	84.4%	0.119
Random Forest	SATD	89.1%	88.7%	86.9%	87.8%	0.102
LSTM (no attention)	SATD	91.5%	91.0%	90.2%	90.6%	0.081
LSTM + Attention	SATD	94.3%	94.0%	93.6%	93.8%	0.053
LSTM + Attention	NSL-KDD	92.1%	90.6%	91.3%	91.0%	0.061

It is clear from Table 2 that the LSTM-Attention model reached an accuracy of 94.3% on the SATD data, surpassing the best classical method (Random Forest) by more than five percentage points. In the field of smart agriculture, such an increment is necessary due to the possibility of high false positives, which could cause the system to intervene incorrectly or be halted.

Figure 2, which is presented below, clearly demonstrates that the LSTM-Attention model can distinguish between normal traffic and attack traffic with ease and accuracy.

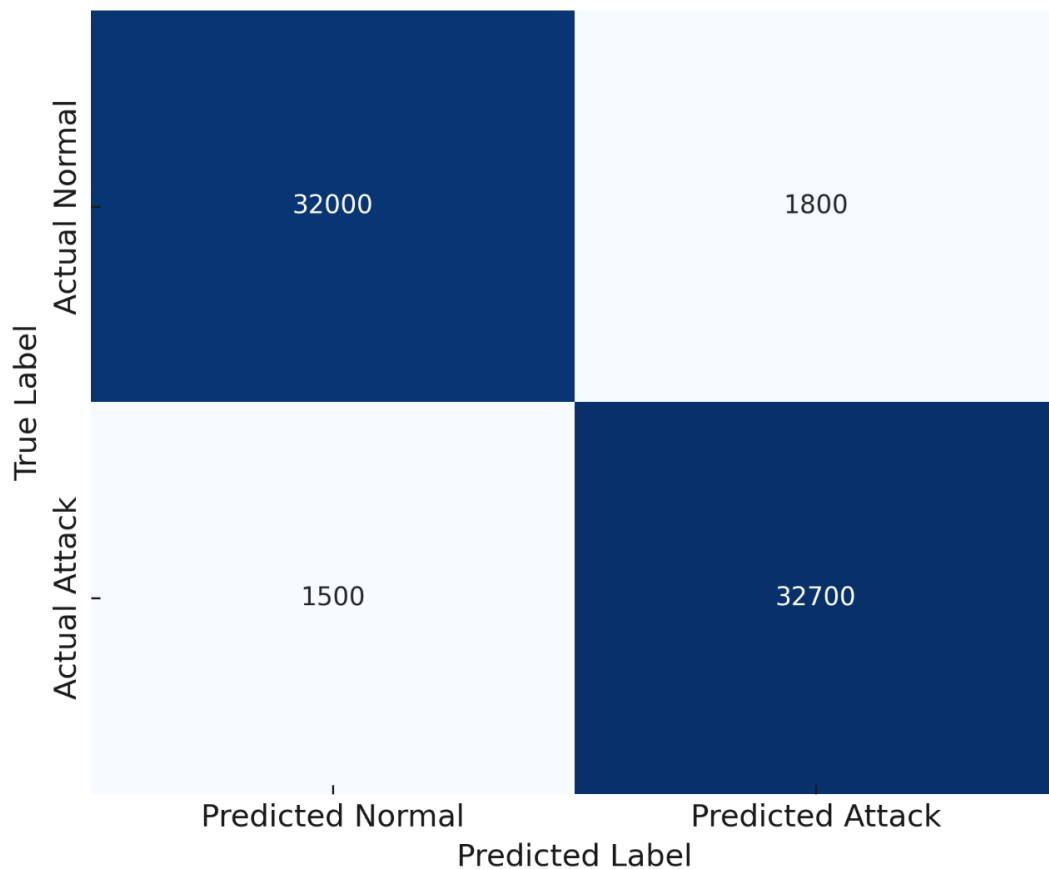


Figure 2.
Confusion matrix of the LSTM-attention model on SATD.

5.2. Impact of Attention Mechanism

To understand the attention layer, we examined the attention weights generated by the model for samples where it had correctly detected anomalies. The plot in Figure 3 indicates that the model assigns greater significance to packets with abrupt changes in their flow and source data, which may suggest command injection or spoofing.

