NEW DISTRIBUTED ARCHITECTURE BASED ON MULTI AGENT SYSTEMS FOR THE CYBERSECURITY OF THE INTERNET OF THINGS

RACHID HDIDOU[1], MOHAMED EL ALAMI[2]

[1,2]ERMIA Team, Department of Mathematics and Computer Science, National School of Applied Sciences of Tangier, Abdelmalek Essaadi University, Morocco

E-mail: [1]hdidou.rachid@etu.uae.ac.ma, [2]m.elalamihassoun@uae.ac.ma

ABSTRACT

The Internet of Things has become one of the technologies that receives great attention from researchers due to its significant impact in various fields. To secure the Internet of Things, many presented research works attempted to propose effective and suitable solutions addressing the features and characteristics of this technology. Despite all the proposed solutions, centralization remains one of the problems that affect the speed, efficiency, and accuracy of these solutions. Distribution can provide faster and more accurate solutions and avoid complete system downtime if a system's node encounters a problem. This is our goal in this research work. In this scientific paper, a distributed architecture based on multi-agent systems has been proposed for the cybersecurity of the Internet of Things. Our architecture presents itself as an exhaustive solution as it ensures three main tasks: proactive monitoring, anomaly detection, and swift response to emerging threats.

Keywords: *Multi-Agent Systems, Cybersecurity, Internet of Things, Intrusion Detection, Distributed intelligence*

1. INTRODUCTION

Recently, the world has witnessed an unparalleled speed in the use of modern technologies in various aspects of life. One of the most significant technologies is the Internet of Things, which has found application in most fields such as sports, medicine, military, and other fields. The focus on using IoT technologies is attributed to their efficacy in solving time, speed, and accuracy problems. Thanks to IoT, we are now able to discuss concepts such as smart homes, smart cities, and other practical applications of IoT technology.

The Internet of Things refers to a network of devices or objects capable of collecting, analyzing, and exchanging data through sensors, software and applications without human involvement. When discussing "things" in the context of IoT, it includes devices, machines, animals, vehicles, and even humans.

As the Internet of Things is essentially an information network built on sensors, software and protocols, its reliable use across various fields relies heavily on the level of protection and security it possesses. Despite the substantial progress and widespread adoption of IoT applications, the persistent security challenge hinders its widespread implementation across all sectors. This challenge is rooted in the unique architecture of IoT networks compared to traditional ones and in the inherent diversity of its devices, leading to the variety and scale of cyberattacks targeting this technology.

Some of the most crucial technologies used in securing IoT networks are Intrusion detection systems, risk management systems, information encryption systems, and others. Despite the numerous proposed solutions for IoT security, whether traditional or utilizing artificial intelligence techniques, centralization remains one of the major problems faced by most of the proposed solutions. The impact of centralization manifests in intrusion and tampering detection times, the energy consumption of the central node, and the overall system performance. If a central unit fails, the entire system is affected, highlighting the need for solutions that rely on distribution.

Several studies have been presented in the context of Internet of Things (IoT) security, including intrusion detection systems, SIEMs, and authentication and encryption algorithms. However, most of these studies present isolated security components, which highlights the incompleteness of these solutions.

The motivation for our work stems from the need for a comprehensive security solution that addresses all security tasks, along with the need for a distributed and intelligent solution for IoT environments. Our approach distinguishes itself from other research by its originality and comprehensiveness, as our architecture integrates all security operations: authentication, traffic monitoring, anomaly detection, vulnerability management, event correlation, intelligent event analysis, and decision-making. Additionally, our solution sets itself apart through its layered structure and the integration of various types of autonomous and intelligent agents, each responsible for performing a specific security task.

In our previous work [1,2] and during the preparation of this research, we observed that most current security solutions fail to keep pace with the rapid evolution of IoT technology. These solutions suffer from several limitations, such as the inability of standard approaches to address the increasing sophistication and frequency of cyberattacks targeting IoT environments, especially as these attacks have become more efficient and intelligent. Another major issue is the centralization of tasks in security systems based on traditional artificial intelligence, which places a significant load on the central node, thereby affecting the speed and performance of security operations.

Based on the stated problems, the following research questions can be posed:

- How can a security architecture for the Internet of Things be built using distributed artificial intelligence?
- How can the characteristics of multi-agent systems be leveraged to present a security architecture for IoT environments?
- How can the principles of distribution, intelligence, and collaboration enhance the security of IoT systems?

The primary aim of this research is to propose a new architecture based on multi-agent systems to protect the Internet of Things technology against cyberattacks.

The rest of our article will be organized as follows: the second section will provide a background of the key terms of our article, such as Internet of Things, Cybersecurity, and Multi-Agent Systems. Following this, a literature review will be presented in the third section. Afterward, the fourth section will introduce the proposed architecture. Subsequently, we will discuss our architecture in the fifth section. Finally, the sixth section will conclude with a summary and outline of future work.

2. BACKGROUND

2.1 Internet of Things (IoT)

The Internet of Things is one of the key technologies in the modern technological revolution. The term ‘Internet of Things’ was proposed by Kevin Ashton in 1999 [3]. It refers to a network of interconnected objects that can communicate without human intervention, each possessing its unique identifier.

The functioning of this technology is based on four elements:

Firstly, there are the sensors, essential for collecting data from their environment. Secondly, the gateways serve as links between the sensors and external networks. Thirdly, there are the Clouds/Internal servers, responsible for storing the collected data. Finally, the visualization platforms (Desktop Applications, Mobile Applications, or websites…). These platforms are the tools for visualizing the results of the analysis and processing of the collected data, facilitating the right decision-making.

