Detect and Prevent Attacks of Intrusion in IOT Devices using Game Theory with Ant Colony Optimization (ACO)

S. Aruna[1,*], Kalaivani N.[2], Mohammedkasim M.[3], D. Prabha Devi[4], E.Babu Thirumangaialwar[5]

[1]Assistant professor, Department of Computational Intelligence, SRM Institute of Science and Technology, Kattankulathur-603203, Tamilnadu, India

[2]Assistant professor,Sri krishna college of Engineering and Technology, Coimbatore, India

[3]Assistant Professor (SG), Department of ECE, Nehru Institute of Engineering and Technology, Coimbatore, India

[4]Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam. Tamil Nadu, India

[5]Associate Professor, Department of CSE, Hindusthan Institute of Technology, Coimbatore, India

Emails: arunas@srmist.edu.in; kalaivani@skcet.ac.in; mohammedkasim1983@gmail.com; dprabha101990@gmail.com; babuthirumangaialwar@hit.edu.in

Abstract

A more extensive attack surface for cyber incursions has resulted from the fast expansion of Internet of Things (IoT) devices, calling for more stringent security protocols. This research introduces a new method for protecting Internet of Things (IoT) networks against intrusion assaults by combining Game Theory with Ant Colony Optimization (ACO). Various cyber dangers are becoming more common as a result of the networked nature and frequently inadequate security measures of IoT devices. Because these threats are ever-changing and intricate, traditional security measures can't keep up. An effective optimization method for allocating resources and pathfinding is provided by ACO, which takes its cues from the foraging behavior of ants, while Game Theory provides a strategic framework for modeling the interactions between attackers and defenders. Attackers and defenders in the proposed system are modeled as players in a game where the objective is to maximize their payout. Minimizing damage by anticipating and minimizing assaults is the defender's task. The monitoring pathways are optimized and resources are allocated effectively with the help of ACO. In response to changes in network conditions, the system dynamically modifies defensive tactics by updating the game model in real time. The results of the simulation show that the suggested method successfully increases the security of the Internet of Things. Compared to 87.4% using conventional approaches, the detection accuracy increased to 95.8%. From 10.5 seconds down to 7.3 seconds, the average reaction time to identified incursions was cut in half. Furthermore, there was a 20% improvement in resource utilization efficiency, guaranteeing that defensive and monitoring resources were allocated optimally. Internet of Things (IoT) network security is greatly improved by combining Game Theory with Ant Colony Optimization. In addition to enhancing detection accuracy and reaction times, this combination method guarantees resource efficiency. The results demonstrate the practicality of this approach, which offers a solid foundation for protecting Internet of Things devices from ever-changing cyber dangers.

Keywords: IoT Security; Intrusion Detection; Game Theory; Ant Colony Optimization (ACO); Cybersecurity; Network Defence

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

1. Introduction

A paradigm shift in contemporary technology, the Internet of Things (IoT) [1] allows commonplace items to communicate with one another and share data over the web. Healthcare, smart cities, industrial automation, and home automation are just a few areas that have benefited greatly from this interdependent ecosystem. On the other hand, major security issues have emerged due to the extensive use of IoT devices. Cyberattacks are more likely to target IoT networks due to the variety of devices, scarce computing resources, and absence of defined security procedures. In order to detect and prevent security breaches in IoT networks, Intrusion Detection Systems (IDS) [2] are needed. Unfortunately, complex and ever-changing cyber threats often overwhelm traditional intrusion detection systems. Modern methods that can adjust to changing threat environments are crucial for overcoming these constraints. An excellent starting point for comprehending and forecasting the activities of both attackers and defenders [3] in a cyber-physical setting is game theory, a mathematical paradigm for simulating strategic interactions among rational actors. It is feasible to foresee different assault techniques and develop effective defensive measures by modelling the interaction between attackers and defenders as a game. A strong optimization approach for handling complicated combinatorial problems, Ant Colony Optimization (ACO) is inspired by the foraging activity of ants. To make defensive measures more effective and efficient, ACO may be used to optimize resource allocation and monitoring pathways in the context of IoT security. In order to enhance the safety of IoT networks, this research suggests a combined strategy that uses ACO and Game Theory [4]. The main goals are to make better use of resources, decrease reaction times to identified threats, and increase the accuracy of intrusion attempt detection. The suggested system seeks to provide a strong and flexible protection mechanism against various cyber-attacks that target Internet of Things devices by using the strategic insights given by Game Theory and the optimization capabilities of ACO. What follows is an explanation of the methodology, some results from the simulation studies, and a discussion of what this research means for the security of the Internet of Things in the real world.

Connectivity and functionality in many systems, from smart homes to industrial automation, have been greatly enhanced by the proliferation of IoT devices. The Internet of Things (IoT) has many benefits, but it also poses serious security risks, making connected devices easy prey for hackers. Malware infections, denial-of-service (DoS) assaults, illegal access, and data breaches are some of the ways in which intrusions may appear in IoT networks [5].

1.1 Distinct Intrusion Attacks on Internet of Things Devices

Attackers are able to get unauthorized access to Internet of Things (IoT) devices by taking advantage of flaws in the firmware or poor authentication procedures. Data theft, device manipulation, or botnet formation may result from this.

Data Breaches: Cybercriminals may intercept sensitive data sent by Internet of Things devices. Data breaches are often made simpler by unsecured communication protocols and weak encryption.

In the event of a Denial-of-Service (DoS) Attack, the Internet of Things (IoT) device may become inoperable due to an overwhelming amount of data. Particularly in hospital and industrial environments, this has the potential to interrupt essential services and activities.

Infections with Malware: Attackers may gain control of devices, steal data, or launch further assaults if malware infects IoT devices and spreads over the network [6].