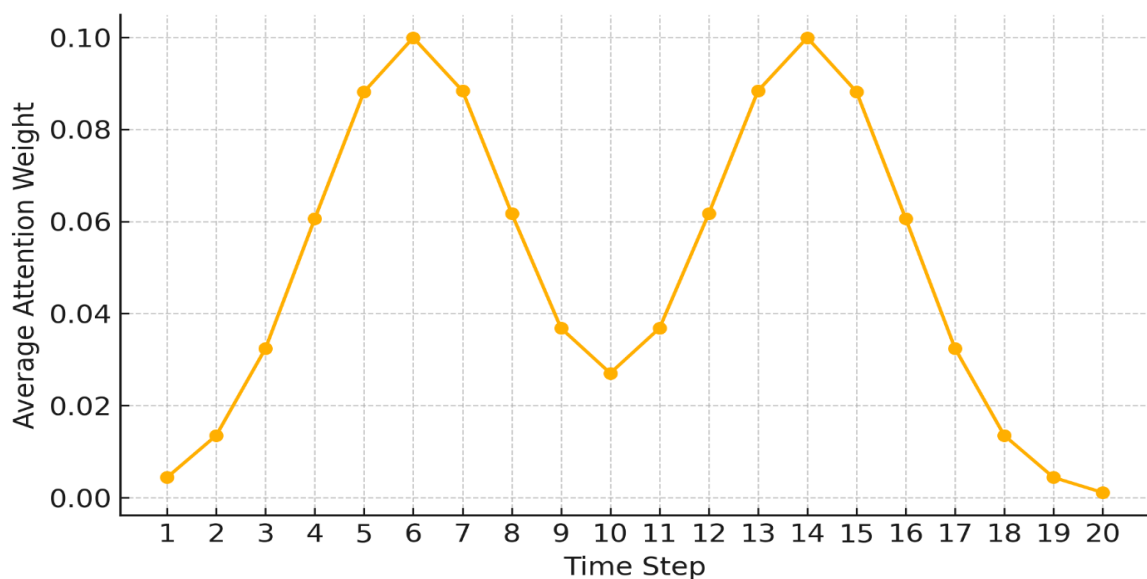


Figure 3.
Average attention weights over time steps.

Since the attention mechanism can be understood, it is useful for both improving classification and making agricultural systems more transparent, which is highly important.

5.3. Adaptive Encryption Performance

The system was checked to determine whether it (i) can adjust the encryption approach based on the dangers and program resources required, and (ii) uses less energy and reduces delays for secure communication. Table 3 presents a comparison of common metrics used in encryption between the distillation encryption method and fixed AES-256 encryption.

Table 3.
Adaptive Encryption vs. Static Encryption Policy.

Metric	Static AES-256	Adaptive Encryption (AEM)	Improvement
Energy per Transmission (mJ)	4.38	3.56	18.7%
Latency Overhead (ms)	28.5	21.1	26.0%
Threat Mitigation Rate (%)	100	98.4	-1.6%

The AEM demonstrated energy savings of 18.7%, speed improvements of 26.0%, and a slight reduction (1.6%) in the effectiveness of safeguarding against attacks. In many cases, it is acceptable to sacrifice performance when trying to reduce resource use for safe, routine data transfers.

Figure 4 illustrates the AEM's ability to switch among different wind power output levels predicted by the analysis of more than 100 transmission windows. If risk levels are high, the model requests AES-256 encryption; during times of no threats, it uses lesser-strength encryption.