The architecture of the Internet of Things consists of three layers [4]:

- **Perception Layer:** It includes the physical devices and sensors, which collect data from their environment.
- **Network Layer:** this layer is responsible for transmitting the data collected from the previous layer to the Cloud/Internal server.
- **Application Layer:** this layer aims to analyze and process the collected data to enable decision-making and device control by the administrator.

2.2 Cybersecurity (CS)

The term "Cybersecurity" has emerged as one of the most widely used terms recently in the field of information technology. According to (ITU, 2009), "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, application, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment"[5].

Cybersecurity has three main objectives [5]:

- **Confidentiality:** It guarantees that data is accessible only to authorized individuals or systems.
- **Integrity:** It guarantees that data cannot be modified during transfer between the source and destination. Integrity may also include authenticity and non-repudiation.
- **Availability:** It guarantees that systems, applications, networks, and data are accessible to authorized individuals and consistently available.

In the context of cybersecurity and to protect networks, systems, and data against cyberattacks, there are several methods and techniques implemented, such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Encryption, Security Information and Event Management (SIEM) Systems, and other techniques.

2.3 Multi-Agent Systems (MAS)

To define Multi-Agent Systems, we will first start by defining the term Agent which forms the basis of all Multi-Agent Systems. In the field of computer science, according to Wooldridge (1999), "An Agent is a computer system that is situated in the same environment, and that is capable of autonomous action in this environment to meet its design objectives" [6].

The role of an agent within an environment is to perform a specific task based on the context of its use and the usage environment to solve a given problem. For this purpose, an agent must possess certain characteristics [7] such as Autonomy which refers to its ability to function independently. Proactivity indicates its initiative, and sociability which facilitates interaction with other agents. The sociability of an agent leads to the need for Multi-Agent Systems.

A Multi-Agent System (MAS) comprises a collection of agents that communicate and interact within a shared environment to achieve specific objectives and thereby resolve a given problem. Multi-agent systems have several advantages due to their characteristics, these include:

- **Distribution:** The basic principle of multi-agent systems is distribution, i.e. data collection, processing, and decision-making are distributed among the agents of the multi-agent architecture.
- **Interaction and communication:** agents of a multi-agent system can interact and communicate with each other to exchange the necessary information to solve the given problem.
- **Adaptability and Flexibility:** Multi-agent systems can adapt to dynamic environments and are flexible with the changes established in these environments.

Multi-agent systems are implemented in several applications domain to solve several types of problems [7][8] such as the medical and healthcare domain [9][10], the robotics domain [11], the smart grid domain [12], the supply chain domain [13], the energy domain [14], the educational domain and E-Learning systems [15][16], the network and security domain [17] and other domains…

These applications show the importance and performance of distribution-based systems as an effective solution for several types of problems.

3. LITERATURE REVIEW

The Internet of Things has recently experienced a wide diffusion and use in several areas. This diffusion has led to an increasing use of connected devices, which consequently gives a remarkable increase in the number and types of cyberattacks [18]. This implies the need to find serious and homogeneous solutions with the characteristics of the Internet of Things, thus overcoming some of the challenges faced by the use of this technology and ensuring the general principles of security of computer systems [19][20].

Several research works attempted to propose effective security solutions that are consistent with the infrastructures of the Internet of Things. These solutions have been divided into several research axes.

The first direction of research is intrusion detection systems, which are considered among the most commonly proposed tools by researchers in the field of security of the Internet of Things [1][2]. Several techniques and methods are used to propose and implement solid IDS solutions compatible with the nature of IoT applications and networks. On the one hand, there are IDSs based on standard techniques such as: in [21] Raza et al. proposed a real-time IDS for intrusion detection in IoT networks, specifically to detect the two types of attacks: Sinkhole and selective Forwarding. This IDS is named SVELTE and is based on the idea that all the nodes in the network collect and send the information to the router, which analyses the collected traffic to detect intrusions. In another work, Lee et al. [22] proposed an IDS for the IoT. This IDS is based on a physical concept, which involves calculating the energy consumption for each node of the network under normal conditions and this calculated value will be considered as the normal state threshold, and when this value changes, IDS classifies this node as a malicious node and removes it from the routing table in 6LoWPAN. On the other hand, there are IDS solutions that are based on artificial intelligence techniques: In [23] Verma et al. proposed an architecture of a NIDS based on Ensemble Learning for IoT. The proposed IDS is named ELNIDS, and its architecture contains four classifiers which are: Boosted Trees, Bagged Trees, Subspace Discriminant, and RUS Boosted Trees. In another work, in 2022, Faysal et al. [24], introduced a design of an IDS for IoT networks. The proposed model consists of two main parts: the first involves feature selection using the Random Forest (RF) algorithm and the second focuses on classification using the Extreme Gradient Boosting (XGB) technique.

The second direction focuses on Security Information and Event Management (SIEM). A SIEM is a security system that collects and analyzes security events generated by applications or devices within a network. The main tasks of a SIEM can be summarized as Data collection, Security event retention, Monitoring and alerting, Threat detection, Forensic analysis, and Incident management. In 2022, Abdalrahman Hwoiji et al. [25] proposed a SIEM architecture for IoT environments, specifically for smart cities. The proposed architecture consists of three parts: the first is the intelligent environment, the second is the SIEM, and the third is the Security Operations Center (SOC). Devices in the intelligent environment generate event logs, which are then collected by the SIEM and transmitted to the SOC, enabling the detection and management of security incidents. In 2018, P. Messa et al. [26] proposed a SIEM system for the security of the Internet of Things (IoT). The proposed solution is a distributed system based on Blockchain technology, with Blockchain playing the role of securely and distributively storing security events. The system implementation was carried out via Ethereum. The main objective of the proposed system is to ensure: resilience, trust-orientation, auditability, and scalability. In 2020, V. Botello et al. [27] proposed a SIEM framework for the security of Smart City services. The proposed framework (named BlockSIEM) is a distributed system based on Blockchain. The basic idea behind the proposed solution is to first collect security events from the IoT services of the smart city. Secondly, the system securely and distributively stores the events using Blockchain registers. Finally, the system detects and prevents cyberattacks.