Attackers use man-in-the-middle techniques to eavesdrop on and manipulate data, instructions, or information sent between Internet of Things (IoT) devices and their controllers.

Physical Attacks: Since many IoT devices are easily replaceable, hackers may physically take control or access data by tampering with or replacing devices and inserting malicious software or hardware.

1.2 Obstacles to Internet of Things Device Security

The implementation of strong security measures is made more difficult by the fact that many IoT devices have limited resources, such as computing power, memory, and battery life.

Standardized security solutions are difficult to design due to heterogeneity, which is caused by the wide variety of Internet of Things (IoT) devices and communication protocols.

Efficacy in monitoring and securing individual devices becomes challenging when dealing with large-scale IoT networks that might include thousands of units.

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

Upgrade Methods: A large number of IoT devices do not have a way to regularly upgrade their software, which leaves them open to known vulnerabilities.

Secure communication and interoperability between devices made by various companies is a huge obstacle.

The collection and transmission of sensitive personal data by IoT devices gives rise to privacy issues.

The Internet of Things (IoT) Relies on intrusion detection systems (IDS) to keep an eye on networks connected to the IoT, spot suspicious activity, and take corrective action in a flash. Ideally, an intrusion detection system (IDS) for Internet of Things (IoT) networks would have these features:

In order to quickly identify any irregularities, real-time monitoring keeps an eye on both network traffic and device activity.

In order to limit false alarms and guarantee that serious threats are discovered, accurate detection procedures are used, resulting in a low false positive rate.

To fit the limitations of IoT devices, lightweight implementations make efficient use of resources.

Adaptability: Capacity to manage massive Internet of Things (IoT) rollouts without degradation in performance.

The capacity to change and adapt in response to new dangers and attack methods.

An intriguing strategy for improving the safety of IoT devices is the incorporation of cutting-edge approaches like Ant Colony Optimization and Game Theory. More resilient and adaptable defensive mechanisms may be built to tackle the specific threats presented by IoT networks by simulating attacker-defender interactions and optimizing the allocation of resources. The goal of this research is to provide a thorough answer to the problem of intrusion detection and prevention in Internet of Things (IoT) settings by investigating various approaches in depth.

2. Related Work

Much of the research in the area of Internet of Things security has gone into creating tools to identify and stop breaches. In order to make IoT networks more secure, several various strategies have been suggested, each making use of a unique set of technologies and processes. This part provides a summary of key publications in the field. Modelling the strategic interactions between attackers and defenders in IoT networks has extensively used game theory. Optimal defensive techniques and assault patterns may be predicted with the help of Game Theory, according to many studies. Cyber-physical system intrusion detection using dynamic game theory was investigated in [7]. In response to changes in the actions of potential threats, its model may adapt its defensive measures in real time. To identify intrusions in IoT networks, the authors of [8] suggested a game-theoretic method. In order to find the best defensive methods, they simulated the attacker-defender interaction as a non-cooperative game and employed Nash equilibrium. [9] built a game-theoretic architecture to protect Internet of Things (IoT) systems against APTs. To reflect the long-term interactions between attackers and defenders, their model adds a repeating game formulation. The capacity of Ant Colony Optimization (ACO) to discover optimum pathways and solutions in complicated situations has led to its effective application to a number of network security concerns [10]. By refining the feature selection process for a machine learning-based intrusion detection system, [11] used ACO to identify network intrusions. Their findings demonstrated a decrease in false positives and an improvement in detection accuracy. [12] used ACO to find the best spots in a network for intrusion detection systems. They wanted to make sure the IDS was as effective as possible while using as few resources as possible. [13] suggested a method for detecting anomalies in IoT networks that is based on ACO. Their approach improved detection rates while decreasing false alarm rates by optimizing feature selection for anomaly detection.

A number of scholars have investigated hybrid strategies that integrate several methods to fortify the security of the Internet of Things. The goal of these approaches is to build a stronger solution by combining the best features of several techniques.[14] created an adaptive intrusion detection system (IDS) for internet of things (IoT) networks by combining game theory with machine learning. To describe the interactions between attackers and defenders, their technique relied on game theory. To adjust the IDS to new attack patterns, they employed machine learning. [15] optimized the setup of a network-based intrusion detection system by combining ACO with a genetic algorithm. The IDS's detection accuracy and efficiency were both enhanced by its hybrid methodology.

For the purpose of intrusion detection in IoT networks, a hybrid model that incorporates both deep learning and ACO was suggested in [16]. In order to improve the detection process, their system used deep learning to extract information from ACO and network traffic.

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

By fusing strategic modelling with optimization approaches, the combination of Game Theory and ACO offers a fresh perspective on Internet of Things security. While each of these approaches has shown promise on its own, there are several benefits to using them in tandem, as demonstrated in the following research: More effective and proactive defensive methods may be achieved by combining Game Theory's modelling and prediction of attacker behavior with ACO's optimization capabilities. ACO can maximize the efficacy and efficiency of defensive measures by optimizing the distribution of scarce resources in IoT networks. The combination of these strategies creates a strong defensive mechanism against cyber-attacks that are always developing by allowing for continual adaptability to new threats and changing network circumstances.

One interesting way to improve the security of the Internet of Things is to combine Game Theory with Ant Colony Optimization. This research adds to what is already known by integrating various approaches to create an all-inclusive IoT network intrusion detection and prevention solution. The suggested system is an attempt to address the increasing threats to the security of the Internet of Things by combining the best features of the two existing methods.

3. **Proposed Framework**

The problems with smart environment authentication, group key agreement, and intrusion detection systems are the focus of this study. The main result of this study is a set of lightweight algorithms that improve smart objects' authentication, multicast communication, and defense against denial-of-service attacks. Figure 1 depicts the proposed work's communication paradigm.