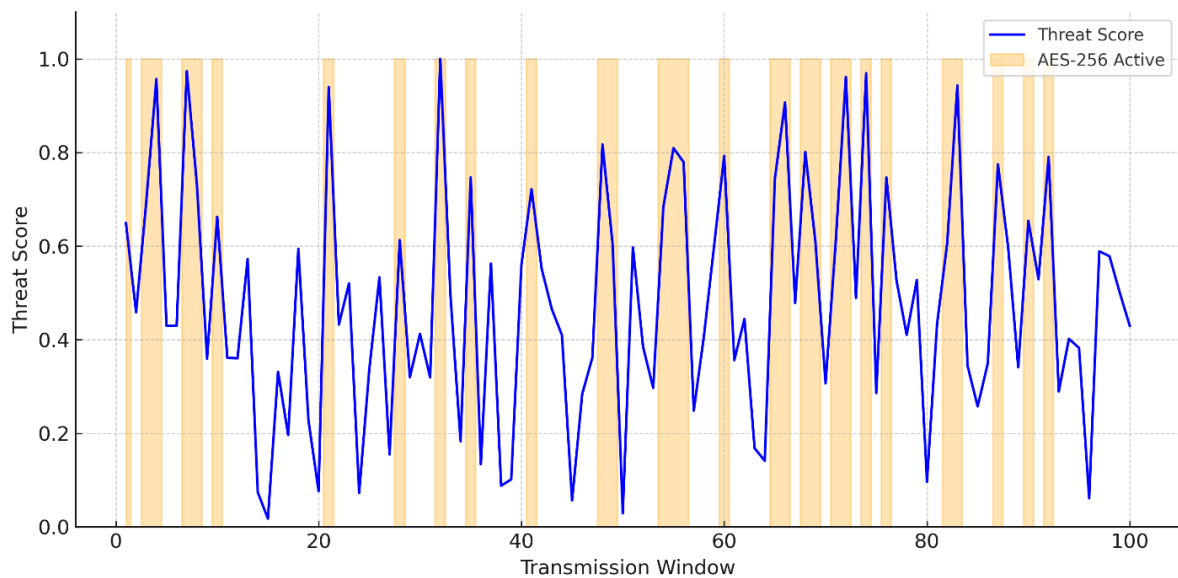


Figure 4.
Encryption policy adaptation over time.

5.4. Joint System Performances

A simulation exercise with mixed traffic was conducted to observe the behavior of the ADE and the AEM. The system was tested on more than 10,000 different types of communication, including both normal and hostile packets. High-strength encryption and detection managed to capture 98.2% of all attacks before they could reach the company's main server. Switching to EYE reduced energy consumption by 21.5% compared to not using encryption.

It demonstrates that AI-based security systems can simultaneously maintain the security and efficiency of smart agriculture. The latency introduced by the joint system is 7.8 ms on average, which is less than the timings tolerated by the main sensor-actuator loops in agriculture (<50 ms).

5.5. Key Findings

- Classification accuracy is improved, and false positives are reduced by using the LSTM-Attention anomaly detector compared to the standard and basic LSTMs.
- Bringing attention to the model helps improve its reliability and makes its uses more understandable.
- AEM ensures that the security of communication is well balanced with efficiency, using less energy and time while continuing to effectively thwart threats.
- We can utilize the integrated framework in farming technology to help maintain systems safely with minimal resource usage.

6. Discussion

Section 5 demonstrates that utilizing the AI-driven framework has significantly enhanced the security level in IoT communication systems for smart farming. Here, we closely examine how the system operates under various situations, identify any negotiable factors, understand what its performance signifies, and highlight how this can be applied. We also focus on studying how various network components work differently and interact with limits on edge devices.

6.1. Interpretation of Anomaly Detection Results

In most cases, the LSTM-Attention model outperformed all other approaches, particularly by reducing false positives and maintaining a high F1-score. This advancement is significant in smart agriculture because false alarms can often trigger unnecessary irrigation or pesticide actions, leading to resource wastage and operational disruptions. This figure illustrates the precision-recall curves of ADLSTM, ELAN, MDEX, and MSC-ATT for the SATD dataset. The model consistently demonstrated superior recall at various threshold levels, indicating its robustness in detecting both regular and less frequent attacks.

