EasyChair Preprint

№ 12822

Effective DDoS Security Scheme for Mobile Cloud Computing Systems

Chaima Ishak and Yosra Ben Saied

March 28, 2024

Effective DDoS security scheme for mobile cloud computing systems

Chaima Ishak, *ISSAT Mateur*, Yosra Ben SAIED, *Carthage University*

***Abstract*— With the increasing use of mobile Cloud Computing systems (MCC) in various domains, including offices, homes, hospitals, and transportation, Distributed Denial of Service (DDoS) attacks have become more frequent and complex, posing new challenges and risks. Therefore, enhancing the three defense mechanisms (prevention, detection, and mitigation) is crucial. In this paper, we propose a machine-learning model that utilizes neural network techniques, such as an Evolutionary recurrent self-organizing map (ERSOM), in combination with a K-means classifier to detect botnet attacks and ensure the establishment of all defense mechanisms in mobile cloud computing system. Our performance results demonstrate the effectiveness of the proposed adaptive ERSOM model compared with the literature.**

***Index Terms*— Mobile Cloud Computing, Neural network, DDoS, Detection, Prevention, Mitigation**

INTRODUCTION

As the number of mobile devices continues to rise and cloud computing becomes more and more common, it is critical to make sure that data and services are secure and accessible. The integration of mobile devices agility with cloud infrastructure's scalability, known as mobile cloud computing, has become a game-changing concept. But it also presents an extensive number of security risks, the most significant is the constantly changing threat landscape posed by DDoS attacks. Mobile devices may send erroneous information, such as during a data poisoning attempt, or an attacker can inject fake nodes into these devices, so it is crucial to build systems that inform about malicious attacks. Anything different than what is considered to be normal activity can be interpreted as an attack or an anomaly, so the objective is to identify the emergence of new events that are unexplained, attacks such as Distributed Denial of Service (DDoS), botnets launch this attack, it employs a network of connected devices to bring down a website or network to interrupt activities in these settings or interrupt the main services of the specific application [1].

In response, various security solutions, including detection and prevention mechanisms, have been recommended to address malicious behaviors, anomalous activities, and the identification of diverse attacks and abnormalities. The integration of Machine Learning (ML) methods into mobile devices is important for establishing robust security and privacy measures. ML techniques in cybersecurity are effective in detecting malicious activities, such as botnet attacks.

This paper proposes the development of an innovative neural network based on an evolutionary recurrent self-organizing map (ERSOM) [2], emphasizing its critical role in the future success of ML. The remainder of this paper is organized as follows: Section II presents related work and background information on DDoS defense mechanisms, while Section III introduces the proposed solution and provides details about the dataset used in this study. Section IV discusses the results, and Section V concludes the paper.

RELATED WORK:

The latest research offers several ways to counteract DDoS attacks, such as machine learning techniques for botnet and attack detection. However, these approaches only address one or two defense mechanisms, without taking all of them into account (prevention, detection, and mitigation). We examine many earlier studies in this field of study that are relevant to our work in this section.

Data security is one of MCC's main problems. Creating a system that ensures security and permits access to shared sensitive data has been the subject of recent research [3-11-1]. The key generation center (KGC) is situated within a cloud environment, making it a potential target server for attackers seeking to disrupt the KGC's services through DoS assaults. As a result, this architecture is ineffective for engagement against DDoS attacks. Such interruptions may have catastrophic effects if the generation and distribution of secret keys could potentially be under threat if there is a chance of a successful attack against the KGC. This leads to several negative consequences, including an issue in communication. Users will not be able to interact securely if they cannot get encryption keys from the KGC, thereby establishing a single point of failure.

A. Defense Mechanisms against DDoS attacks:

Given that DDoS attacks have the greatest possibility of rendering resources unavailable in comparison to other threats, security methods against them need to be as strong as the attacks' sophistication. In this part, we provide a taxonomy of the well-known and most used defense mechanisms of DDoS attacks, including prevention, detection, and mitigation [3].

In [23-6-7-9], an analysis of DDoS defense mechanisms is presented highlighting that existing work has primarily

considered one or two specific defense mechanisms, and none of them considered all defense techniques together.

1. *Detection mechanisms:*

DDoS attack detection is a critical component of cloud security. DDoS attacks can overwhelm cloud resources, making them unavailable to legitimate users. There are several different DDoS attack detection techniques, each with its advantages and disadvantages [6].

- *Anomaly-based detection:*

Anomaly-based detection is a common technique that involves analyzing network traffic for patterns that deviate from normal behavior. Machine learning can be used for anomaly-based detection and is often used to develop anomaly-based detection systems because it can learn to identify patterns in data that are difficult or impossible to identify using traditional methods as explored in [17].

A CNN considered in the context of Android malware detection obtains an impressive accuracy rate of 89.7% [19], demonstrating its efficiency in protecting mobile devices. Moving on to [20], a DNN specializing in botnet detection offers a phenomenal accuracy of 96.8%, demonstrating its ability to secure desktop computers. [21] provides an LSTM model that is deliberately deployed at the fog layer and has an amazing accuracy of 99.91% in spotting vulnerabilities connected with wireless communication assaults. Finally, [22] shows that a hybrid LSTM-CNN model is exceptionally effective in identifying network malware with a remarkable accuracy of 99.83% when applied on desktop devices with GPU capabilities.

Also [2] proposed an Evolutionary Recurrent self-organizing Map (ERSOM) algorithm that integrates principles from evolutionary computing, recurrent neural networks, and self-organizing maps to create a robust framework for identifying anomalies in industrial processes.

- *Signature-based detection:*

Signature-based detection is a popular cybersecurity solution that works by checking incoming network traffic against a database of known threat signatures. When an incoming traffic pattern matches a recognized signature, the system flags the traffic as malicious and stops it. As mentioned in reference [28], this strategy is quite effective in recognizing and mitigating known attacks with established signatures. However, it has a limitation in that it is vulnerable to new or zero-day attacks because they lack pre-existing signatures in the database, making signature-based detection less effective in such cases, as explained in [18], because attackers become more sophisticated and develop new ways to evade signature-based detection. As a result, academics are creating new detection approaches, such as anomaly-based detection.

- *Hybrid-based detection*

Hybrid-based detection combines signature-based and anomaly-based methods. It initially employs signature-based detection to identify known attacks. If no signature match is found, the system then utilizes anomaly-based detection. While effective for both known and unknown attacks, hybrid-based detection tends to be more complex and computationally demanding compared to alternative detection techniques. [15] discovered that hybrid-based detection, such as AI-HydRa [25], produces fewer false positives compared to standalone signature-based or anomaly-based detection. This is attributed to the hybrid approach's utilization of multiple techniques to confirm the occurrence of an attack before triggering an alert.

2. *Mitigation Mechanisms:*

- *Software-based and Hardware-based Firewall Against the DoS and DDoS Attacks:*

Firewalls effectively mitigate DDoS attacks, reducing their impact. Adhering to fundamental firewall standards makes these attacks less effective [27]. For enhanced cloud computing security, deploy a combination of software-based and hardware-based Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). These solutions, utilizing stateful protocol analysis, signature-based, and statistical anomaly-based methods [26], detect and prevent attacks efficiently.

- *Victim Migration:*

The idea of a victim migration is to shift the entire running server, during a DDoS attack, to another physical server with unnoticeable downtime. The new server that was shifted is isolated from the DDoS attack. After detecting and mitigating the attack, the work is returned to the old "main" server [18]

Among the innovative solutions in this domain, honeypots have gained significant attention as a powerful defense strategy. Honeypots are decoy systems [15] or network components strategically placed within an infrastructure to lure and engage potential attackers. They operate by diverting malicious traffic and attacks away from legitimate resources, effectively serving as a sacrificial target.

3. *Prevention Mechanisms:*

Prevention mechanisms consist of protecting the cloud resources and services from DDoS attacks. DDoS attack prevention is built on the management of network traffic, rescheduling, and hidden proxy/server [2].

Filtering encompasses six methods employed to proactively prevent attacks, Ingress Filtering utilizes routers to block incoming packets originating from spoofed IP addresses and Egress Filtering permits packets with legitimate IP addresses within a specified network range to exit the network using outbound filters [11].

History-based IP Filtering establishes an IP address database (IAD) during normal traffic to record the history of frequently used destination IP addresses. This method aids in preventing DDoS attacks by disregarding any IP address not present in the IAD. Hash and bloom techniques are applied to search for the source IP address in the IAD. However, this approach is less effective when attackers use legitimate IPs to launch DDoS attacks [20, 21]. Source Address Validity Enforcement Protocol (SAVE) enhances the Route-Based Distributed Packet Filtering method by introducing a protocol that compels source routers to transmit updated information regarding expected and unexpected IP addresses to each destination router. This information is then employed to filter out spoofed IP addresses [20, 21].

Challenge-response protocols (CRPs) play a pivotal role in discerning the authenticity of incoming requests within a system, aiming to differentiate between legitimate users, automated bots, and potential attackers. The primary objective is to verify if a request originates from a genuine user, and CRPs

employ the Turing test through mechanisms like CAPTCHA [29] or Crypto puzzles [1]. On a parallel front, Restrictive Access emerges as a defensive strategy, permitting controlled access to the service. This technique strategically introduces delays in responses or access for presumed attackers and even additional clients. The delay implementation involves prioritizing legitimate clients or favoring those with a history of positive interactions, contributing to a more secure and discerning access management approach [18].

DISCUSSION:

The existing landscape of DDoS defense mechanisms reveals certain limitations that necessitate the exploration of innovative solutions. The current ways we defend against DDoS attacks, like using CNN, DNN, LSTM, and CNN-LSTM, have some weaknesses. These weaknesses are clearly shown in Table I, where we list the problems with each method. Looking at this table, it is clear that we need a better, smarter way to defend against DDoS attacks. Table I highlights the issues with the existing methods, and it tells us we need a defense mechanism that can handle these problems more effectively. We are essentially aiming for a new and improved defense strategy that not only fixes the issues pointed out in the table but also adapts to new challenges that may come up during DDoS attacks.

We found security drawbacks in the mobile cloud computing architecture due to the centralized key generator center's design, creating a vulnerability with a potential single point of failure if maliciously targeted.

To enhance security, recognizing the importance of lightweight encryption in the distributed key generator center is crucial. Existing literature often focuses on network traffic anomaly detection but lacks comprehensive support for alternative defense mechanisms.

TABLE I
COMPARATIVE ANALYSIS OF DDoS DEFENSE AND PREVENTION MECHANISMS: DISADVANTAGES OVERVIEW

Types	**Mechanisms**	**Disadvantages**
Detection	CNN	Limited adaptability to dynamic network traffic
	DNN	Lack of robustness in handling complex patterns
	LSTM	Challenges in addressing real-time network variations
	CNN-LSTM	Combined limitations of CNN and LSTM
Prevention	IP Spoofing Checks	Vulnerable to advanced IP spoofing techniques
	History-based IP Filtering	Limited in handling evolving attack patterns
	Challenge-response protocols	Susceptible to man-in-the-middle attacks and replay attacks
Mitigation	Software-based Firewall	Resource-intensive, impacting overall system performance
	Hardware-based Firewall	Limited in handling evolving attack patterns

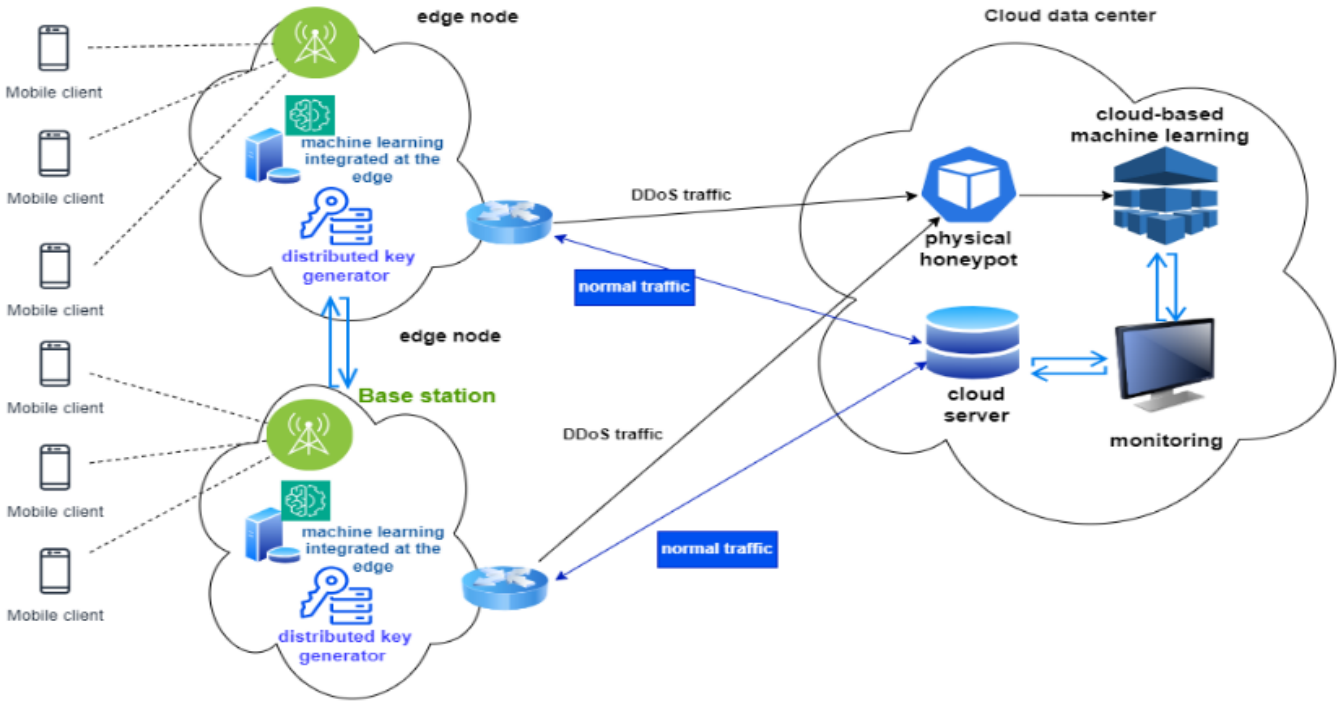

Fig. 1: The proposed architectural defense against a DDoS attack

PROPOSED SOLUTION:

The proposed architecture as shown in Fig. 1 consists of end-user devices (mobile devices) that are used to access the cloud computing environment through edge nodes deployed close to it, to perform a variety of tasks, including traffic filtering, caching, and load balancing. In the edge node, machine learning is used to detect and mitigate DDoS attacks. The machine learning model is trained on historical data of DDoS attacks and legitimate traffic. The trained model is then deployed on the edge nodes. This allows the edge nodes to detect and mitigate DDoS attacks quickly and effectively.

A DKG is used to generate and distribute keys to the edge nodes and mobile devices. This makes it more difficult for attackers to compromise the KGC and launch DDoS attacks.

Additionally, a honeypot is used to attract and deceive attackers. This can help to waste the attacker's resources and to collect information about their methods and tools. This information can then be used to improve the detection and mitigation of DDoS attacks.

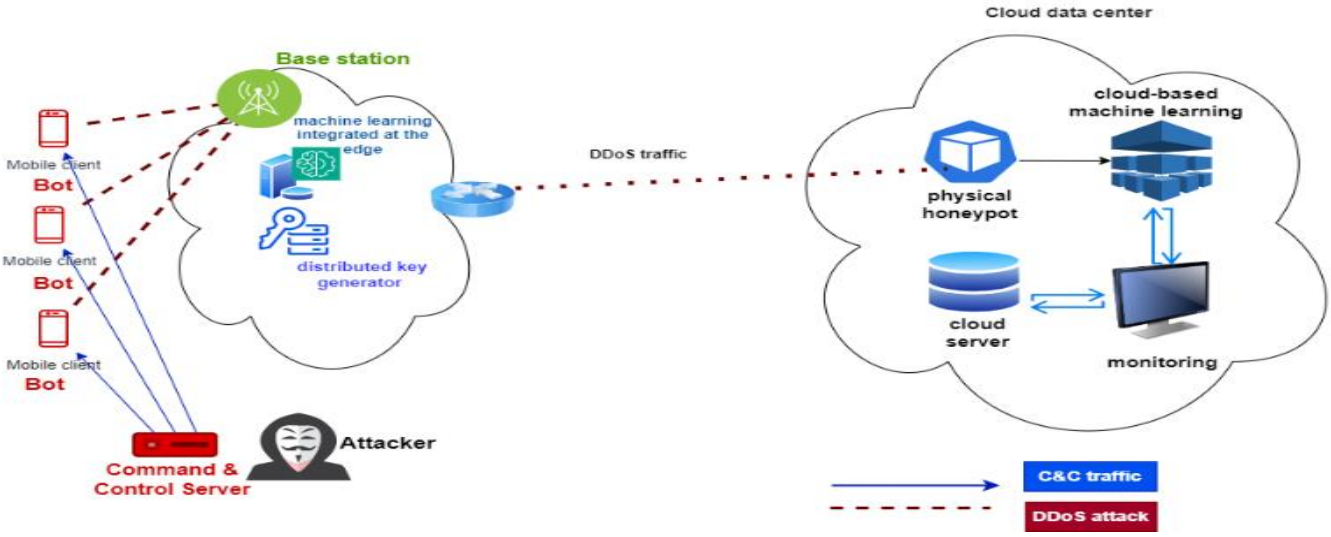

Fig. 2: Mitigating Mobile Cloud Computing DDoS Attacks: A Cybersecurity Framework Against C&C Command Assaults

The following measure is taken to ensure the availability and confidentiality of data, the data is replicated across multiple edge nodes and the cloud data center. This ensures that the data is available even if one of the components fails.

The plan protects a mobile cloud system from DDoS attacks by using different defense methods. It also eases the load on cloud servers, speeds up responses for mobile devices, and uses lightweight cryptography to save battery power.

As shown in Fig. 2, the attackers established a command and control (C&C) server, which is a hidden server on the internet that serves as the central hub for controlling the botnet. This server communicates with the infected devices by sending commands and instructions. When the attacker decides to begin a DDoS attack, they send commands to the command and control server, ordering it to activate the botnet. The C&C server then passes these orders to the hacked devices, ordering them to send malicious traffic to the intended victim. The botnet's deluge of traffic overwhelms the intended victim's network resources, rendering them unavailable to normal users. Slow response times, dropped connections, or even total denial of service may be experienced by the victim.

THE ADAPTIVE ERSOM ALGORITHM:

In developing our solution for the challenges posed by the MCC environment, we strategically chose to leverage the ERSOM algorithm. Recognizing its potential for anomaly detection and pattern recognition, we have undertaken the task of adapting the ERSOM algorithm to suit the specific intricacies of the MCC domain. This adaptation aims to optimize the algorithm's performance in the context of mobile devices accessing cloud resources, addressing the unique characteristics and demands of MCC scenarios. By tailoring the ERSOM algorithm to the MCC environment, we anticipate enhancing the accuracy and efficiency of anomaly detection in this dynamic and resource-constrained setting.

The ERSOM algorithm merges two machine learning techniques, the self-organizing map (SOM) and the genetic algorithm (GA). The SOM organizes data into a grid of nodes, each representing a group of data points, by learning to map them onto the grid through training. Meanwhile, the GA, a search algorithm, generates and evaluates solutions based on a fitness function, selecting the best ones to further refine solutions. The ERSOM algorithm initializes a SOM with training data and evolves it over time using GA, aiming to create a SOM proficient in identifying outliers.

The ERSOM algorithm's process involves creating a SOM with training data and evolving it using GA to accurately pinpoint outliers. This algorithm excels in anomaly detection, adept at learning intricate patterns even in noisy or incomplete data. It can identify outliers in real-time. The adaptive ERSOM algorithm creation includes initializing a SOM, training it on data, evolving it with a genetic algorithm, and repeating until the SOM effectively identifies outliers, Fig.3 shows all these steps.

In our proposed algorithm, the fitness function is the formula of the Manhattan distance:

$$\textbf{Manhattan distance } (x, y) = \Sigma |x_i - y_i|$$

where x is the current traffic pattern and y is the historical traffic pattern. Each xi and yi is a feature of the traffic pattern, such as the number of packets per second, the number of bytes per second, or the distribution of packet sizes.

If the Manhattan distance between the current traffic pattern and the historical traffic pattern is greater than a certain threshold, then this may indicate an anomaly.

In the realm of DDoS detection, the Manhattan distance reigns supreme over the Euclidean distance due to its inherent strengths in dealing with the characteristics of DDoS attacks. While both distances detect anomalies, the Euclidean distance, by squaring feature differences, magnifies the impact of outliers, potentially masking true attacks hidden within the noise. This vulnerability stems from the inherent nature of DDoS attacks, which involve overwhelming a system with a surge in traffic, leading to significant deviations from normal patterns. The Manhattan distance, on the other hand, excels in this scenario due to its focus on absolute differences. This approach assigns less weight to extreme values, making it less susceptible to the skewing effects of outliers. Consequently, the Manhattan distance offers a clearer picture of the underlying traffic patterns, allowing the system to effectively differentiate between normal fluctuations and the significant deviations indicative of a DDoS attack. Furthermore, the Manhattan distance boasts advantages in terms of computational efficiency and interpretability, making it a more suitable choice for real-time DDoS detection scenarios. Its efficient nature allows for faster anomaly detection and mitigation, while its interpretability facilitates the understanding of the attack, enabling the implementation of targeted countermeasures. In essence, the Manhattan distance's resilience against outliers, computational efficiency, and interpretability collectively empower the DDoS detection system with the necessary tools for robust and reliable identification and mitigation of attacks.

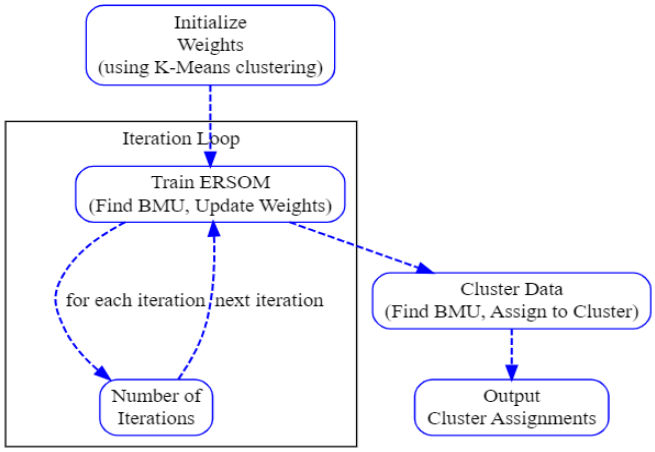

Fig. 3: Representation of our adaptive ERSOM algorithm

EXPERIMENT AND RESULTS:

During this study, we utilized PyCharm on Python 3.11, operating on a 64-bit Windows 10 system with 8GB of RAM and a 2.20 GHz CPU core i5 to handle extensive datasets efficiently. For data pre-processing and analysis, we employed the powerful WEKA machine-learning tool.

Figure 4 shows our proposed model for detecting DDoS attacks in a dataset

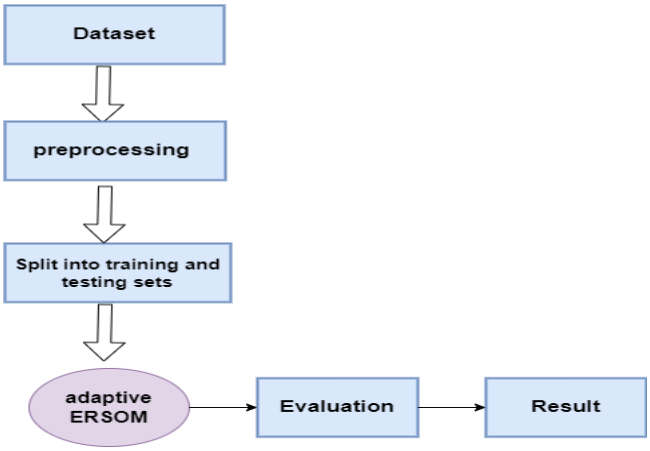

Fig. 4: Process for Machine Learning Model Evaluation

A. Dataset

The CICDoS2019 dataset is a public dataset created by the Canadian Institute for Cyber Security (CIC). The dataset contains data on network traffic from DDoS attacks generated using a variety of attack tools and techniques. The dataset contains a total of 80 million network flows, including both legitimate and malicious traffic.

In this dataset, we have different modern reflective DDoS attacks such as PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, and SYN. Attacks were subsequently executed during this period, the dataset executed 7 DDoS attacks including LDAP, MSSQL, NetBIOS, Portmap, UDP, UDP-Lag, and SYN.

B. Data pre-processing

This study proposes the following pre-preprocessing steps: encoding, handling missing values, removing redundant values, sampling, and feature selection.

For these steps, we use WEKA (Waikato Environment for Knowledge Analysis) a free open-source machine learning tool that has been built on the Java platform. The pre-processing tab in WEKA allows us to use filters like Remove duplicates and others.

C. Results and Comparisons with other studies:

In Table II, we compare our proposed adaptive ERSOM algorithm with other neural network algorithms like DNN and CNN, LSTM, and CNN-LSTM, these existing studies have less percentage of precision, recall, and f1 score than our adaptive algorithm proving the viability of our proposed solution in the studied context of DDoS detection in the MCC environment.

TABLE II
THE RESULTS OF OTHER SIMILAR STUDIES

	A-ERSOM	**DNN**	**CNN**	**LSTM**	**CNN-LSTM**
Precision	**100%**	**99.18 %**	**99.96 %**	**98.89 %**	**99.77 %**
Recall	**100%**	**57.77 %**	**98.68 %**	**98.94 %**	**98.93 %**
F1	**100%**	**73.61 %**	**99.32 %**	**98.91 %**	**99.35 %**

Results showed that all the evaluation metrics of our solution consistently score 100%. This achievement signifies the effectiveness of our proposed algorithm in identifying DDoS attacks with precision.

V. Conclusion

In conclusion, the proposed architecture for mobile cloud computing, relying on edge nodes empowered with machine learning, signifies a significant leap forward in enhancing the security and effectiveness of the system. The adaptive ERSOM algorithm, showcased in this framework, has demonstrated an impressive 100% accuracy in detecting, mitigating, and preventing DDoS attacks. This not only strengthens the resilience of the mobile cloud environment but also contributes to the overall reduction in computational power consumption and extends the battery life of mobile devices. By effectively offloading computational tasks to the edge node, the proposed architecture not only reduces the strain on mobile devices but also alleviates the burden on cloud servers, thereby optimizing resource utilization.

References

[1] D. Radain, S. Almalki, H. Alsaadi, and S. Salama, "A Review on Defense Mechanisms Against Denial of Service (DDoS) Attacks on Cloud Computing," in *International Conference of Women in Data Science at Taif University*, Taif, Saudi Arabia, 2021.

[2] M. S. Salhi, S. Kashoobb, and Z. Lachiric, "Progress in Smart Industrial Control based on Deep SCADA," *Turkish Online Journal of Qualitative Inquiry*, vol. 12, no. 8, 2021.

[3] P. Farina, E. Cambiaso, G. Papaleo and M. Aiello, "Understanding DDoS Attacks from Mobile Devices," in *3rd International Conference on Future Internet of Things and Cloud*, Italy, 2015.

[4] A. Khadija, G. Micheal and H. Hamid, "Mobile cloud computing for computation offloading: Issues and challenges," *Applied Computing and Informatics*, vol. 14, no. 1, pp. 1-16, 2018.

[5] X. Lu, Z. Pan, and H. Xian, "An efficient and secure data sharing scheme for mobile devices in cloud computing," *Journal of Cloud Computing: Advances, Systems, and Applications*, vol. 9, no. 60, 2020.

[6] A. Mahfouz, A. Abuhussein, D. Venugopal and S. Shiva, "Ensemble classifiers for network intrusion detection using a novel network attack," *Future Internet*, vol. 12, pp. 1-19, 2020.

[7] B. AlDuwair, Ö. Özkasap, A. Uysal, C. Kocaoğullar, and K. Yildirim, "LogDoS: A Novel logging-based DDoS prevention mechanism in path identifier-Based information centric networks," *Computers and Security*, vol. 99, 2020.

[8] M. P. NOVAES, L. F. CARVALHO, J. LLORET, and M. L. PROENÇA, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network," *IEEE Access*, vol. 8, pp. 83765-83781, 2020.

[9] J. A. Filho, L. Brandão, B. Fernandes and A. Maciel, "A review of neural networks for anomaly detection," *IEEE Access*, vol. 10, pp. 112342-112367, 2022.

[10] M. A. Kohnehshahri, R. Mohammadi, H. Abdoli and M. Nassiri, "An Efficient Method for Online Detection of DRDoS Attacks on UDP-Based Services in SDN Using Machine Learning Algorithms," *Mobile Information Systems*, vol. 2022, p. 13, 2022.

[11] R. Ma, Q. Wang, X. Bu and X. Chen, "Real-Time Detection of DDoS Attacks Based on Random Forest in SDN," *Applied Sciences*, vol. 13, no. 13, 2023.

[12] J. Raj and e. al., "A Novel Encryption and Decryption of Data using Mobile Cloud Computing Platform," *IRO Journal on Sustainable Wireless Systems*, vol. 2, no. 3, 2021.

[13] L. B. Mehmedovic, "Edge AI: Reshaping the Future of Edge Computing with Artificial Intelligence," in *Basic technologies and models for implementation of Industry 4.0*, Sarajevo, Bosna and Herzegovina, 2023.

[14] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-Edge AI: Intelligentizing Mobile Edge Computing, Caching, and Communication by Federated Learning," *IEEE Network*, vol. 33, no. 5, pp. 156-165, 2019.

[15] A. N. Cahyo, A. K. Sari and M. Riasetiawan, "Comparison of Hybrid Intrusion Detection System," in *12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Yogyakarta, Indonesia, 2020.

[16] J. Franco, A. Aris, B. Canberk and A. S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351-2383, 2021.

[17] T. Yang, M. Qin, N. Cheng, W. Xu and L. Zhao, "Liquid Software-Based Edge Intelligence for Future 6G Networks," *IEEE Network*, vol. 36, no. 1, pp. 69-75, 2022.

[18] S. E. Kafhali, I. E. Mir and M. Hanini, "Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing," *Archives of Computational Methods in Engineering*, 2021.

[19] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications*, vol. 107, pp. 30-48, 2017.

[20] N. McLaughlin, A. Doupé and G.J.Ahn, "Deep Android malware detection," in 7th ACM Conf. Data Appl. Secure. Privacy, Proc, 2017

[21] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network

for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, 2016.

[22] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in Fogto-Things communications," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124-130, 2018.

[23] J. Yan, Y. Qi, and Q. Rao, "Detecting malware with an ensemble method based on deep neural network," *Secur. Commun. Network*, pp. 51964-51974, 2018.

[24] J. Jiang, C. Lin, G. H. Adnan, M. Abu-Mahfouz, S. B. H. Shah and M. