AI Driven Adaptive Security Mesh: Cloud Container Protection for Dynamic Threat Landscapes

Edi Marian Timofte
"Stefan cel Mare"University
Suceava, Romania
edi.timofte@usm.ro

Alexandra Ligia Balan
"Stefan cel Mare"University
Suceava, Romania
alexandra.balan@usv.ro

Teodor Iftime
Suceava, Romania
iftime.teo@gmail.com

***Abstract*—This work explores the new approach of integrating Artificial Intelligence (AI) into an adaptive mesh security system and discusses the challenges and opportunities of this innovative method. In a digital world where cyber-attacks and technological innovations are rapidly increasing, making AI a core tool in security architectures is not just an upgrade to defensive efficacy, but also a strategic necessity. By examining technical and operational barriers, as well as the requirement of advanced computational resources and specific expertise, the paper emphasizes the need to tailor security system design to each IT infrastructure. Access to extensive, diverse data to facilitate the training of AI algorithms for efficient threat recognition is needed, but also raises challenges in data collection, processing, and confidentiality. This paper also stresses the urgent need for cross sector collaboration and standardization in adaptive security as key to efficiently meet challenges and accelerate innovation adoption. In conclusion, though facing significant challenges, incorporating AI into adaptive mesh security systems blazes a path towards developing innovative solutions that enable organizations to navigate effectively in a constantly evolving cyber landscape. It highlights the need for research, development, and collaboration across disciplines to create a robust, adaptable, and transparent security ecosystem.**

Keywords—Information security, Wireless mesh networks, Clouds, Defense industry, Machine Learning, Image edge detection, Pattern analysis

I. Introduction

As technology advances, the digital age is evolving radically. How we store, operate, and access data and software have been changed mainly due to cloud services and container technologies. These advances have reshaped IT infrastructures and boosted the development and implementation of software applications. However, this progress has not been without challenges, particularly in cyber-security, where the dynamic and distributed nature of container-based environments opens doors to potential threats.

Container technologies, represented by Docker and Kubernetes, brought notable benefits regarding development efficiency, portability, scalability, and application isolation. These technologies allow organizations to deploy and manage microservices more dynamically and efficiently. Yet, as applications and data shift from data centers to distributed cloud infrastructures, a new set of vulnerabilities and attack vectors are exposed. This shift underscores the critical need to rethink and innovate in the cyber-security domain.

Traditional security approaches, which often rely on well-defined perimeters and assume internal infrastructures are inherently secure, are proving inadequate given the current threat landscape, marked by increasing complexity. In this scenario, threats are evolving alarmingly fast, taking advantage of emerging technologies like Artificial Intelligence and automation to orchestrate sophisticated and targeted attacks. Additionally, the growth of microservices and containers has further fragmented the application landscape, complicating the tasks of monitoring, managing, and protecting them.

We need a fresh approach to cloud container security, one that goes beyond traditional models and actively uses AI, behavioral analytics, and adaptive incident response. Not only should this approach be ready for threats, but it should ride the wave of continual tech advancements and opponent tactics. This new security system aims to dive deep into the belly of an AI-driven adaptive security network; giving a new protective layer to cloud containers as threats shift and evolve. In doing so, we will delve into the current challenges and innovative solutions giving a fresh and deep view on security in a fast paced digital age.

II. Research and analysis

The paper [1] describes the DRCKDS that uses sensors to track different environmental factors like energy, transmission speed, and success rate. These are used to find the safest data transmission routes, each path being checked using a Safe Route Score (SRM) to pick out an optimal transmission path. The system then creates many encryption keys for data transmission on the chosen path. This ensures data is sent securely and clients are satisfied with the safety quality in WMNs. The paper [1], proposes that, using trustworthy measurement technologies that are native to the cloud and based on webhook, makes a unique method to protect container data via encryption and decryption, allowing for transparent protection of container data. Our solution improves this kind of security by verifying the same energy consumption data to make sure the client requesting it is genuine.

The article [2] explores an innovative CSI (Channel State Information) method of securing homes by using Radio Frequency (RF) technology combined with a Wi-Fi mesh network. This system proposes an advanced security solution, such as alarm systems based on motion sensors or surveillance cameras, by exploiting the unique capabilities of RF technology and mesh networks to create a more robust and flexible security network. It uses a learning model to figure out if there is an intrusion. Then it triggers an alarm based on this information. Tests show over 90% accuracy in catching intrusions, proving its effectiveness and reliability. Adding our system on top of this would exponentially increase its accuracy even further by verifying the energy consumption patterns of the connected devices. And because it showed great results on measuring the energy consumption patterns, it

979-8-3503-4929-0/24/$31.00 ©2024 IEEE

could also work on analyzing the used RF spectrums to detect anomalies.

Article [3] explains the connection of two Edge IoT devices and their data sharing capabilities through Kubernetes clusters and services mesh hosted on distinct OpenStack cloud environments and Virtual Machines (VMs). Their testing results show that the planned structure provides a straightforward method for connecting different IoT devices, with barely any effect on performance and resource usage. Adding a Raspberry Pi to this system that check the energy consumption of these devices would hardly change the performance and resource usage while adding a robust layer of security.

The research [4] presents an approach for integrating cloud computing into Wireless Mesh Networks (WMNs). It suggests solutions to secure and optimize communications in these networks. The framework aims to leverage the flexibility and extensive coverage of WMNs while providing a robust structure to overcome existing limitations and streamline integration with cloud technologies. This is another great system in which our solution would make a great difference, because, once one of the communication devices are compromised, our system could detect the anomaly and flag it as a danger.

The design of a new Directional Mesh Network (DMN), which enhances radio spectrum resources distribution through Machine Learning (ML) and AI is presented in [5]. The system considers antenna power gain, which can further minimize detection probability and DMN system interference. A critical research aspect is the use of fog computing to process data close to the signal source. This enables early, efficient data examination and an intelligent spectrum resource distribution. The implemented ML methods adapt according to the fog nodes' computational capacity, thereby enhancing the network's ability to dynamically respond to environmental changes. While this is optimizing the quality of the transmission, our system, also using ML, is looking at the rates of data distribution to detect anomalies. We believe that, joining the two, a more robust system could do both at the same time. This really shows the power of putting the ML algorithms in the right place to make the most of it and bring the current security systems to the next level.

Reference [6] introduces a thorough defense plan to fight the vulnerabilities linked to container management procedures. These can lead to "container escape" attacks. This lets attackers move out of an isolated container and get unauthorized access to the host system. It brings a big threat to the security of cloud infrastructure and the apps running in containers. The authors suggest a three-tier approach to strengthen defense against potential security vulnerabilities. As prevention, they recommend strict security policies and container software updates to rectify known vulnerabilities and advanced monitoring solutions for detection, capable of identifying unusual activities that may indicate attempted container escapes. Our system seems like the perfect solution for this as it is analyzing most of the traffic parameters and fits their suggestions exactly.

The exponential growth of IoT devices has led to a surge in complex cyber-attacks, making the task of identifying malicious links a significant hurdle. The article [7] emphasizes the role of automatic learning technologies and Intrusion Detection Systems (IDS) in fighting these threats efficiently. While their solution uses AI alone to identify the possible threats, using ML to check the hardware data is covering most of the overlooked ground, making a merged system of the two, one of the toughest security systems for a IoT network.

The research papers [8] proposes a unique framework that handles the exponential growth of data and resource needs by optimizing resource management in such diverse environments. The framework uses an influence-based learning technique to predict optimal application deployment configurations, demonstrating over 90% accuracy. Although the accuracy is high, their learning technique is influenced, and this may lead to issues that would need to further tune the data to influence the system. Our system relies on the device's own data, and the ML algorithm is set to keep improving based on more and more data analyzed, so it becomes increasingly accurate, which exceeds 90% at a later point in time.

The article [9] explores the enhancement of WMN using AI-supported routing methods with the aim of meeting the increasing demands of web connectivity, even in hard-to-reach areas. Due to their self-healing capability and adaptive behavior, wireless mesh networks represent an advanced solution to modern connectivity challenges. This system could be used in a IoT network to determine a fast route of sending the data from the IoT devices while simply adding a Raspberry Pi to the network to actively check for potential hacked devices ensures the security of the system.

The method in the [10] makes use of SDN capabilities and the sFlow-RT app. It is built to spot and lessen DDoS attacks by using REST APIs to enforce a Policy-Based Flow Management (PBFM) through an SDN controller. This system aims to make sure services do not get interrupted during DDoS attacks. It also makes managing mesh-based networks easier and better. Mesh networks add security through multiple communication links. But they also complicate setup and troubleshooting. When used in critical networks like the ones used in cloud computing, mesh topology offers extra protection by keeping services available.

The article [11] proposes, using container virtualization technology, to set up mirror servers and nodes between IoT devices and the cloud. By using virtual desktop container technology, the system can bring devices closer to service terminal locations. In turn, it prevents network attacks through communication line nodes, thereby improving communication efficiency in dispersed AI systems.

The article [12] tackles security issues in cloud container systems, highlighting container architecture complexity and associated risks. The study looks at moving from traditional network management, which relies heavily on manual settings and is slow to adapt to changes, to a more dynamic, intelligent approach, made possible through SDN. By separating the network's control layer from the data layer, SDN allows centralized control and greater automation in managing resources and delivering services. This architecture is like the human central nervous system, with the SDN Controller acting like a brain, directing network operations based on a complete awareness of the network's status. The authors call for extra research to extend these capabilities, especially in AI-based network management. The goal is to achieve completely autonomous networks that can self-organize in response to internal dynamics and external threats, and that can continuously learn and improve their performance and security stance.

Today's challenges in integrating Internet of Things (IoT) technology with Artificial Intelligence (AI), featured in [13], suggest a decentralized AIoT system. This system meshes Docker's containerization technology and the cloud-fog integration concept for better handling and securing IoT devices. The aim is to build a smarter, more efficient IoT system that can meet the rising demands for service quality and smart needs. The decentralized system architecture encompasses three primary levels: endpoint device layer, fog processing layer, and cloud computing layer.

Each layer is pivotal in data collection, processing, and action execution, thereby shaping a structure akin to a Backpropagation (BP) neural network. Here, perception devices, fog devices, and execution devices mirror the input layer, hidden layer, and output layer of the neural network, respectively.

III. Fundamentals of AI Driven Adaptive Security Mesh

Figure 1 shows the general architecture of the adaptive security system we proposed. This diagram illustrates how artificial intelligence (AI) components are integrated into the security network to provide dynamic and adaptive protection against cyber threats. The diagram highlights the flow of data from data capture points, through analysis processes, and to automated intervention in the event of threat detection.

The architecture includes AI modules responsible for behavioral analysis of network traffic, machine learning modules that adjust security parameters in real time, and automated response systems that execute measures to contain detected incidents. This configuration is critical to understanding how our solution adapts and responds to dynamic developments in the cyber threat landscape.

Figure 1 serves as a benchmark for the technical discussions in the document and as a visual foundation for evaluating the benefits of integrating AI into adaptive security systems. For example, readers can better understand how AI-based predictions help anticipate suspicious behavior and minimize the impact of security incidents.

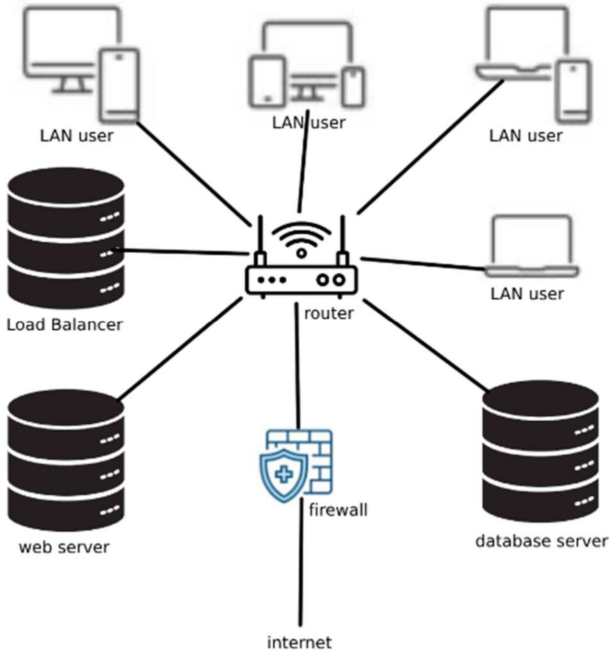

Fig. 1. Typical network diagram

As part of the implementation of the new network infrastructure, our research team conducted an extensive series of controlled tests to verify the system's resistance to Distributed Denial of Service (DDoS) cyber attacks. This thorough assessment was conducted using various advanced simulation tools such as GoldenEye, Katana Framework and Xerxes, specially configured to generate heavy and malicious traffic to the TP-Link AC1750 Router, Model Archer C7 [14]. These rigorous testing procedures were aimed at mapping the device's responsiveness to a continuous assault, thus evaluating the effectiveness of the built-in security mechanisms and identifying potential vulnerabilities in its security architecture, also providing information related to the ports and technologies installed in the network. The results obtained provide valuable insight into systemic vulnerabilities, paving the way for strategic improvements in modern network security design.

```
$ nmap 79.112.151.122
Starting Nmap 7.93 (https://nmap.org) at 2023-06-19 04:48 EDT
Nmap scan report for 79-112-151-122.rdsnet.ro (79.112.151.122)
Host is up (0.037s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT            STATE     SERVICE
22/tcp  filtered ssh
23/tcp filtered telnet
```

Fig. 2. Scanning and identifying network vulnerabilities

We have built a smart code that uses ML techniques to train a sophisticated model specifically for spotting network traffic anomalies. This model, by studying traffic data, accurately and efficiently picks out signals hinting at malicious activities. A set of complex algorithms helps it to pull out important features and apply deep learning methods to learn from data. This strengthens its capability to differentiate normal and abnormal traffic. This approach does not just find anomalies in network traffic. It significantly enhances network security by providing a comprehensive view of threats.

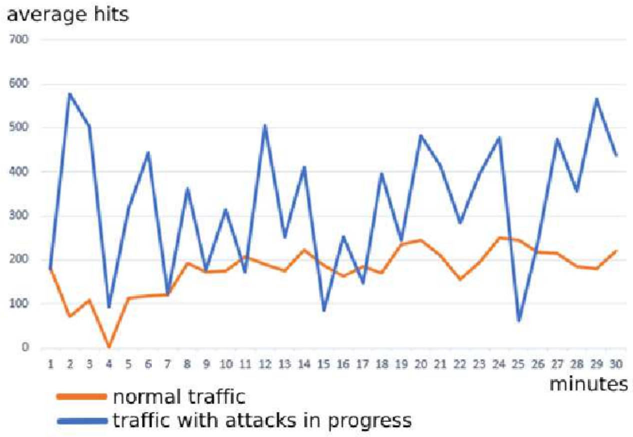

Fig. 3. Attacked network traffic graph

We created a simulation framework to identify unusual network traffic behaviors using a method called One-Class Support Vector Machine (SVM). This advanced technique is often used to identify different patterns, including detecting anomalies and extreme values (outliers).

Our model uses a sequential architecture, which makes adding layers in a linear way easier - each layer takes the output of the previous one as input. We use dense layers, equipped with ' ReLU ' (Rectified Linear Unit) activation functions, as a strategy for extracting and learning non-linear features in data. ' ReLU ' is preferred due to its effectiveness in accelerating convergence during training, as well as its ability to counter the vanishing gradient problem common in deep dense networks.

This illustrates (Fig.2) how advanced Machine Learning and neural network techniques can tackle complex cyber-security challenges like malicious traffic detection. The results drawn from training and evaluating the model provide valuable insights on its effectiveness in classifying traffic data, highlighting the potential and limitations of the approach in real-world application scenarios.

In this scenario, the model is trained with a data set labeled as "normal" behavior (initial test data). This means it can form an idea of standard network traffic. Then, the model is applied to new data sets (normal data flow) and compares the two to identify which data matches the learned profile and which shows big differences. The tested data set includes features like the number of requests per second, data volume in megabytes, and session length in seconds. The related labels, as shown in the Fig.2 graph, indicate if the traffic is normal (orange line) or abnormal (blue line). The data set is then split up into training (pre-tested activity set) and testing (current data received) subsets using the train_test_split library.

Fig.2 shows on the X axis the time since the system was online, in minutes, while the Y axis indicates the number of average hits the system had for the last minute.

Adding a Dropout layer comes with a smart way to avoid overfitting, as it is a regularization technique used in neural networks to prevent overfitting. Overfitting is when the model learns too much from the training set and loses its power to generalize. To combat this, the Dropout method randomly skips parts of the network. This leads to a stronger model that performs better with new, unseen data.

Any detected variations are signs of harmful actions or other forms of anomalies. Since the model is trained solely with normal data, any detected anomaly suggests a deviation or novelty. As a result, the One-Class SVM, proves to be effective within the cyber-security field and it showed that it allows for early identification of potential threats by analyzing network behaviors that divert from the established models.

This process not only improves the response to security incidents, but its proactive nature allows for a deep understanding of network traffic dynamics, aiding in the constant fine-tuning of cyber-defense mechanisms.

These advanced systems show a remarkable capacity to analyze, in a split second, the massive volume data from network activities. This allows it to identify anomalies or suspicious behaviors indicative of an active threat. From this analysis, AI-based mechanisms can instantly put into action custom security policies. These aim to not only neutralize detected threats immediately but also to prevent potential damage spread. This is achieved by strategically isolating affected resources or network segments, substantially limiting malicious actors' ability to exploit system vulnerabilities to widen their access or impact.

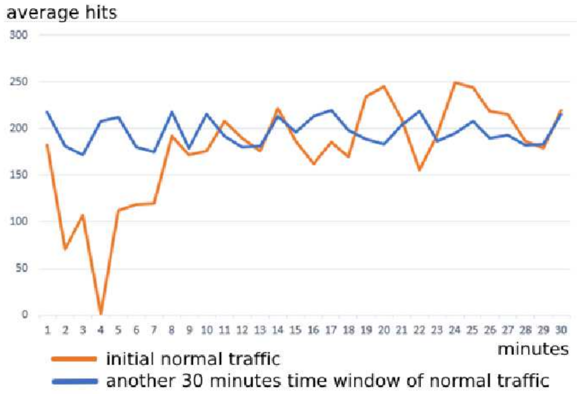

Fig. 4. Network traffic graph without incidents

The system will continue to constantly watch the network, spotting security incidents and responding to them. It is set up to find suspicious IP addresses and performs isolation and notification tasks in response. Spotting security incidents, isolating resources, and alerting administrators means working with real monitoring and security management systems. It also involves using AI-based decision-making logic to assess and rank incidents based on their seriousness and kind.

While monitoring the network traffic, the system responds only to abnormal behavior, normal network traffic (Fig.3) just being added to the system's continuous learning algorithm.

With the `collect_system_metrics` function, our system collects and returns critical system metrics such as CPU usage percentage (Fig.4), memory usage and available disk space, effectively exploiting the `psutil` library to access these information. At the same time, the `monitor_network_traffic` function starts a listening channel on port 80 for all IP addresses, using a socket to monitor network traffic and collect data packets. These packets are then processed and analyzed for comprehensive analysis and full visibility of the data traversing the network. Finally, another block plays a key role in running this script as the standalone module. It initiates an endless loop that allows regular collection and visualization of system metrics every 300 seconds (5 minutes), thus reinforcing continuous monitoring and performance optimization of our cloud infrastructure.

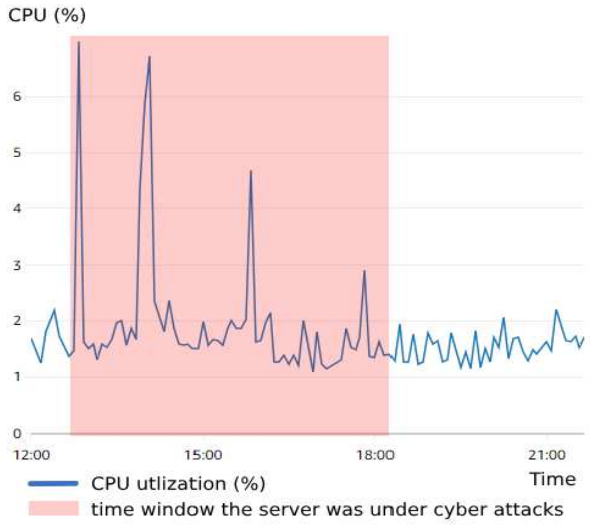

Fig. 5. CPU utilization graph

IV. Cloud Security and Containers

Setting up an adaptive security mesh in a containerized cloud environment helps securing and making IT infrastructures resilient in today's constantly changing cyber-threat landscape. This task requires a rigorous approach, broken down into several steps, each with its own unique role in strengthening the organization's security posture. The whole process focuses on four key areas: planning, designing, implementing, and continuous monitoring. Each phase is vital to ensure an effective and lasting implementation.

A. Planning

The initial planning and analysis stage forms the base for all adaptive security strategies in a cloud environment with containers, providing a strong base for the further application of security measures. This starter phase involves a careful breakdown of the current infrastructure, focusing on pinpointing the high-value components and possible attack vectors, as well as thoroughly assessing system vulnerabilities.

The first task during this stage is to thoroughly map out the IT architecture to understand the structure and connections between various system components. This includes a detailed analysis of networks, servers, applications, and databases, and the way they interact and communicate with each other.

In the process of mapping a company's computer network visually, we created a detailed diagram (Fig.1). It shows the network architecture, it includes crucial elements for data security and efficiency. These elements are a firewall, two server units (specifically, one for web applications and one for database management), a load balancer, and a variety of client devices (like laptops, desktop systems, and mobile devices) that connect to the LAN. The diagram clearly shows the firewall's strategic placement. It is in between the public internet and the internal network. This helps filter and prevent unauthorized access to the server's resources.

In line with these analyses, the company's data and resources are classified based on sensitivity and criticality levels. This classification is key in determining fitting protection levels and security effort prioritization. It ensures resources are efficiently allocated to the most strategically important elements.

Based on gathered information we define the security goals. These should match our organization's business aims and reflect specific compliance regulation needs. These goals will guide us in choosing the right security solutions and technologies. We are led towards options giving the best balance of performance, cost, and efficacy in tackling identified threats.

In conclusion, the initial planning and analysis stage is layered, needing a methodical approach and an eye for detail. This step lays the foundation of any cloud security strategy, providing direction and frameworks essential for building a secure ecosystem, capable of standing against the ever-changing dynamic threats of today's cyber landscape.

B. Design and architecture

We created a script crafted to heighten security in a Docker environment. The Docker Engine connection kicks off with the script to exchange information directly with the Docker API on the host system. Then, it creates SSL/TLS certificates. This aims to protect communications between users and the services provided by containers. Integrating these certificates in the container configuration involves identifying those exposing web services by verifying open ports. Lastly, it repetitively checks the security setup and traffic of all active containers. It evaluates their settings, like the filesystem that is set to read-only. However, how this is done depends on the host infrastructure's design and requirements.

C. Continuous Monitoring and Improvement

It is a recurring, dynamic process that safeguards the integrity of the IT infrastructure against evolving cyber threats. This phase involves systematic advanced surveillance activities that detect anomalies, suspicious behavior, and potential security breaches in real-time, thereby enabling swift and efficient incident response.

Complex monitoring and analysis systems equipped with AI and ML technologies help organizations filter and comprehend large volumes of log data and performance metrics, thus spotting patterns indicating malicious or unauthorized activities. These advanced systems can learn from network behavior and adapt to new types of attacks, providing superior detection and response capabilities compared to traditional monitoring solutions.

In response to the shifting and challenging nature of the current cyber landscape, we have created a security monitoring script. Its purpose is to give organizations the ability to detect possible security breaches and abnormal behaviors within their IT infrastructure by analyzing security logs in real-time. As cyber threats become increasingly advanced and difficult to identify using conventional methods, the adoption of solutions based on advanced technologies and ML becomes essential for efficient data and IT resource protection.

We use technologies like Kafka for real-time data processing, Elasticsearch for fast data storage and analysis, and Kibana for data visualization and alerts. These make a complete security monitoring solution. The script employs the Isolation Forest Machine Learning model to find anomalies in log data. This is a first step towards early detection of potential security incidents.

Mixing these tech-tools and methods, our script makes a security monitoring ecosystem capable of processing and examining real-time data. It can swiftly identify oddities and create alerts for remedial action.

V. CONCLUSION

The paper "AI Driven Adaptive Security Mesh: Reinventing Cloud Container Protection for Dynamic Threat Landscapes" highlights the significance and effectiveness of incorporating artificial intelligence (AI) into adaptive security systems for cloud container protection in a constantly changing threat landscape.

AI integration in adaptive mesh security systems has exhibited superior ability in swiftly and accurately identifying complex and evolving cyber threats, providing robust protection for cloud infrastructures and related containers.

However, the use of AI in adaptive security faces technical and operational challenges such as integration complexity, reliance on vast and diverse data sets, and data security and privacy risks. These aspects require considerable attention and resources to be effectively tackled.

The success of AI implementation in adaptive mesh security needs close collaboration between IT engineers, research, and regulatory fields to facilitate knowledge sharing, develop common standards, and effectively handle ethical and privacy challenges.

The future of adaptive security is exciting, with advances in self-learning and self-adapting, AI interpretability, and the development of solutions that integrate privacy by design. These innovations have the potential to revolutionize how organizations protect their cloud infrastructures and containers from cyber threats.

AI stands as a catalyst for reinventing container protection in cloud environments, offering an adaptive and dynamic solution for managing evolving cyber threats. However, to maximize AI's potential in adaptive security, it requires a strategic approach to existing challenges, promoting cross-sector collaboration, and continuous adaptation to new technological developments and changes in the cyber threat landscape. Therefore, the work emphasizes the need for an integrated vision and a proactive approach to efficiently navigate the complexity of contemporary cyber security.

By weaving AI into the "Security Mesh" architecture, it creates a security outlook that not only responds to known threats but also predicts and adjusts to new, sophisticated tactics. This degree of intelligence and adaptability is vital in a cyber landscape where threats constantly update their strategies to exploit emerging vulnerabilities. The AI's role in this setting is not just to enhance security, but also to make sure organizations can maintain a strategic edge against ever-evolving and dynamic threats.

Integrating AI into information security brings about new security risks, including vulnerabilities unique to AI algorithms and models. Additionally, managing sensitive data used for training and operationalizing AI systems entails notable challenges in matters of privacy and ethics, requiring sturdy data protection mechanisms and transparency.

Focusing on developing AI systems capable of self-learning and independently adapting to new types of threats presents a promising horizon. They provide dynamic security solutions, capable of predicting and nullifying cyber-attacks through continuous adjustment of protective parameters.

Advancements in the field of AI model interpretability promise to boost automated decision transparency, making it easier to understand and validate the security processes carried out.

REFERENCES

[1] A. Shameem, S. K. Shukla, M. Tiwari, D. Buddhi, Y. Singh and U. R, "A design of dynamic rate aware classified key for network security in wireless sensor network through optimized distributed secure routing protocol,"*2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, Greater Noida, India, 2023, pp. 605-608, doi: 10.1109/AISC56616.2023.10085033.

[2] M. -Y. Wu, S. -H. Wu, Y. -E. Chang, Y. -H. Lin, S. -J. Huang and H. -T. Tseng, "Intrusion Detection with Radio Frequency Sensing based on Wi-Fi Mesh Network for Home Security,"*2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*, PingTung, Taiwan, 2023, pp. 329-330, doi: 10.1109/ICCE-Taiwan58799.2023.10226838.

[3] L. Gattobigio, S. Thielemans, P. Benedetti, G. Reali, A. Braeken and K. Steenhaut, "A multi-cloud service mesh approach applied to Internet of Things,"*IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*, Brussels, Belgium, 2022, pp. 1-6, doi: 10.1109/IECON49645.2022.9968384.

[4] R. Li, Q. Liu, M. Wang and X. We, "A Novel Framework for Application of Cloud Computing in Wireless Mesh Networks,"*2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Guangdong, China, 2014, pp. 448-452, doi: 10.1109/3PGCIC.2014.91.

[5] J. Lu *et al.*, "Artificial intelligence based directional mesh network design for spectrum efficiency,"*2018 IEEE Aerospace Conference*, Big Sky, MT, USA, 2018, pp. 1-9, doi: 10.1109/AERO.2018.8396558.

[6] Z. Guo, Z. Lv, N. Li, T. Yuan, X. Gao and Z. Yuan, "Comprehensive defense scheme against container escape related to container management procedure,"*2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Suzhou, China, 2022, pp. 263-266, doi: 10.1109/CyberC55534.2022.00051.

[7] K. Garg, K. S. Gill, R. Chauhan, D. Rawat and D. Banerjee, "Distributed Denial of Services (DDoS) Botnet Attack Prevention in Internet of Things (IoT) Devices Using AI,"*2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10442302.

[8] C. Symvoulidis, A. Kiourtis, A. Mavrogiorgou, J. -D. T. Tom-Ata, G. Manias and D. Kyriazis, "Dynamic deployment prediction and configuration in hybrid cloud / edge computing environments using influence-based learning,"*2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Palembang, Indonesia, 2023, pp. 315-320, doi: 10.1109/EECSI59885.2023.10295768.

[9] P. G. Senthilvel, T. D. R, R. K. K, H. K. Palani and K. Sundravadivelu, "Enhancing Wireless Mesh Network Performance Through AI-Based Routing Algorithms,"*2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, Greater Noida, India, 2023, pp. 931-935, doi: 10.1109/ICCSAI59793.2023.10421320.

[10] S. Mani and M. J. Nene, "Preventing Distributed Denial of Service Attacks in Software Defined Mesh Networks,"*2021 International Conference on Intelligent Technologies (CONIT)*, Hubli, India, 2021, pp. 1-7, doi: 10.1109/CONIT51480.2021.9498378.

[11] Z. Li and P. Zhao, "Research on Dispersed Artificial Intelligence IoT System Based on Container Virtualization,"*2022 International Symposium on Advances in Informatics, Electronics and Education (ISAIEE)*, Frankfurt, Germany, 2022, pp. 299-303, doi: 10.1109/ISAIEE57420.2022.00068.

[12] Y. Yang, W. Shen, B. Ruan, W. Liu and K. Ren, "Security Challenges in the Container Cloud,"*2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, GA, USA, 2021, pp. 137-145, doi: 10.1109/TPSISA52974.2021.00016.

[13] Y. Cao, "System Design and Function Implementation Based on Decentralized Artificial Intelligence Internet of Things,"*2023 5th International Conference on Artificial Intelligence and Computer*

Applications (ICAICA), Dalian, China, 2023, pp. 600-605, doi: 10.1109/ICAICA58456.2023.10405571.

[14] E. M. Timofte and D. Balan, "Improving Network Security Using DD-WRT as a Solution for SOHO Routers," 2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet), Craiova, Romania, 2023, pp. 1-5, doi: 10.1109/RoEduNet60162.2023.10274916.