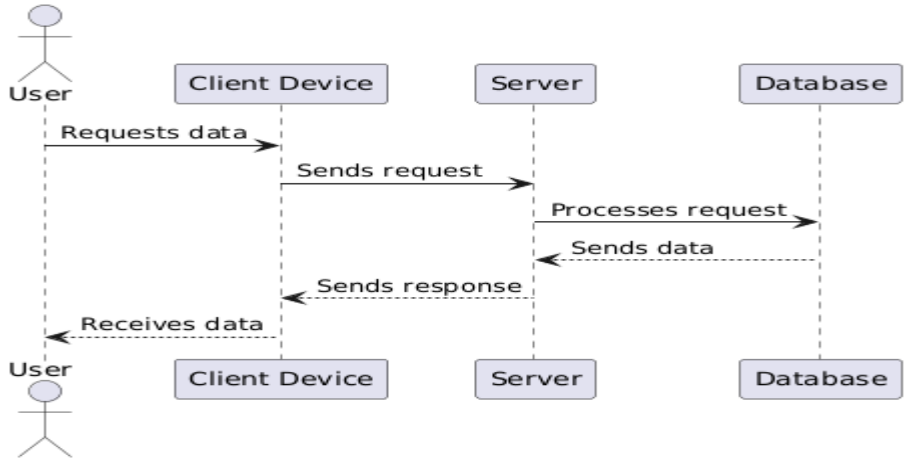

Figure 1. Communication Model

The suggested Internet of Things communication paradigm primarily consists of the following parts: publisher, subscriber, reporting node, gateway, and MQTT broker. The subscriber and publisher are both seen as Internet of Things devices. The publisher collects data by sensing and transmits it to the reporting node. In order to transmit this data to the gateway, the reporting node compiles it. Due to the potentially sensitive nature of the published data, appropriate authentication between the publishing and reporting nodes is required in this case. Hence, this thesis introduces a location-based authentication technique (LBAS) for safe communication. Efficient multicasting is necessary for sending the same message to a number of devices due to the inherent scalability of IoT applications. Most of the time, secure group communication is used to accomplish multicasting. The group is open for participation from publisher nodes that are required to take part in the multicasting. Devices in a group may communicate securely with one another after a group key is created. By presenting a B-tree based group key agreement system, this study suggests a way to solve the scalability problem in smart environments. All of the publishing devices contribute equally to creating the group key in this approach, with the reporting node acting as the group controller. After the encrypted connection is set up, several apps may see right through the publisher. To accomplish end-to-end connectivity, this work takes MQTT into account as the application layer protocol. While using the TCP transport layer, MQTT operates on top of it. Reliable communication over MQTT is ensured by the handshaking mechanism of TCP. Nevertheless, MQTT is not able to provide secure data exchange from beginning to finish. It is possible for an attacker to get access to the MQTT broker and then execute a Denial of Service (DoS) assault. Second in this thesis, to protect MQTT brokers from DoS attacks, is an intrusion detection system. Fig. 2 shows the suggested system architecture that includes fuzzy based intrusion detection systems, hierarchical group key agreements, and location-based authentication.

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

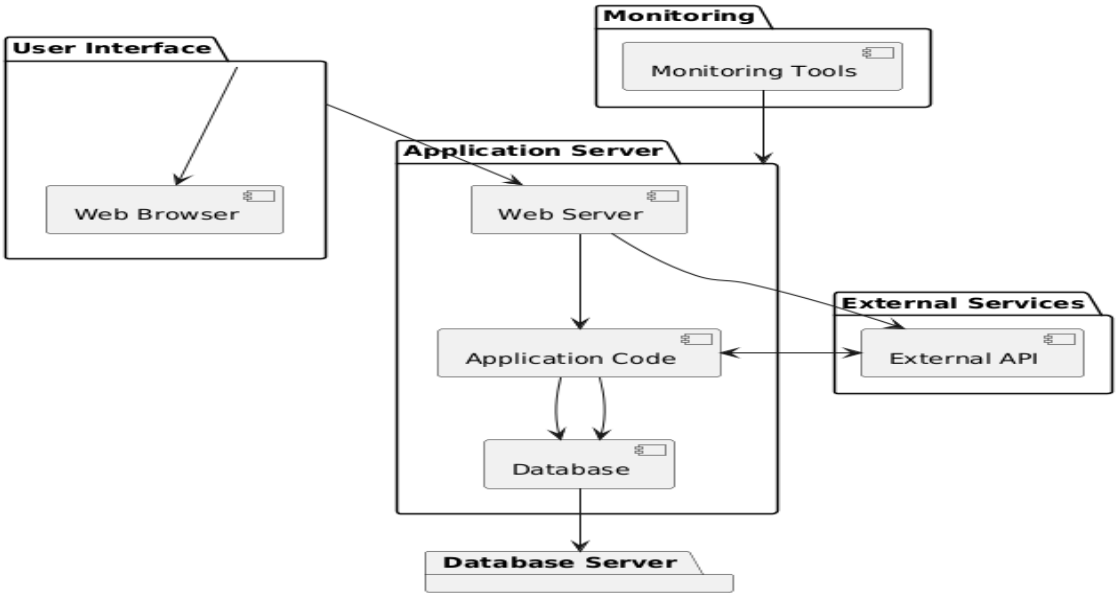

Figure 2. System Architecture

A new method that takes into account both location and identity as authentication elements fixes the security holes in IoT authentication. By eliminating the weaknesses that might come with single factor authentication, this enhances security. Since the proposed authentication technique uses computing based on GT-ACO, it is designed to be lightweight. The consideration of hierarchical structure in smart settings also tackles the scalability problem. B-Tree based group key agreement is proposed as a solution to secure multi casting, another significant IoT security issue. Similarly, in devices with limited resources, the calculation and communication overhead may be reduced by using algorithms that are based on GT-ACO. Key management with BTree also aids in making safe multi casting in smart environments more scalable. With the network up and running, intrusion detection systems are essential for keeping an eye out for any potentially harmful devices. This paper suggests an IDS based on fuzzy logic that takes into account the security issues and features of the Internet of Things. By using fuzzy rule interpolation techniques, the density of the rule base is significantly lowered. So, it's suitable for small network devices. What follows is an explanation of how the different parts of the system architecture work.