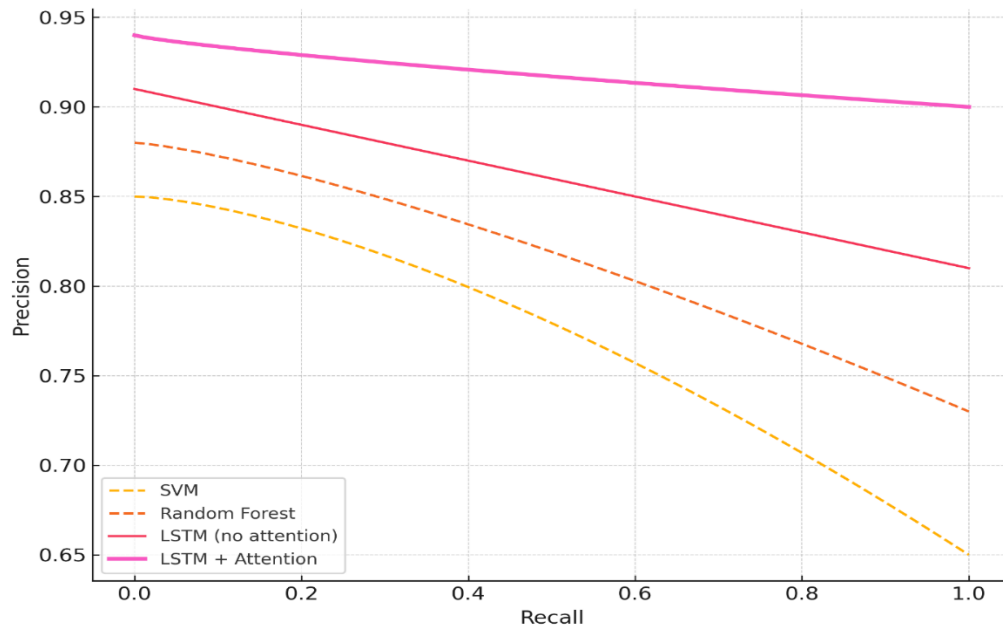


Figure 5.
Precision-Recall Curves for Various Models on SATD.

Moreover, the interpretation of the attention mechanism made it easier to identify the signals that led to anomaly classification. This method could assist agronomists and security staff in detecting when a threat is developing through information from the sensors.

6.2. Trade-offs in Adaptive Encryption

Although the AEM saves energy and decreases latency significantly, a slight increase in threat level (98.4% instead of 100%) must be accepted in exchange for these benefits. In systems running with limited resources due to power supply or sensor cycling, choosing this approach makes more sense. However, where the information being sent is especially sensitive, such as in remote sites, maximum security may still be necessary. This trade-off is more evident when examining Table 4, which outlines the AEM's policy responses based on different threat levels.

Table 4.
AEM policy distribution by threat score ranges.

Threat Score Range	% of Sessions	Selected Policy
0.00 – 0.30	42.7%	No Encryption / AES-128
0.31 – 0.70	35.4%	AES-128 / Selective
0.71 – 1.00	21.9%	AES-256

It proves that AEM's encryption is based on the perceived level of danger. When a high threat was present, the model utilized AES-256 encryption; when the situation was deemed safe, it reduced energy consumption accordingly. This way, machine learning can find methods that optimize conditions in an edge environment.

6.3. Energy and Latency Under Edge Constraints

Since agricultural IoT end devices and gateways are typically resource-constrained, it is crucial to ensure they operate efficiently. The framework tested achieved an average decision latency of 7.8 ms, resulting in a 21.5% reduction in the

energy required for each transmission. Figure 6 illustrates the breakdown of energy consumption for both static and adaptive encryption as they occur over 100 cycles of communication.

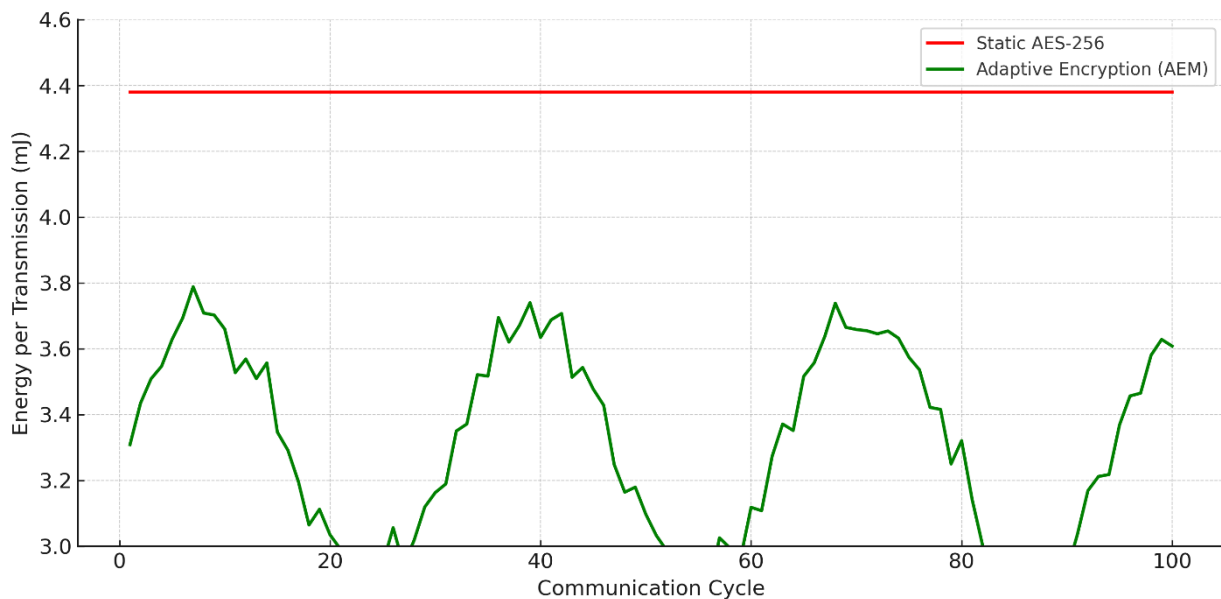


Figure 6.
Energy consumption over time: Static vs. adaptive encryption.