The third direction is cryptography, which focuses on the encryption and decryption of data during communication between computing devices. Several protocols and algorithms have been proposed to enhance the security of data in Internet of Things (IoT) networks. In 2015, P. Gaikwad et al. [28] proposed an authentication system for the Internet of Things, specifically for smart homes. The proposed smart home scheme consists of three parts: an Online server, a Smart Central Controller, and a Small Microcontroller. As mentioned in the title, the proposed system is based on three levels of authentication: the first level contains the steps for user login to monitor and control the smart home. The second level focuses on user authentication steps, and finally, the third level involves the process of using keys and managing tickets to secure the user's session. In 2017, Usman et al. [29] proposed a Lightweight Encryption Algorithm (named SIT) designed for the security of the Internet of Things. The proposed algorithm is based on a hybrid architecture, consisting of a Substitution-Permutation network and Feistel architecture. SIT is a block cipher with a 64-bit key and only five rounds of processing. According to the researchers, the proposed work is more suitable for IoT applications as it ensures security and reduces energy consumption. In 2021, K. Sowjanya et al. [30] proposed a lightweight authentication scheme based on Elliptic Curve Cryptography for the security of the Internet of Medical Things. The proposed scheme ensures mutual authentication between the patient and the medical service, as well as a reduction in computational overhead. According to the authors, the proposed protocol is more robust and better suited for IoMT applications compared to previous techniques and methods.

Centralized security solutions are increasingly inadequate for managing IoT security due to challenges related to speed, scalability, and performance. Our motivation for this research stems from the urgent need to propose intelligent, distributed, scalable, and adaptive solutions for securing IoT environments.

To lay a solid foundation for our research, we selected three key research avenues for our literature review: first, cryptography, to analyze the current state of data encryption and authentication mechanisms for IoT devices, second, Intrusion Detection Systems (IDS), to evaluate traffic monitoring and intrusion detection processes, and third, Security Information and Event Management (SIEM) systems, to explore additional security tasks such as analysis, correlation, and decision-making.

This selection enabled us to identify, analyze, and assess existing security challenges in previous solutions, allowing us to propose more efficient approaches for IoT security.

The analysis of the literature review presented here shows that several relevant research studies have been conducted in the context of Internet of Things (IoT) security, including work on Intrusion Detection Systems (IDSs), Security Information and Event Management (SIEM) systems, as well as encryption and authentication mechanisms. Although these studies offer valuable insights and solutions, they have certain weaknesses and limitations, such as focusing on isolated security tasks and relying on centralized solutions. These factors negatively affect the speed, scalability, and overall performance of IoT security systems.

Our work addresses these limitations by proposing distributed architecture based on multi-agent systems for securing IoT environments. This approach tackles the limitations of previous work by integrating several points: First, it introduces the concept of distributed security tasks, which mitigates the issues associated with centralized approaches. Second, it integrates multiple security tasks into a unified solution, overcoming the fragmentation seen in isolated task-specific approaches. Finally, by implementing multi-layered architecture and leveraging various types of agents, our solution improves the maintainability, speed, and scalability of IoT technology security solutions.

4. PROPOSED ARCHITECTURE

4.1 Motivation of Proposed Architecture

Most of the research in IoT security proposes solutions based on centralization. Centralizing solutions presents several weaknesses, including the time required to detect vulnerabilities and intrusions and the significant pressure on the central node of the system. Furthermore, the centralization issue ties the entire system's operation to the central node. If this node fails, the entire system will collapse. Other important issues must be considered, such as the lack of exhaustiveness and the security of the proposed protection system itself. All these issues highlight the need for solutions based on distribution, integrity, and the security of the proposed system itself.

4.2 Proposed Architecture

Our work aims to propose a distributed architecture based on multi-agent systems for the cybersecurity of the Internet of Things. Our architecture can be considered a comprehensive solution for IoT security due to several key features: First, the proposed architecture will ensure three main tasks: proactive monitoring, anomaly detection, and rapid response to emerging threats. Additionally, it will guarantee the three fundamental principles of computer system security: confidentiality, availability, and integrity. Moreover, it will ensure the security of the security system itself. Furthermore, the proposed architecture is based on the principle of collaboration among agents, meaning that the tasks of the proposed security system are carried out in an interactive, collaborative manner by the agents of the architecture. Finally, this architecture will be structured in layers, allowing for clear and efficient management of our security system.

The originality of the proposed architecture stems from principles derived from military theory and the art of warfare. These principles include the principle of the cyber guerrilla to ensure agile defence, the principle of dividing the team into squads to ensure improved responsiveness, the principle of deception and disinformation tactics to thwart attacks, the principle of defence in depth strategy, the principle of espionage and infiltration to gather intelligence on threats, the principle of commando operations to provide rapid and targeted responses, the principle of deployment as scouts to ensure proactive intrusion detection, the principle of bypass strategy, and finally, the principle of deploying specialized forces for special missions to address specific threats with speed and effectiveness.