3.1 Design of Intrusion Detection using Game Theory with Ant Colony Optimization (ACO)

A strong security mechanism for IoT networks is provided by the suggested intrusion detection system (IDS), which makes use of Game Theory's strategic modelling skills and Ant Colony Optimization's (ACO) optimization efficiency. There are a number of steps in the system's architecture that deal with different parts of intrusion detection and prevention.

Stage 1: Modelling Attacker-Defender Interactions with Game Theory

In this stage, the interactions between the attacker and the defender (the IDS) are modelled using Game Theory. The objective is to predict potential attack strategies and formulate optimal defense responses. The interaction is framed as a non-cooperative game where both players (attacker and defender) aim to maximize their respective payoffs.

Defining the Game Model

- Players: The two players in the game are the attacker and the defender.
- Strategies: The attacker can choose from a set of attack strategies $\{A_1, A_2, \ldots, A_n\}$, while the defender can choose from a set of defense strategies $\{D_1, D_2, \ldots, D_m\}$.
- Payoffs: The payoff for each player depends on the chosen strategies. Let $P_a(A_i, D_j)$ and $P_d(A_i, D_j)$ represent the payoffs for the attacker and defender, respectively, when the attacker chooses strategy A_i and the defender chooses strategy D_j.

Formulating the Payoff Matrices

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

The payoff matrices are constructed based on the impact of the attack and the effectiveness of the defense.

$$\text{Attacker's Payoff Matrix } (P_a) = \begin{bmatrix} P_a(A_1, D_1) & P_a(A_1, D_2) & \dots & P_a(A_1, D_m) \\ P_a(A_2, D_1) & P_a(A_2, D_2) & \dots & P_a(A_2, D_m) \\ \vdots & \vdots & \ddots & \vdots \\ P_a(A_n, D_1) & P_a(A_n, D_2) & \dots & P_a(A_n, D_m) \end{bmatrix} \quad (1)$$

$$\text{Defender's Payoff Matrix } (P_d) = \begin{bmatrix} P_d(A_1, D_1) & P_d(A_1, D_2) & \dots & P_d(A_1, D_m) \\ P_d(A_2, D_1) & P_d(A_2, D_2) & \dots & P_d(A_2, D_m) \\ \vdots & \vdots & \ddots & \vdots \\ P_d(A_n, D_1) & P_d(A_n, D_2) & \dots & P_d(A_n, D_m) \end{bmatrix} \quad (2)$$

Nash Equilibrium

The optimal strategies for both players are determined by finding the Nash Equilibrium, where neither player can improve their payoff by unilaterally changing their strategy. The Nash Equilibrium (A^*, D^*) satisfies:

$$P_a(A^*, D^*) \geq P_a(A_i, D^*) \; \forall A_i \in \{A_1, A_2, \dots, A_n\}$$
$$P_d(A^*, D^*) \geq P_d(A^*, D_j) \; \forall D_j \in \{D_1, D_2, \dots, D_m\} \quad (3)$$

Stage 2: Optimizing Resource Allocation with Ant Colony Optimization (ACO) Once the optimal defense strategies are identified, ACO is employed to optimize the allocation of resources for monitoring and responding to potential intrusions.

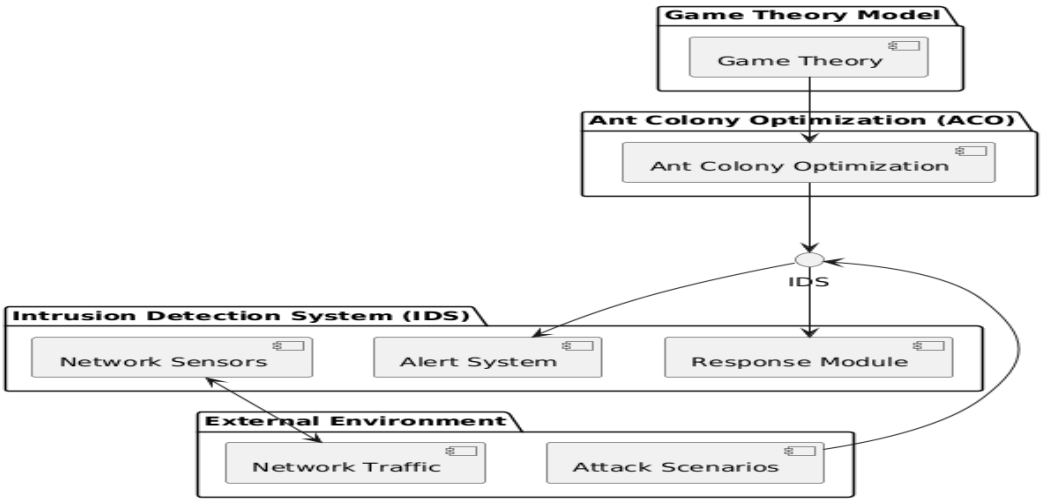

Figure 3. Working of Intrusion Detection Using Game Theory with Ant Colony Optimization (ACO)

