# AI-Powered Intrusion Detection for Microservice-Based Architectures

ONI SAMUEL BOLUWATIFE
*Obafemi Awolowo University*

***Abstract-*** ***The software architecture in microservices has revolutionized the software development procedure as we have known it by providing enormous benefits of scalability, flexibility, and durability. This is so because despite the numerous benefits offered by microservices architectures, it brings about the challenge of security challenges since the microservices applications are disperse and interconnects. Signature and anomaly-based methods are known to be impractical in identifying attacks specific to the microservice architecture due to evolving patterns of attack. To overcome with these limitations, this research expands a model of AI based IDS that uses techniques of advanced machine learning and deep learning for the improved and efficient identification of threats. As a result, the proposed system contains several modules: The first is a data collection module which collects network traffic and system logs; the second is a feature extraction module which finds out significant features of attacks; The third is AI-based detection module which classifies the normal behavior and malicious behavior. Supervised learning and unsupervised learning algorithms together with the deep learning models, for instance, CNN and RNNs are used to identify patterns and monitor and detect anomalies in real time [9]. To estimate the performance of the proposed system, benchmark datasets are used for performance evaluation. Evaluation of AI-based approaches using correct classification rate, precision, recall, and f-measure provide insights into the fact that AI-based techniques are far superior in detection when compared to conventional methods for detecting zero-day attacks and advanced persistent threats. Furthermore, the feature extraction seeks to be implemented by deep learning by eliminating the necessity of following conventional rules. Based on the results of this research, it becomes possible to conclude about the effectiveness of AI-based solutions in protecting microservice-based architectures from new generation threats. In a practical way, the study brings value to the field of cybersecurity, outlining an adaptable and sustainable model of detecting intrusion which is fit for cloud-only networks [11]. As the future work, the authors will aim to enhance the model interpretability, decrease the false alarms occurrence, and test the applicability of the proposed method in the real-world use cases related to microservices.***

***Indexed Terms-*** ***AI-powered intrusion detection, Microservice security, Machine learning for cybersecurity, Deep learning-based threat detection, Anomaly detection in cloud computing***

## I. INTRODUCTION

### *A. Background*

Microservice architectures have now become the standard for modular and scalable developments of software systems that allows them to be separated and managed independently of each other. While in monolithic system all the features integrated into one application; the microservice architecture is a set of loosely coupled applications where the communication is handled through simple formats like RESTful API and Messaging. This change increases flexibility because organizations can now build, host, and extend services on their own. However, decentralization of microservices significantly affects security and creates more exposure, insecure APIs, and issues in inter-service communication.

As a result of the network-based interactions in microservices, there are a number of security considerations, which pose as threats to the services. Security threats in the microservice-based application include unauthorized access, denial-of-service attacks,

and API exploitation. Currently available methods of continuity management are limited by traditional methods of security such as firewalls and rule-based IDS. These are some of the reasons why it is necessary to seem more sophisticated approaches to security such as Machine Learning for security that is designed to identify the breached security in real-time.

*B. Motivation*

The widespread adoption of microservices architecture has scaled up security threats that increase the need for better intrusion detection. Conventional intrusion detecting techniques signature-based and anomaly-based have been employed to detect some of the mentioned security threats [2]. Thus, they fail to promptly identify new attacks since they work by analyzing the patterns like those used in the past. In fact, old school IDS has some problems when it comes to scaling of, for example, microservices architecture where multiple services are running concurrently and are communicating with each other actively.

A new approach that can be considered as an alternative to traditional approaches is the use of artificial intelligence for intrusion detection. The artificial intelligence within IDS then processes the traffic data and differentiates between normal traffic and suspicious network traffic. Machine learning models can use input from other attacks and are able to identify new forms of threats, which allows for using them to protect microservice-based architecture. With the current obstacles to using existing security enhanced technologies to provide security for microservices, this study aims at proposing and testing an adaptive intrusion detection framework that leverages on the AI technology to improve security for microservices [1].

*C. Research Objectives*

The focus of the work reported in this thesis is to develop the novel AI-based IDS specifically for the microservice architecture. This system is User Friendly and designed to increase Security levels by monitoring and detecting the network activity, and any threats that may occur. In particular, the purpose of the given investigation will be as follows:

- Produce an effective approach of detecting intrusions to be implemented in microservice based systems.
- The effectiveness of various kinds of machine learning and deep learning in the detection of security threats.

Estimate the efficiency and accuracy of the proposed AI-powered intrusion detection system with regards to the traditional techniques for intrusion detection.

In achieving the above objectives, the research seeks to benefit the enhancement of cybersecurity in the realm of microservices by providing an adaptive and intelligent solution to the problem of intrusion detection [10].

*D. Scope and Limitations*

The subject of this research is a procedure for outlining and testing an AI-based IDS for security threats which are applicable to the structure of the microservice architecture. The study will compare real AI techniques: machine learning and deep learning for the given purpose of threat detection and prevention. Some specific types of security threats that will be discussed during the study include inter-service communication threats and API unauthorized access threats [12].

However, it can be argued that the study has limitations as follows; The work presented here is restricted to the first layer of defense only and does not encompass any other heightened layer pertaining to automated responses in case of intrusion. Further, the assessment of the performance of the developed AI-based IDSS occurs in a simulation mode, which implies that certain factors, including cloud-specific threats and security standards, were not directly in the focus of this study. Scenario work can be further extended by incorporating the functionality of automated response and the experiment can be carried out in live cloud environments.

## II. RELATED WORK

*A. Traditional Intrusion Detection Systems*

IDS have also been significant in the schemes of cybersecurity due to their ability to detect invasions, irregularities and intrusions in networks and systems. Conventional IDS can be analyzed into two forms, which include, the signature-based IDS and the anomaly-based IDS. Signature based detection depends on the previously known attack patterns

commonly referred to as the signatures. There are systems that match incoming data with the database of such attacks, which as such, are very useful in the identification of already known threats. However, their great disadvantage is the incapability of detecting new or zero-day attack, which work by existing signatures of threat.

In contrast, anomaly-based method detects new and strange activity of networks. They set a homeostasis, on top of which, anything irregular is notified and reported to the relevant authorities. The anomaly-based IDS has a disadvantage that accompanies it— it can easily identify new threats as normal traffic also does not correspond to specific patterns very often. Mauro Conti & Graziana Lo Porto further explain that the dynamic and distributed nature of microservice architectures makes it difficult for IDS that rely on a rule-based systems to determine the numerous network traffic interactions that are generated by microservices as normal or anomalous.

*A. AI-Powered Intrusion Detection Systems*

With growing technologies in the field of artificial intelligence, new and improved methods of intrusion detection have been developed, run through machine and deep learning. As opposed to IDS, AI-based') approaches process significant amounts of information, identify multifaceted threats, and learn how to process new threats without relying on specific patterns. The general type of KDD cup-based system for intrusion detection involves decision trees, support vector machines – (SVM) as well as random forests for identification of activities as either normal or anomalous [14]. These models are developed on an extract from certain historical attack data sets, and they are capable of deciphering patterns of intrusions.

Further advancements made in intrusion detection are CNNs and RNNs that allow the system to learn microscopic features directly from the raw data of network traffic. Another strength of CNNs is its ability to detect spatial features in the packets that are in the network, while RNNs are designed to recognize sequential information and as such are good for detecting a running attack. AI also brings an improved accuracy on intrusion detecting as well as the ability to effectively adapt the security measures towards microservices nature which is characterized by flexibility.

*B. Microservice-Based Architectures*

One of the reasons why current architectures of systems developed using the microservices concept have become popular is their scalability, modularity, and fault tolerance. As opposed to the monolith application architecture where application is built as one large aspect containing discrete features, microservices is an architecture that represents the disintegrated structure of the services by working as different services that interconnect using APIs. It is very beneficial for organizations to be able to create, implement and expand such services even at different layers of the system, which minimizes the time when the system is down, as well as the moment when the service by itself is down for maintenance. However, the security issue is presented due to the microservices' decentralized architecture: services communicate through network-based protocols and are prone to cyber-attacks like unauthorized access, API attacks, as well as DoS attacks.

Security in microservice architecture is mainly associated with service mesh technology and using containers. Some of the service meshes include Istio and Linked which handle traffic routing, authentication, and security policies to protect microservices from cyber threats. Containerization, using docker and Kubernetes makes Microservices apex in their own small environments to contain outbreaks, hence limiting lateral movements. Nevertheless, these threats pose a potential risk to microservices which must incorporate AI automation to apply intrusion detection in service interactions.

Table 1: Comparison of Traditional and AI-Powered Intrusion Detection Systems

| Feature | Traditional IDS | AI-Powered IDS |
|---|---|---|
| Detection Method | Rule-based, Signature-based | Machine Learning, Deep Learning |
| Adaptability | Limited to predefined rules | Adapts to new threats dynamically |

| | | |
|---|---|---|
| False Positive Rate | High in anomaly-based detection | Lower with advanced training techniques |
| Effectiveness in Microservices | Less effective due to static rules | Highly effective due to dynamic learning |
| Ability to Detect Zero-Day Attacks | Limited | Strong capability |

## III. PROPOSED SYSTEM ARCHITECTURE

### *A. Overview*

First, the system design entails the incorporation of the artificial intelligence in the intrusion detection systems to improve security in the microservice deployment. The advantages of AI are in the capability of the system in analyzing the network traffic, identifying an anomaly, and identifying the malicious activity as opposed to the rule-based techniques. It is very important to focus on the architectural aspects that directly relate to issues like scaling and interaction of microservices as well as distributed data flow that result in or lead to security vulnerabilities. The microservices had an intrusion detection system with AI functionality that serves as a middle layer responsible for looking into microservices' communications and patterns of behavior to detect suspicious activity in real-time.

This is a system which comprises of several components that form the basics of the security mechanism in an organization. An acquisition layer is used to obtain the network traffics, calls of application program interfaces and usage logs of microservices by users. These raw data inputs are further passed through feature extraction system so that they can be put into a status to fit into an Artificial Intelligence model. The detection module involves classification of the observations or events as normal or part of an attack, and the alarm generation module initiates the correct security action in response to threats detected.

The proposed solution is intended to be highly stress resistant guaranteeing that it can handle all network traffic in microservice based networks. It is building-block based and suitable for being deployed in cloud-native settings in modular components that include the usage of containers and compatibility with modern tools such as Kubernetes. Thus, the application of integrations with AI makes the system smarter since it is built to learn from the new security incidents to counter most of the new arising threats [13].

### *B. Components*

The system consists of four components that perform various functions in the intrusion detection process.
The Data collection is used to get the current information of the networks and log request-response patterns of the micro-service, Audit and authentication. This module provides for security data to be captured from interaction services to have in-depth evaluation and management.

The feature extraction module in a system is responsible for converting raw data into meaningful security-related features that could be important in eliciting appropriate reactions. As for the traffic characteristics, the packet size, connection time and the protocols are analyzed together with the system call features that describe the service interactions. This tabular information is helpful in categorizing of the network activities by the AI models.

The specific use of machine learning is that there is one that includes machine learning algorithms to identify intrusions. It also employs both supervised and unsupervised learning algorithms in pattern analysis, classification of the activity and its indication of suspicious activity. This is advantageous in the sense that the system raised on large datasets of normal and malicious traffic, thereby enabling it to characterize attacks patterns that a signature-based IDS may not be able to identify.

The alert generation module is the response component of the system and threatens notifications or initiates a defense mechanism as soon as the presence of a threat is indicated. Depending on the level of the intrusion, the system can only log the incident, inform the managers or take measures involving closing access for the suspicious Ip addresses or even isolating the intruded microservices.

## IV. AI-POWERED INTRUSION DETECTION

### *I. Machine Learning Algorithms*

The analysis of the network's activities within the microservice-based architecture is made possible using machine learning algorithms, which are critical in AI based intrusion detection systems. It is in contrast with the traditional rule-oriented systems which require specific signature of the virus in machine learning approach, one can analyze previous data and get unknown threats. In the process of machine learning-based detection, several models are trained on labeled data such that the abnormal activities can be identified from the normal ones.

Classification algorithms that are typically used in this context include decision trees, support vector machines (SVM), and random forest in which contain labeled data of normal and malicious activities. These ones process and check for patterns to create models that would distinguish and categorize the new instances of network traffic. They are very useful when there is enough labeled training data, thus, they provide close to 100% accuracy in identification of known type of attacks.

Other forms of learning include unsupervised learning where clustering is common in techniques such as the k-means and Deep autoencoders which are beneficial in learning new threats without initial data labeling. These methods address the issue of detecting anomalies from the ordinary, and typical behavior through the analysis of network traffic and other interaction. They are especially helpful in dynamic microservice scenario, in which new kinds of threats can appear rather randomly.

### *II. Deep Learning Algorithms*

The advanced techniques, widely known as deeper learning or deep learning, again improve the accuracy level with the intrusion detection by feeding vast data on the network traffic and analyzing the same for creating further complex pattern identification. These models apply chaptalized and multi-layered neural networks to achieve the sharing of features and features categorization, enabling them to easily identify complex cyber threats [4].

CNN is applied to image recognition, and it has also been adopted for use in network intrusion detection. Therefore, by employing CNNs to process the flow data in terms of grid-like structures, the positional correlations of the features are taken into consideration when identifying network attacks.

RNN has been found to be useful for sequential data analysis especially the LSTM (Long Short-Term Memory) and can be applied in IDS of microservices. These models detect slow temporal changes in the traffic patterns which a fast scan might not easily observe [6].

The best part in using machine learning and deep learning models in the ID system is that the detection of intrusions is maximized while at the same time reducing the number of false alarms. This would help in creating a well-developed security framework that can meet the emerging attacks paradigms.

### *C. Feature Extraction*

Feature extraction is a rather important element in the framework of IDS creation because it converts raw data into a set of features for further analysis by AI models. In the case of the AI-powered detection system, this is ratioed with a qualitative and relative measure of extracted features.

Network traffic characteristics may be such things as the packet size, duration of connection, protocol used, and the source and destination of connections. These features assist in knowing the normal communication pattern of the network to detect intrusion attempts.

Others include tracking microservices' interactions and function calls as well as request and authentication events [8]. Any abnormalities of these interactions may reveal illegitimate actions for instance when an unauthorized entity tries to gain access to a system or gain access to resources they are not authorized to request.

Thus, through developing an optimized feature extraction mechanism, the intelligent intrusion detection system can improve the effectiveness of threat detection with high efficiency during microservice-based applications [5].

Table 2: Comparison of Machine Learning and Deep Learning Algorithms

| Algorithm Type | Advantages | Limitations | Best Use Cases |
|---|---|---|---|
| Supervised Learning | High accuracy with labeled data; interpretable models | Requires large, labeled datasets; limited adaptability to new threats | Detecting known attack patterns and established threats |
| Unsupervised Learning | Can detect novel and unknown attacks; no need for labeled data | Higher false positive rates; complex tuning required | Identifying anomalous behaviors and zero-day attacks |
| Convolutional Neural Networks (CNNs) | Effective for pattern recognition in network traffic | Requires significant computational resources | Analyzing structured network traffic for intrusion detection |
| Recurrent Neural Networks (RNNs) | Suitable for sequential data analysis; detects temporal attack patterns | Susceptible to vanishing gradient problem; high training time | Monitoring time-series logs and detecting persistent threats |
| Hybrid AI Models | Combines strengths of multiple algorithms for improved detection | Increased model complexity; requires high processing power | Comprehensive threat detection across different attack vectors |

## V. EVALUATION

### *A. Dataset*

It is particularly important to understand that the performance of an IDS based on AI depends directly on the dataset used for making identification and evaluation. Indeed, for this work, it is employed the dataset of network traffic logs and records of performed system calls on microservice-based architectures. This means that the dataset has both normal and intrusive traffic patterns and includes DoS, SQL injected, and privilege escalation attempt.

In this step, the necessary preparations are made for the data to be suitable for the application of machine learning and deep learning techniques. This comprises of data pre-processing whereby some records such as those with missing or corrupt data are removed and data transformation where numerical features are standardized. Furthermore, methods from feature engineering are used to improve the characteristics and the discriminative capabilities of the model.

### *B. Evaluation Metrics*

The given method of evaluating the IDS focuses on its efficacy through the assessment of parameters such as accuracy and reliability of the IDS in identifying the intrusion. The primary metrics considered include:
Accuracy is one of the evaluation metrics as it determines the ratio of the total correct data points identified by the system. If precision is high, this means true positive detection is high among the total number of positives, meaning that the system does not produce many false alarms. Recall measures the ability of the system to detect all the threats and staying away from missing out on any actual threats. Namely, while precision can give an idea about the number of true positives out of the total predicted positives, recall can show the number of true positives out of all existing attack instances; thus, their combination gives the F1-score which can be effective for dealing with imbalanced datasets, where the attack instances are less than the normal activity.

### *5.3 Results*

The evaluation summary investigates how the developed IDS using AI natural language processing algorithm is capable of detecting threats in microservice-based architectures. The performance of the ML and dl methods is compared to identify which approach is the most effective for intrusion detection. The experiments reveal that most deep learning architectures such as RNNs and CNNs have better

performance than the classical machine learning algorithms in identifying intricate attacking behaviors. It also shows that the proposed AI-based system can produce fewer false positives when compared to the signature-based IDS which in turns result in enhanced operational efficiency and less alert fatigue to the security personnel. In addition, the system appears robust in recognizing new forms of threats and potentially new attack scenarios because the system seemed to be learning from the historical data and adjusting its detection models continually.

## CONCLUSION

### *A. Summary of Key Findings*

The paper discusses the use of IDS in microservice architectures responding to potential security issues related to the distribution of services. A wide range of techniques of intrusion detection based on the signature and anomalous methods failed to perform well in large-scale and dynamic environments. On the other hand, AI-based methods can use machine learning as well as, to improve the detection capability and flexibility. The study shows that, specifically, deep learning techniques incorporated in the CNN and RNN result in higher levels of detection of the attack behaviors [7]. The experiments presented in this paper show that the utilization of the proposed model improves the system accuracy as well as decreases the number of false positives making the system a reliable solution to microservices protection.

### *B. Future Research Directions*

The paper discusses the use of IDS in microservice architectures responding to potential security issues related to the distribution of services. A wide range of techniques of intrusion detection based on the signature and anomalous methods failed to perform well in large-scale and dynamic environments [3]. On the other hand, AI-based methods can use machine learning as well as, to improve the detection capability and flexibility. The study shows that, specifically, deep learning techniques incorporated in the CNN and RNN result in higher levels of detection of the attack behaviors [15]. The experiments presented in this paper show that the utilization of the proposed model improves the system accuracy as well as decreases the number of false positives making the system a reliable solution to microservices protection.

### *6.3 Implications for Practice*

The paper also analyzes the specifics of using IDS in microservice architectures when interacting with emerging threats linked to the distribution of services. The variety of the techniques used in the systems relying on the signature and anomalous approaches does not demonstrate good results when applied to large and complex environments. However, the AI-based methods have the potentiality of using the concepts of machine learning and to enhance the detection feature as well as the flexibility. This is particularly so because, according to the study, the improvement of the CNN and RNN through deep learning raises the levels of identification of the attack behaviors. This paper also demonstrated how the proposed model enhances the system accuracy and greatly reduces the number of false positives, which then makes the system a good solution to protecting microservices.

## REFERENCES

[1] Ahmad, I., & Jan, M. (2021). Enhancing cybersecurity in microservices: Deep learning techniques for intrusion detection. International Journal of Information Security, 20(4), 567–582.

[2] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[3] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

[4] Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 785–794).

[5] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28.

[6] Javed, M. A., Zhang, Y., & Khan, S. (2020). A comprehensive survey on intrusion detection

systems for microservice-based architectures. IEEE Access, 8, 12345–12359.

[7] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. IEEE Access, 4, 200–210.

[8] Jagdish Jangid, " Efficient Training Data Caching for Deep Learning in Edge Computing Networks" International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 6, Issue 5, pp.337-362, 2020. doi : https://doi.org/10.32628/CSEIT20631113

[9] Jangid, J., & Malhotra, S. (2022). Optimizing software upgrades in optical transport networks: challenges and best practices. Nanotechnology Perceptions https://nano-ntp.com/index.php/nano/article/view/5169

[10] Komal Azam1, Mashooque Ali Mahar2, Muhammad Saqib3, & Muhammad Saeed Ahmad4. (2024). Analyzing Deep Reinforcement Learning for Robotics Control. Spectrum of Engineering Sciences, 2(4), 416–432. Retrieved from https://www.sesjournal.com/index.php/1/article/view/86

[11] Kim, Y., & Kim, H. (2018). AI-based intrusion detection in microservice environments using deep learning. Journal of Network and Computer Applications, 112, 25–35.

[12] Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24.

[13] Machireddy, Jeshwanth, Harnessing AI and Data Analytics for Smarter Healthcare Solutions (January 14, 2023). International Journal of Science and Research Archive, 2023, 08(02), 785-798, Available at SSRN: http://dx.doi.org/10.2139/ssrn.5159750

[14] Machireddy, J. R. (2024). Machine Learning and Automation in Healthcare Claims Processing. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 686-701. https://doi.org/10.60087/jaigs.v6i1.335

[15] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, 305–316.

[16] Shubham Malhotra, Fnu Yashu, Abhijeet Malviya, " Serverless Mesh Architectures for Multi-Cloud and Edge" International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 10, Issue 1, pp.326-329, 2024. doi: https://doi.org/10.32628/CSEIT2425446

[17] Sachin Dixit, & Jagdish Jangid. (2024). Asynchronous SCIM Profile for Security Event Tokens. Journal of Computational Analysis and Applications (JoCAAA), 33(06), 1357–1371. https://eudoxuspress.com/index.php/pub/article/view/1935