4.2.1 The agents of our architecture

The proposed architecture is a distributed architecture based on multi-agent systems for cybersecurity for the Internet of Things. Our proposed architecture consists of several types of agents:

- **Security Management Agent (SMA):** Coordinates and oversees the entire Multi-Agent System, managing security policies, agent monitoring, and security alerts.
- **Traffic Monitoring Agent (TMA):** Monitors the network traffic of IoT devices to detect anomalies and analyzes communication patterns to identify suspicious behaviors or attacks.
- **Authentication and Authorization Agent (AAA):** Manages the authentication mechanisms for IoT devices, ensures appropriate authorization for access to network resources, and implements identity management mechanisms.
- **Intrusion Detection Agent (IDA):** Uses intrusion detection algorithms to identify malicious activities, generate alerts, and trigger automated responses in case of threats.
- **Vulnerability Management Agent (VMA):** Identifies and monitors potential vulnerabilities in IoT devices and proposes patches or countermeasures to mitigate risks.
- **Artificial Intelligence Agent (AIA):** Uses machine learning techniques to detect abnormal behaviors, evolves in threat detection, and adapts to new forms of attacks.
- **Incident Response Agent (IRA):** Implements response actions upon incident detection, such as isolating compromised devices, blocking malicious traffic, and restoring secure configurations.
- **Event Correlation Agent (ECA):** Correlates security events from different information sources and helps distinguish real attacks from false alerts by aggregating data from multiple agents.

4.2.2 The agents of our architecture

Our proposed architecture, based on Multi-Agent Systems, includes several agents as mentioned above, with each type of agent assigned a specific task. Some tasks require collaboration between multiple agents. Below, we present our architecture along with the interactions between the different types of agents in the proposed architecture:

The Traffic Monitoring Agents (TMA) send reports on detected anomalies and traffic statistics to the Central Node Agent (SMA) (1). Furthermore, the Intrusion Detection Agents (IDA) share intrusion alerts with SMA for response coordination and with the Artificial Intelligence Agent (AIA) for further analysis (2). In addition, the Vulnerability Management Agents (VMA) communicate with SMA to report identified vulnerabilities and with AIA for detailed analysis (3). The Authentication and Authorization Agent (AAA) reports authentication and authorization activities to SMA (4). Moreover, the Incident Response Agents (IRA) communicate with the Traffic Monitoring Agents (TMA), Vulnerability Management Agents (VMA), and Authentication and Authorization Agent (AAA) to take action in response to a detected incident (5). Additionally, the Traffic Monitoring Agents (TMA) may share information among themselves on surveillance activities, traffic patterns, and detected anomalies (6). The Event Correlation Agent (ECA) communicates with all types of agents to receive event data and provide an overall view of security (7). Finally, the Vulnerability Management Agents (VMA) may share information about detected vulnerabilities and proposed patches among themselves to ensure continuous and collaborative improvement of the proposed system (8).

Figure 1 illustrates our proposed system architecture:

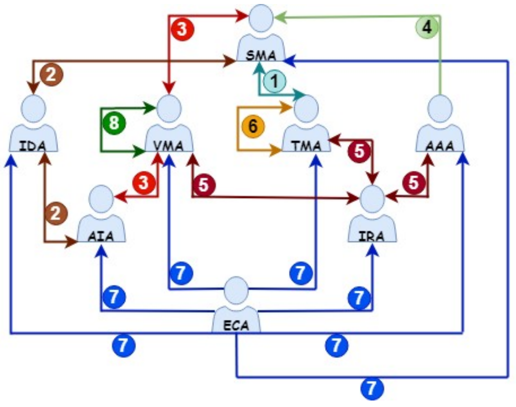

Figure 1: Proposed System Architecture

4.2.3 Communication and Collaboration among Agents in the Proposed Architecture

The agents in our proposed architecture are responsible for communicating and collaborating to build a more secure system, with enhanced confidentiality, faster threat detection and incident response. In the proposed architecture, the following collaborations will take place:

- Collaboration between the Traffic Monitoring Agents (TMA) and Intrusion Detection Agents (IDA) to monitor traffic and detect intrusions[(1)].
- Collaboration between the Vulnerability Management Agents (VMA) and Traffic Monitoring Agents (TMA) to share information about vulnerabilities[(2)].
- Collaboration between the Intrusion Detection Agents (IDA) and Incident Response Agents (IRA) for a collaborative response to incidents[(3)].
- Collaboration between all types of agents and the Event Correlation Agents (ECA) for event correlation[(4)].
- Collaboration between all types of agents and the Artificial Intelligence Agent (AIA) for collaborative adaptation and learning[(5)].
- Collaboration between Traffic Monitoring Agents (TMA) to share information on surveillance activities, traffic patterns, and detected anomalies[(6)].
- Collaboration between the Vulnerability Management Agents (VMA) to share information about detected vulnerabilities and proposed patches[(7)].
- Collaboration between all types of agents and the Security Management Agent (SMA) for centralized management of security policies[(8)].

Figure 2 summarizes the communication and collaboration between the agents in our proposed architecture.

4.2.4 Layers of the proposed architecture

The proposed architecture can be designed using a layered approach, which offers better management of the solution's complexity, a clear separation of responsibilities, and improved modularity. In our work, we have divided the proposed architecture into seven layers, with each layer containing one or more agents as needed. To arrange the proposed layers in a proper order, we based this on the logical flow of operations carried out by the security systems, from authentication to decision-making. Below, we will present the layers of our architecture from bottom to top, along with the roles and agents of each layer.

- **Authentication and Authorization Layer**

This layer contains the Authentication and Authorization agent (AAA) to manage and ensure the authentication of IoT devices and authorize their access. This layer is considered the first layer of the proposed architecture as access control is the initial step in securing an IoT environment.

- **Monitoring and detection Layer**

In this layer, two types of agents are implemented: Traffic Monitoring Agents (TMA) and Intrusion Detection Agents (IDA). The main role of these agents is to monitor network traffic and detect anomalies. This layer is positioned as the second layer in our architecture since successful authentication to a network requires the next step to focus on monitoring IoT network traffic and detecting potential anomalies in real-time.