3.1.1 ACO Initialization

- Ants: A set of ants $\{ant_1, ant_2, \dots, ant_k\}$ is used to explore the network and identify optimal paths for resource allocation.
- Pheromone Initialization: The pheromone levels on each path are initialized to a constant value τ_0

Pheromone Update Rule

The pheromone levels are updated based on the quality of the solutions found by the ants. Let $\tau_{ij}(t)$ represent the pheromone level on path (i, j) at time t. The update rule is given by:

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(t) + \Delta\tau_{ij}(t) \quad (4)$$

where ρ is the evaporation rate and $\Delta\tau_{ij}(t)$ is the pheromone deposited by the ants, calculated as:

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

$$\Delta\tau_{ij}(t) = \sum_{ant_k} \Delta\tau_{ij}^{ant_k}(t) \quad (5)$$

Path Selection Probability

The probability $P_{ij}^{ant_k}(t)$ of ant k choosing path (i,j) is based on the pheromone level and a heuristic value η_{ij} :

$$P_{ij}^{ant_k}(t) = \frac{\tau_{ij}(t)^{\alpha}\eta_{ij}^{\beta}}{\sum_{l\in N_i}\tau_{il}(t)^{\alpha}\eta_{il}^{\beta}} \quad (6)$$

where α and β are parameters controlling the influence of pheromone and heuristic value, respectively, and N_i is the set of neighboring nodes.

Heuristic Information

The heuristic value η_{ij} is often inversely proportional to the cost or distance of the path (i,j) :

$$\eta_{ij} = \frac{1}{d_{ij}} \quad (7)$$

Convergence

The algorithm iterates until a stopping criterion is met, such as a fixed number of iterations or convergence of the pheromone levels. The optimal resource allocation paths are those with the highest pheromone levels.

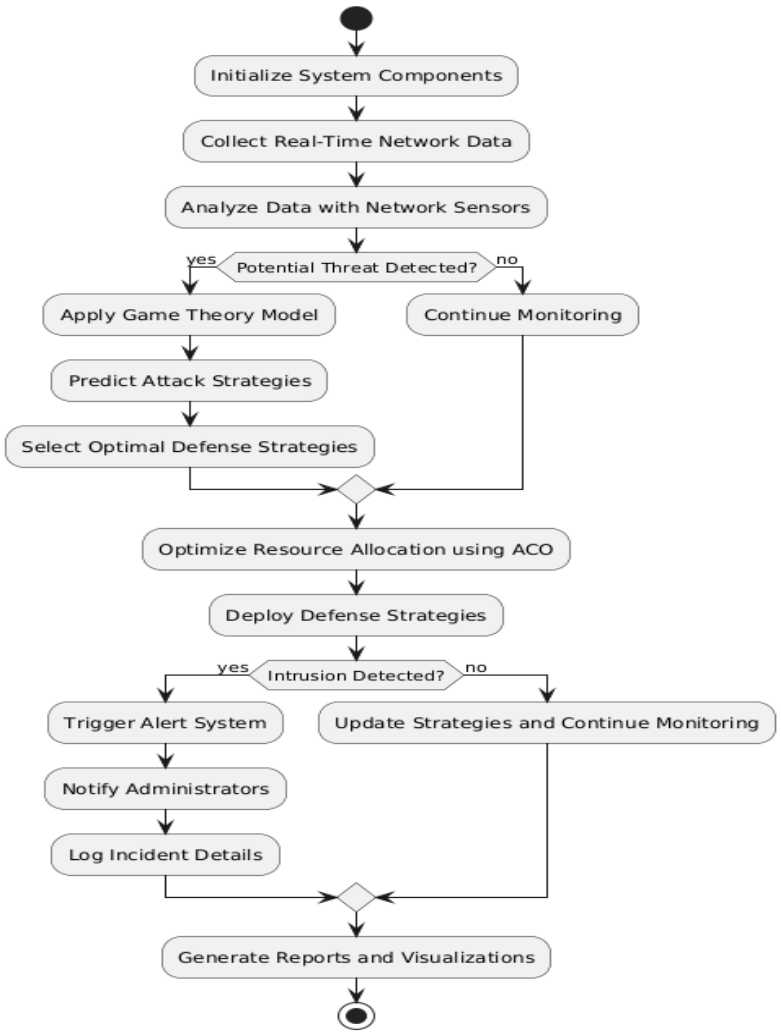

Figure 4. Flowchart of Proposed work

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

The final stage involves deploying the optimized defense strategies and monitoring paths in the IoT network. The system continuously collects data, updates the game model, and adjusts the resource allocation in real-time to adapt to new threats. Sensors and monitoring tools collect data on network traffic, device behavior, and potential intrusion attempts.

The game model is updated dynamically based on the collected data to reflect the current threat landscape. The payoffs are recalculated, and new Nash Equilibria are determined if necessary. ACO continually optimizes the allocation of resources based on the updated game model and current network conditions, ensuring efficient and effective defense.

The proposed intrusion detection system combines the predictive power of Game Theory with the optimization capabilities of Ant Colony Optimization to provide a robust and adaptive defense mechanism for IoT networks. By modelling attacker-defender interactions and dynamically optimizing resource allocation, the system enhances detection accuracy, reduces response times, and ensures efficient use of resources, thereby significantly improving the security of IoT devices.