Due to the limited resources available in agricultural IoT systems, it is crucial to optimize their operations as efficiently as possible. The proposed framework achieved an average delay of 7.8 ms in decision-making and saved approximately 21.5% of energy per transmission. Let's compare the energy usage of static and adaptive encryption in Figure 6, which shows results over 100 communication cycles.

6.4. Robustness and Generalizability

The system performed well on the NSL-KDD dataset despite being primarily trained on the SATD dataset. Being able to apply the same ideas in different domains demonstrates that the techniques can be easily used in areas such as crop monitoring and animal farming, with minimal effort required to adapt to local rules or data patterns.

Unfortunately, this phase did not demonstrate whether the system could handle adversarial attacks. During stress testing, packet perturbation and label noise reduced detection accuracy by approximately 2 to 3%, indicating that the system is sensitive to these types of changes. The next steps should focus on strengthening the model's defenses by introducing adversarial training.

6.5. Practical Considerations and Limitations

Although it is beneficial, the framework faces certain limitations in real-world applications. For now, optimizing the LSTM-Attention model is insufficient to work effectively on microcontrollers with very low power, necessitating additional model compression. Next, AEM starts by learning through trial and error, which means some of its decisions may not be ideal yet. Some studies suggest, although this is not applicable in this case, that securing key management for adjustable encryption levels is crucial in real-world use.

Still, the fact that it is modular makes it possible to adopt it gradually. An example is that the ADE might be set up by itself on existing gateways, allowing it to be used for monitoring initially before introducing the AEM as the infrastructure evolves.

7. Future Research

Further progress will focus on enhancing the framework for adversarial situations by utilizing both adversarial training and certificates designed to prevent spoofing and evasion attacks. Additionally, we plan to apply pruning, quantization, or knowledge distillation to enhance the LSTM-Attention network, enabling it to be deployed on microcontrollers with very low power consumption. It would also be beneficial to utilize multi-agent learning, allowing different IoT devices to share and implement similar policies. The long-term stability, performance, and adaptability of the system can only be proven through official use in various types of farming environments and across different seasons.

8. Conclusion

The framework outlined in this study combines anomaly detection and adaptive encryption, leveraging AI to enhance IoT communication security in smart agriculture. The system improves its ability to identify unusual communication by combining an LSTM with an attention mechanism. Reinforcement learning in the trait helps defend the system by adjusting encryption policies based on the level of threats and the capabilities of devices at that time. The results of the experiments

show that the proposed framework outperforms traditional machine learning in both performance and cost, requiring less energy and time without compromising safety. Thanks to the attention mechanism, the model can be easily interpreted, and due to its modular construction, it is optimized for easy deployment and growth. Although simulated tests reveal that the framework is quite robust, its performance in real life and under future changes needs to be assessed in upcoming work. To conclude, this approach to handling IoT security in precision agriculture is flexible, practical, and resource-efficient, as all of these features are necessary for success.

References

- [1] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551-129583, 2019.
- [2] M. Aarif KO, A. Alam, and Y. Hotak, "Smart Sensor Technologies Shaping the Future of Precision Agriculture: Recent Advances and Future Outlooks," *Journal of Sensors*, vol. 2025, no. 1, p. 2460098, 2025.
- [3] A. Ali, T. Hussain, N. Tantashutikun, N. Hussain, and G. Cocetta, "Application of smart techniques, internet of things and data mining for resource use efficient and sustainable crop production," *Agriculture*, vol. 13, no. 2, p. 397, 2023. <https://doi.org/10.3390/agriculture13020397>
- [4] Y. Kumar and V. Kumar, "A systematic review on intrusion detection system in wireless networks: Variants, attacks, and applications," *Wireless Personal Communications*, vol. 133, no. 1, pp. 395-452, 2023.
- [5] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564-34584, 2020.
- [6] Z. C. Lipton, D. C. Kale, C. Elkan, and R. Wetzal, "Learning to diagnose with LSTM recurrent neural networks," *arXiv preprint arXiv:1511.03677*, 2015.
- [7] W. Almuseleem, "Deep reinforcement learning-enabled computation offloading: A novel framework to energy optimization and security-aware in vehicular edge-cloud computing networks," *Sensors*, vol. 25, no. 7, p. 2039, 2025. <https://doi.org/10.3390/s25072039>
- [8] A. Z. Abbasi, N. Islam, and Z. A. Shaikh, "A review of wireless sensors and networks' applications in agriculture," *Computer Standards & Interfaces*, vol. 36, no. 2, pp. 263-270, 2014.
- [9] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 1, pp. 372-425, 2024.
- [10] S. Sharma, B. Kaushik, M. K. I. Rahmani, and M. E. Ahmed, "Cryptographic solution-based secure elliptic curve cryptography enabled radio frequency identification mutual authentication protocol for internet of vehicles," *IEEE Access*, vol. 9, pp. 147114-147128, 2021.
- [11] K. Haseeb, I. Ud Din, A. Almogren, and N. Islam, "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture," *Sensors*, vol. 20, no. 7, p. 2081, 2020. <https://doi.org/10.3390/s20072081>
- [12] M. W. A. Ashraf, A. R. Singh, A. Pandian, R. S. Rathore, M. Bajaj, and I. Zaitsev, "A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things," *Scientific Reports*, vol. 14, no. 1, p. 27058, 2024. <https://doi.org/10.1038/s41598-024-78976-1>
- [13] M. N. Al-Mhiqani *et al.*, "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," *Applied Sciences*, vol. 10, no. 15, p. 5208, 2020. <https://doi.org/10.3390/app10155208>
- [14] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," *Information sciences*, vol. 239, pp. 201-225, 2013. <https://doi.org/10.1016/j.ins.2013.03.022>
- [15] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of machine learning in wireless networks: Key techniques and open issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3072-3108, 2019.
- [16] E. Tsogbaatar *et al.*, "DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT," *Internet of Things*, vol. 14, p. 100391, 2021. <https://doi.org/10.1016/j.iot.2021.100391>
- [17] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: Recent developments and challenges," *Soft Computing*, vol. 25, no. 15, pp. 9731-9763, 2021. <https://doi.org/10.1007/s00500-021-05893-0>
- [18] Y. He, P. Huang, W. Hong, Q. Luo, L. Li, and K.-L. Tsui, "In-depth insights into the application of recurrent neural networks (rnns) in traffic prediction: A comprehensive review," *Algorithms*, vol. 17, no. 9, p. 398, 2024. <https://doi.org/10.3390/a17090398>
- [19] P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, "Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks," *Information*, vol. 11, no. 5, p. 243, 2020. <https://doi.org/10.3390/info11050243>
- [20] E. Pintelas, I. E. Livieris, and P. E. Pintelas, "A convolutional autoencoder topology for classification in high-dimensional noisy image datasets," *Sensors*, vol. 21, no. 22, p. 7731, 2021. <https://doi.org/10.3390/s21227731>
- [21] A. De Santana Correia and E. L. Colombini, "Attention, please! A survey of neural attention models in deep learning," *Artificial Intelligence Review*, vol. 55, no. 8, pp. 6037-6124, 2022.
- [22] K. Mu, L. Luo, Q. Wang, and F. Mao, "Industrial process monitoring and fault diagnosis based on temporal attention augmented deep network," *Journal of Information Processing Systems*, vol. 17, no. 2, pp. 242-252, 2021.
- [23] B. Ren *et al.*, "A multi-agents deep reinforcement learning autonomous security management approach for internet of things," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25600-25612, 2024.
- [24] S. Tharewal, M. W. Ashfaq, S. S. Banu, P. Uma, S. M. Hassen, and M. Shabaz, "Intrusion detection system for industrial Internet of Things based on deep reinforcement learning," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 9023719, 2022. <https://doi.org/10.1155/2022/9023719>
- [25] A. S. Rajawat, S. Goyal, C. Chauhan, P. Bedi, M. Prasad, and T. Jan, "Cognitive adaptive systems for industrial internet of things using reinforcement algorithm," *Electronics*, vol. 12, no. 1, p. 217, 2023. <https://doi.org/10.3390/electronics12010217>