- **Vulnerabilities Management Layer**

This layer contains the Vulnerability Management Agent (VMA). Its role is to identify, monitor, and manage potential vulnerabilities. It is the third layer in our architecture because, after monitoring traffic and detecting anomalies, the security system must manage the identified vulnerabilities to prevent their exploitation by cybercriminals.

- **Event Correlation Layer**

This layer contains a single agent, the Event Correlation Agent (ECA). The role of the ECA agent is to correlate security events and distinguish between real attacks and false alarms. This layer is positioned as the next layer in our architecture because, after authentication, traffic monitoring, anomaly detection, and vulnerability management, the next step is to correlate all security events to identify security patterns and differentiate between false positives and real security threats.

- **Artificial Intelligence Layer**

The Artificial Intelligence Layer contains a single agent, the Artificial Intelligence Agent (AIA). The role of this layer is to analyze the data and patterns identified in the previous layer and, as a result, detect abnormal behaviors. The placement of this layer is justified by the need for rapid and efficient analysis of identified security events. For this reason, after event correlation and security pattern identification in the previous layer, the Artificial Intelligence Layer is implemented to intelligently analyze these patterns, detect abnormal behaviors, and consequently make intelligent decisions.

- **Incidents Response Layer**

This layer contains a single agent called Incident Response Agent (IRA). The main role of IRA is to implement response actions when an incident is detected. This layer is in the sixth position in our architecture because it is responsible for utilizing all the operations previously performed by the lower layers to implement the appropriate countermeasures.

- **Global Management Layer**

The global management layer contains an agent known as the Security Management Agent (SMA). The role of this layer is to perform the overall coordination of the entire security system, manage security policies, and analyze aggregated data. Its position at the top of our architecture is justified by the need for a node capable of managing the system as a whole and coordinating between all types of agents within the architecture.

Figure 3 summarizes all layers of our proposed architecture.

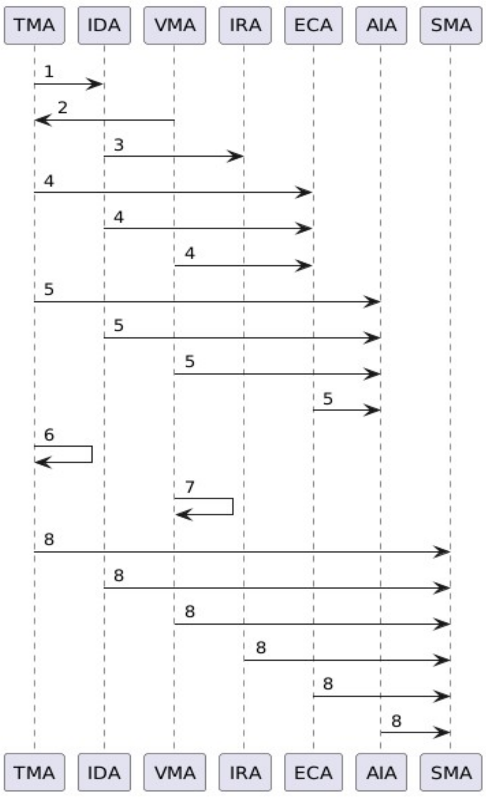

Figure 2: Communication between agents

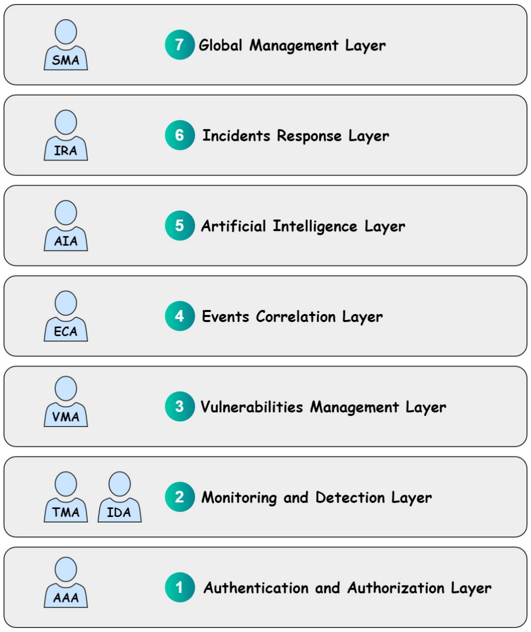
SMA
7 Global Management Layer
IRA
6 Incidents Response Layer
AIA
5 Artificial Intelligence Layer
ECA
4 Events Correlation Layer
VMA
3 Vulnerabilities Management Layer
TMA
IDA
2 Monitoring and Detection Layer
AAA
1 Authentication and Authorization Layer

Figure 3: Layers of the proposed architecture

4.2.5 Data Flow Chart

Our proposed architecture is distributed, implying that the IoT network security process within this framework is distributed across multiple agents, each assigned a specific task. To clarify the functioning of our proposed system, we will present in this part a data flow diagram of our proposed security architecture. The diagram in figure 4 illustrates all the operations of the proposed security system, starting with authentication, through traffic monitoring, intrusion detection, vulnerability detection, event correlation, intelligent analysis of security events, and incident response, arriving at the security management layer for a global view of events and an update of security policies. The diagram contains decision points such as IoT Device Authentication, Anomaly or Threat Detection, Vulnerabilities Detection, Event Significant, and Threat Mitigation. These points determine the data flow direction and ensure that only critical events are forwarded to advanced layers such as the AI layer, Event Correlation layer, and Security Management layer. The two processes of intrusion detection and vulnerability detection occur simultaneously. Following the intelligent analysis of the events, the AI layer sends the analysis reports simultaneously to the Incident Response layer for an efficient and effective response to the detected incidents, and to the Security Management layer to update security policies and make smarter and more effective decisions. Finally, the diagram contains feedback loops that show that the proposed system is always