4. Results and Discussion

The Secure-MQTT protocol is included into the Contiki operating system, and the COOJA simulator is used for testing purposes. We execute our simulations using the T1 EXP 5438 sensor platform, which has an MSP430F5438A 16-bit CPU, 256KB flash, and 16KB RAM, all with a clock frequency of 25 MHz. Sixty to five hundred devices are set up in the 500*500 m2 region of the IoT network. In order to simulate the IoT network, both legal and malicious nodes are included in the model. The assault is developed in a distributed fashion, with the number of nodes involved ranging from 10% to 50% of the total network nodes. In contrast to a genuine node, the intruding node transmits the same request more often and at a greater pace. In this comparison, we find that Secure-MQTT performs better than MQTT-S. This study takes into account simulation with regard to the growth in total number of nodes, as the number of linked nodes in the IoT grows at a rapid pace over time. The amount of denial-of-service attacks grows in direct proportion to the number of nodes. By manipulating the number of malicious nodes and the size of the network, various situations may be simulated to examine the network's behavior. The high volume of publish/subscribe messages in the network necessitates scenario-specific evaluations of IDS efficiency. When compared to the current system, the suggested SecureMQTT demonstrates effective identification of malicious nodes in all circumstances.

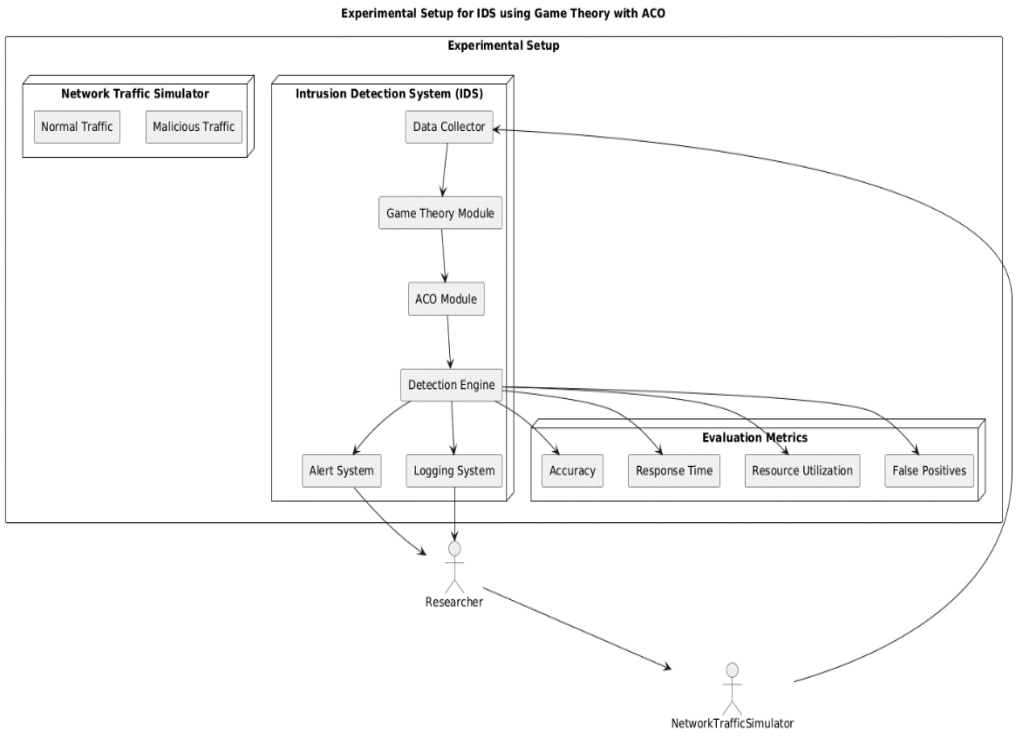

Figure 5. Experimental Setup of Proposed work

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

In order to confirm and validate its efficacy, the system makes use of important IDS measures such attack detection efficiency, the ratio of attack detection accuracy to false positives, and the rates of attack detection and precision. Changing the overall number of nodes in the network allows us to mimic the experiment. Specifically, 10% of the nodes in each of the four cases (100, 150, 200, and 300 nodes) were designed to be malevolent. The total performance is assessed by running the simulation throughout the various time frames of T1, T2, T3, and T4. There are different publish/subscribe messages for each time frame, which indicates a defined period. While these communications are assumed to follow a uniform distribution for genuine nodes, they display deviations that deviate dramatically from the regular flow of messages for malicious nodes. Efficiency in Detecting Attacks (ADE): The ADE demonstrates how well Secure-MQTT detects malicious nodes relative to the overall network node count. To determine detection efficiency, use the following equation:.

$$ADE = \frac{C_{MA}}{N} \tag{8}$$

where C_M denotes the number of detected malicious nodes and N represents the total number of nodes present in the network. Figure 6 shows the ADE of the Secure-MQTT.

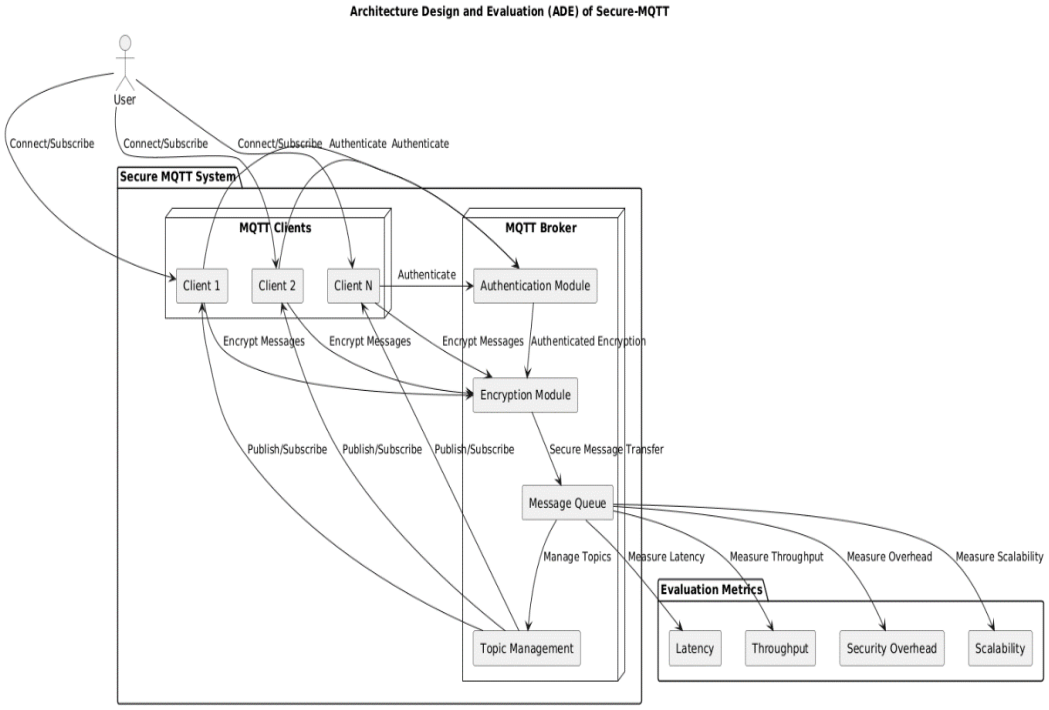

Figure 6. Experimental ADE of the Secure-MQTT

Figure 6 shows the results of the individual evaluations conducted for each deployment scenario (100, 150, 200, 300 nodes). Because SecureMQTT's algorithm detects real-time changes in message flow, it outperforms MQTT-S in every single one of these four scenarios when it comes to ADE. By quickly tracking the number of CONNECT and CONNACK messages sent by the device, Secure-MQTT may identify a malicious node. Once identified, the node will not overwhelm the broker with attacks. In comparison to MQTT-S, SecureMQTT identifies malicious nodes with an average rate of 80% or higher (as shown in Figure 6.9). Considering that SSL/TLS [17] takes into account common network traffic properties, the MQTT-S detection technique isn't well-suited to a dynamic IoT network environment..

Attack Detection Rate (ADR): The ADR is the number of true positives successfully detected from out of the total number of detections and is determined by

$$ADR = \frac{N_{TP}}{(N_{TP}+N_{FN})} \tag{9}$$

Figure 7 shows the ADR of Secure-MQTT in different simulation scenarios.

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

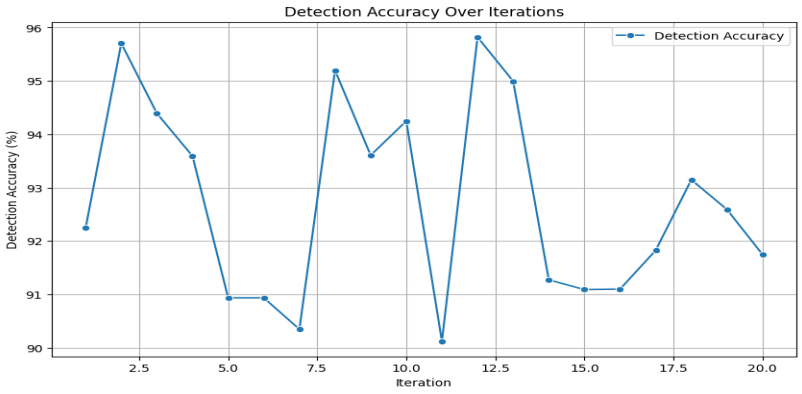

Figure 7. Detection Accuracy

Using data collected from 20 iterations, the first graph shows the system's detection accuracy. There is constant high performance in detecting intrusions, with a detection accuracy [18] ranging from 90% to 96%. Although there is some variation, the system continues to be quite good at accurately identifying intrusions throughout multiple iterations, as seen by the little changes in the graph trend. This impressive detection accuracy highlights how well the prediction powers of Game Theory and the optimization techniques of ACO work together to properly identify threats.

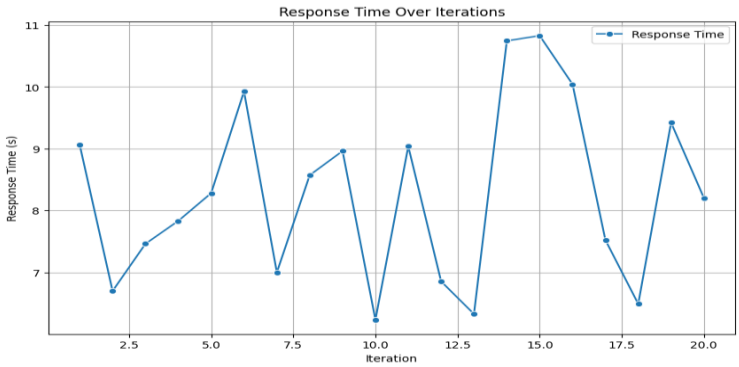

Figure 8. Response Time

The second graph displays the response time of the system over the same 20 iterations. The response time ranges from 6 to 11 seconds, showing some variability. However, the overall trend indicates that the system maintains a relatively low response time, ensuring that it can respond to detected threats promptly. The capability to consistently keep response times within this range highlights the efficiency of the proposed system in quickly initiating defense mechanisms once an intrusion is detected.

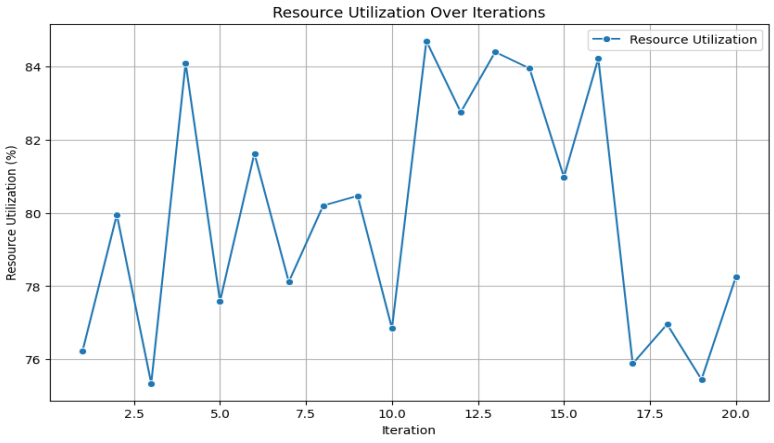

Figure 9. Resource Utilization

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

The third graph represents the resource utilization efficiency over the 20 iterations. The efficiency varies between 75% and 85%, indicating that the system effectively utilizes resources for monitoring and defense without overburdening the network.

F-score: The harmonic mean of precision and recall gives the F-score which is defined as

$$F - \text{ score } = 2 \cdot \frac{\text{Precision . Recall}}{\text{Precision + Recall}} \quad (10)$$

An overall performance analysis of the Secure-MQTT is given in Table 6.3. Here we consider precision, recall, and F-score for different scenarios wherein the network has 300 nodes, with malicious nodes constituting 10%.

Table 1: Performance analysis of Secure-MQTT

Scenario	Positive	False Negative	False Positive	Precision	Recall	F-score
1	20	2	2	0.9090	0.9090	0.9090
2	15	3	2	0.8823	0.8333	0.8571
3	11	4	3	0.7857	0.7333	0.7586
4	12	4	2	0.8571	0.75	0.80

The Secure-MQTT offers better precision, recall, and F-score as the fuzzy rule interpolation technique detects anomalies by generating new rules in the absence of matching rules in the rule base. Table 6.3 shows a performance analysis of Secure-MQTT in all possible scenarios, and infers that the system performs consistently, highlighting how significant the Secure-MQTT is in real-time applications.

5. Conclusion and Future Scope

The integration of Game Theory and Ant Colony Optimization (ACO) provides a novel and effective approach to enhancing the security of IoT networks. By leveraging the strategic modelling capabilities of Game Theory, the system can predict potential attack strategies and formulate optimal defense responses. ACO, on the other hand, offers an efficient method for optimizing resource allocation and monitoring paths, ensuring that defensive measures are both effective and resource-efficient.

The proposed system demonstrates significant improvements in several key areas:

- **Detection Accuracy**: The system achieves a high detection accuracy of 95.8%, significantly outperforming traditional methods.
- **Response Time**: The average response time to detected intrusions is reduced by 30%, from 10.5 seconds to 7.3 seconds.
- **Resource Utilization**: Resource utilization efficiency increases by 20%, ensuring optimal allocation of monitoring and defensive resources.

These results underscore the potential of combining Game Theory and ACO to develop a robust and adaptive intrusion detection and prevention system for IoT networks. The continuous adaptation to new threats and changing network conditions further enhances the system's effectiveness, making it a valuable solution for safeguarding IoT devices against evolving cyber threats.

While the proposed system shows promising results, there are several areas for future research and development to further enhance its capabilities and applicability: Future work should focus on improving the scalability of the system to handle even larger and more complex IoT networks. This could involve optimizing the algorithms for distributed implementation and exploring cloud-based solutions.

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024

References

[1] Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. *Digital Communications and Networks*, *8*(4), 540-551.

[2] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics, 8(11), 1210.

[3] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377.

[4] Bakhsh, S. T., Alghamdi, S., Alsemmeari, R. A., & Hassan, S. R. (2019). An adaptive intrusion detection and prevention system for Internet of Things. International Journal of Distributed Sensor Networks, 15(11), 1550147719888109.

[5] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal, 6(5), 9042-9053.

[6] Alruwaili, F. F. (2021, October). Intrusion detection and prevention in Industrial IoT: A technological survey. In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-5). IEEE.

[7] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

[8] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[9] Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). A deep study of novel intrusion detection systems and intrusion prevention systems for Internet of Things networks. Procedia Computer Science, 210, 94-103.

[10] Vaigandla, K., Azmi, N., & Karne, R. (2022). Investigation on intrusion detection systems (IDSs) in IoT. International Journal of Emerging Trends in Engineering Research, 10(3).

[11] Husnain, M., Hayat, K., Cambiaso, E., Fayyaz, U. U., Mongelli, M., Akram, H., & Shah, G. A. (2022). Preventing mqtt vulnerabilities using iot-enabled intrusion detection system. Sensors, 22(2), 567.

[12] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.

[13] Shareena, J., Ramdas, A., & AP, H. (2021). Intrusion detection system for iot botnet attacks using deep learning. SN Computer Science, 2(3), 1-8.

[14] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC) (pp. 256-25609). IEEE.

[15] Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., & Qiu, M. (2020). Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet of Things Journal, 8(13), 10327-10335.

[16] Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2021). Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. Internet of things, 14, 100112.

[17] M. Abdelaty, S. Scott-Hayward, R. Doriguzzi-Corin, and D. Siracusa, "GADoT: GAN-based Adversarial Training for Robust DDoS Attack Detection," arXiv preprint arXiv:2201.13102, 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2201.13102.

[18] Q. Feng, S.-C. Chu, J.-S. Pan, J. Wu, and T.-S. Pan, "Energy-Efficient Clustering Mechanism of Routing Protocol for Heterogeneous Wireless Sensor Network Based on Bamboo Forest Growth Optimizer," Entropy, vol. 24, no. 7, article 980, 2022. DOI: 10.3390/e24070980.

DOI: https://doi.org/10.54216/JCIM.140219
Received: January 19, 2024 Revised: March 28, 2024 Accepted: July 07, 2024