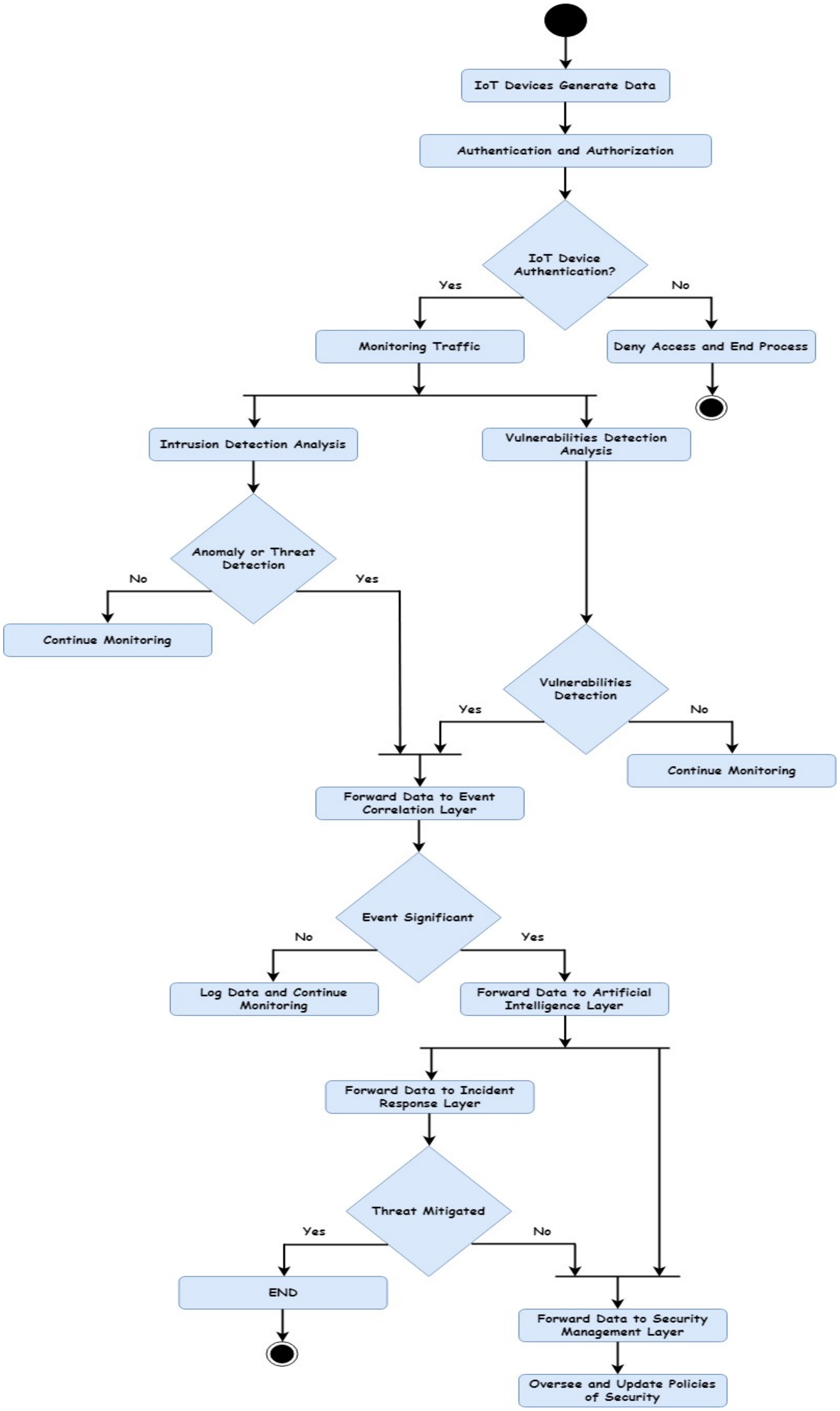
IoT Devices Generate Data
Authentication and Authorization
IoT Device Authentication?
Yes
No
Monitoring Traffic
Deny Access and End Process
Intrusion Detection Analysis
Vulnerabilities Detection Analysis
Anomaly or Threat Detection
No
Yes
Continue Monitoring
Vulnerabilities Detection
Yes
No
Continue Monitoring
Forward Data to Event Correlation Layer
Event Significant
No
Yes
Log Data and Continue Monitoring
Forward Data to Artificial Intelligence Layer
Forward Data to Incident Response Layer
Threat Mitigated
Yes
No
END
Forward Data to Security Management Layer
Oversee and Update Policies of Security

Figure 4: Data Flow in the proposed architecture

improving its security level to continuously adapt to the changing numbers and types of threats against IoT networks and devices.

Figure 4 summarizes the data flow in our proposed architecture.

5. DISCUSSION

Our architecture is a distributed system based on multi-agent systems with the main goal of providing an exhaustive solution for the cybersecurity of the Internet of Things. This architecture offers several advantages such as the distribution of the security solution, which provides speed and efficiency in monitoring, detecting, and responding to threats. Additionally, there is collaboration between agents, where each agent in the architecture has its task. However, the tasks performed, data collected, and decisions made by one agent can be shared with other agents to improve the efficiency of the tasks performed by these agents. Furthermore, the division of the architecture into layers allows for task separation, with each layer offering a well-defined task in a precise manner. Using a layered architecture also provides flexibility and ease of updates if necessary. Moreover, the division of our architecture into layers enhances the security of the security system itself, as it allows for the implementation of an independent access control policy for each layer. If one layer is compromised, the other layers remain secure. Finally, the structure of our proposed architecture presents the possibility of improving and developing our solution, by integrating other distribution-compatible techniques such as Machine Learning algorithms to anticipate threats in real time, Blockchain mechanisms to strengthen data traceability and integrity and Federated Machine Learning techniques to allow agents to learn locally while sharing models without compromising confidentiality.

Most security solutions for the Internet of Things suffer from several issues, such as task centralization and a focus on specific security tasks like encryption and authentication, monitoring and anomaly detection, or analyzing and correlating security events. This work proposes distributed and intelligent architecture based on multi-agent systems for securing IoT environments. The architecture is divided into layers, with each layer responsible for performing a specific security task, from authentication to decision-making. Each layer contains specialized, autonomous, and intelligent agents. Our work makes a significant contribution to the field of IoT security by addressing key challenges such as centralization, speed, and scalability.

Current best practices in IoT cybersecurity rely on centralized IDS solutions, lightweight encryption and authentication mechanisms, and SIEM systems for security event management. While these approaches offer valuable and relevant solutions, most of them are centralized and address isolated security tasks. Our work is a purely original research contribution, with its originality rooted in concepts derived from military theory. We propose an intelligent, distributed architecture based on multi-agent systems for the cybersecurity of IoT environments. This architecture is organized into seven layers, each assigned a specific security task. Each layer includes one or more types of agents responsible for performing specific security tasks. Our approach presents significant improvement to best practices in IoT cybersecurity and offers a conceptual advancement toward new models of intelligent, distributed security systems for IoT environments.

Our work is original and proposes a distributed intelligent architecture based on multi-agent systems for IoT security. Like any research project, it has several limitations that need to be addressed in future work, such as: First, our work is conceptual and does not include implementation or simulation to validate its performance. Second, although the system relies on cooperation between agents, the issue of secure communication between agents has not been addressed in detail. This represents a potential vulnerability in the face of advanced threats. Finally, risk management is not sufficiently explored. There are currently no defined mechanisms if an agent is compromised. These limitations arise from the desire to focus on proposing well-detailed conceptual architecture and the inherent challenge of addressing all aspects in a single research project. These limitations will serve as the foundation for our future work, where we aim to present a high-performance, fast, and adaptable security solution for IoT environments.

6. CONCLUSION

The security of the Internet of Things is one of the very important points to address to use this technology safely and suitably in all fields. Standard security solutions, including those based on classical artificial intelligence techniques, suffer from several problems, such as pressure on the central node and the dependence of the entire security system on this node. This highlights the need to develop distributed and intelligent security solutions. This work proposes an intelligent distributed architecture based on multi-agent systems for securing IoT environments. Our proposed architecture is layered, with each layer assigned specific tasks and containing agents responsible for performing various security functions such as authentication, monitoring, detection, analysis, correlation, and decision-making. The proposed architecture presents a powerful solution for IoT applications and networks, thanks to several advantages such as reducing the workload on the central node, accelerating the security process from authentication to decision-making, and structuring the architecture in layers, which facilitates system maintenance and the updating of security policies. Though efforts have been made, there are still areas for improvement and several research questions to be addressed in future work, such as ensuring secure communication between agents, managing risks within the proposed architecture, and achieving interoperability between heterogeneous IoT protocols. Our future work will focus on the development and implementation of the proposed architecture, either through simulation or real-world deployment. Ultimately, we believe that our architecture offers a strong and flexible model for advancing distributed IoT through intelligence, adaptability, and autonomy.

AUTHORS' CONTRIBUTIONS

- ❖ **Conceptualization:** Rachid Hdidou and Mohamed El Alami
- ❖ **Methodology:** Rachid Hdidou and Mohamed El Alami
- ❖ **Writing – original draft:** Rachid Hdidou
- ❖ **Project administration:** Mohamed El Alami
- ❖ **Supervision and validation:** Mohamed El Alami

REFERENCES:

[1] Rachid Hdidou, Mohamed El Alami, "Intrusion Detection System in Internet of Things: A Recent State of the Art", Journal of Theoretical and Applied Information Technology, Vol. 102, no. 1, 2024, pp. 297-317.

[2] Rachid Hdidou, Mohamed El Alami, "Advancements in Intrusion Detection Systems for Internet of Things: A State Of The Art and Comprehensive Analysis of Machine Learning Algorithms", Journal of Theoretical and Applied Information Technology, Vol. 102, no. 2, 2019, pp. 297-317.

[3] Parul Goyal, Ashok Kumar Sahoo, Tarun Kumar Sharma, "Internet of Things: Architecture and Enabling Technologies", Materials Today: Proceedings, Vol. 34, 2021, pp. 719-735.

[4] Leonel Santos, Carlos Rabadão, Ramiro Gonçalves, "Intrusion detection systems in internet of things A literature review", Proceedings of the 13th Iberian Conference on Information Systems and Technologies(CISTI), IEEE Xplore, 13-16 June, 2018, pp. 1-7.

[5] Telecommunication Standardization Sector Of UTI, "ITU-Tx. 660", Interfaces, Vol. 10, no. 20-X, 1996, pp. 49.

[6] Michael Wooldridge, "Intelligent Agents" in Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence, G. Weiss, Ed., The MIT Press, London, England, 1999, pp. 1-51.

[7] Ali Dorri, Salil S Kanhere, Raja Jurdak, "Multi-agent systems: A survey", IEEE Access, Vol. 6, 2018, pp. 28573-28593.

[8] Jing Xie, Liu Chen-Ching, "Multi-agent systems and their applications", Journal of International Council on Electrical Engineering, Vol. 7, no .1, 2017, pp. 188-197.

[9] Elhadi Shakshuki, Reid Malcolm, "Multi-Agent System Applications in Healthcare: Current Technology and Future Roadmap", Procedia Computer Science, Vol. 52, 2015, pp. 252-261.

[10] Mohamed EL Alami, Najoua Tahiri, Fernando Arriaga, "DIAUTIS: A Fuzzy and Affective Multi-Agent Platform for the Diagnosis of Autism" British Journal of Applied Science & Technology, Vol. 21, no. 4, 2017, pp. 1-28.

[11] Cecilia Garcia Cena, Pedro F. Cardenas, Roque Saltaren Pazmino, Lisandro Puglisi, Rafael Aracil Santonja, "A Cooperative Multi-Agent Robotics System: Design and Modelling", Expert Systems with Applications, Vol. 40, no. 12, 2013, pp. 4737-4748.

[12] Abdulfetah Abdela Shobole, Mohammed Wadi, "Multiagent Systems Application for the Smart Grid Protection", Renewable and Sustainable Energy Reviews, Vol. 149, 2021, pp. 111352.

[13] J.-H Lee, C.-O Kim, "Multi-Agent Systems Applications in Manufacturing Systems and Supply Chain Management: A Review Paper", International Journal of Production Research, Vol. 46, no. 1, 2021, pp. 233-265.

[14] Alfonso González-Briones, Fernando De La Prieta, Mohd Saberi Mohamad, Sigeru Omatu, Juan M. Corchado, "Multi-Agent Systems

Applications in Energy Optimization Problems: A State-of-the-Art Review", Energies, Vol. 11, no. 8, 2018, pp. 1928.

[15] F. De Arriaga, M. El Alami, A. Arriaga, F. Arriaga, J. Arriaga, "NEOCAMPUS: Multi-Agent Software Environment for On-Line Learning", Educational Technology, Vol. 3, 2002, pp. 1355-1360.

[16] F. De Arriaga, M. El Alami, A. Arriaga, "NEOCAMPUS2: A Multi-Agent Environment for Educational Research and Applications", Innovation, Technology and Research in Education, IADAT, 2004, pp. 194-199.

[17] Mohssine El Ajjouri, Siham Benhadou, Hicham Medromi, "New Collaborative Intrusion Detection Architecture Based on Multi-Agent Systems", Journal of Communication and Computer, Vol. 13, 2016, pp. 1-10.

[18] Ismail Butun, Patrik Österberg, Houbing Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures", IEEE Communications Surveys & Tutorials, Vol. 22, no. 1, 2019, pp. 616-644.

[19] Shapla Khanam, Ismail Bin Ahmedy, Mohd Yamani Idna Idris, Mohamed Hisham Jaward, Aznul Qalid Bin Md Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things", IEEE Access, Vol. 8, 2020, pp. 219709-219743.

[20] Mourade Azrour, Jamal Mabrouki, Azidine Guezzaz, Ambrina Kanwal, "Internet of Things Security: Challenges and Key Issues", Security and Communication Networks, Vol. 2021, no. 1, 2021, pp. 5533843.

[21] Raza Shahid, Linus Wallgren, Thiemo Voigt, "SVELTE: Real-Time Intrusion Detection in the Internet of Things," Ad Hoc Networks, Vol. 11, no. 8, 2013, pp. 2661-2674.

[22] Tsung-Han Lee, Chih-Hao Wen, Lin-Huang Chang, Hung-Shiou Chiang, Ming-Chun Hsieh, "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LoWPAN", Advanced Technologies, Embedded and Multimedia for Human-Centric Computing, 2014, pp. 1205-1213.

[23] Abhishek Verma, Virender Ranga, "ELNIDS: Ensemble Learning Based Network Intrusion Detection System for RPL Based Internet of Things", Proceedings of the 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE Xplore, 18-19 April, 2019, pp. 1-6.

[24] Jabed Al Faysal, Sk Tahmid Mostafa, Jannatul Sultana Tamanna, Khondoker Mirazul Mumenin, Md. Mashrur Arifin, Md. Abdul Awal, Atanu Shome, Sheikh Shanawaz Mostafa, "XGB-RF: A Hybrid Machine Learning Approach for IoT Intrusion Detection," Telecom, Vol. 3, 2022, pp. 52-69.

[25] Abdalrahman Hwoij, As'har Khamaiseh, Mohammad Ababneh, "SIEM Architecture for the Internet of Things and Smart City", Proceedings of the International Conference on Data Science, E-Learning and Information Systems, ACM Library, 5-7 April, 2021, pp. 147-152.

[26] Andrés Pardo Mesa, Fabián Ardila Rodríguez, Daniel Díaz López, Félix Gómez Mármol, "sSIEM-IoT: A Blockchain-Based and Distributed SIEM for the Internet of Things", Proceedings of the International Conference on Applied Cryptography and Network Security, 5-7 June, 2019, pp. 108-121.

[27] Juan Velandia Botello, Andrés Pardo Mesa, Fabián Ardila Rodríguez, Daniel Díaz-López, Pantaleone Nespoli, Félix Gómez Mármol, "BlockSIEM: Protecting Smart City Services Through a Blockchain-Based and Distributed SIEM", Sensors, Vol. 20, no. 16, 2020, pp. 4636.

[28] Pranay P. Gaikwad, Jyotsna P. Gabhane, Snehal S. Golait, "3-Level Secure Kerberos Authentication for Smart Home Systems Using IoT", Proceedings of the 1st International Conference on Next Generation Computing Technologies (NGCT), 04-05 September, 2015, pp. 262-268.

[29] Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, Usman Ali Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", International Journal of Advanced Computer Science and Applications, Vol. 8, no. 1, 2017, pp. 1-10.

[30] K. Sowjanya, Mou Dasgupta, Sangram Ray, "Elliptic Curve Cryptography Based Authentication Scheme for Internet of Medical Things," Journal of Information Security and Applications, Vol. 58, 2017, pp. 102761.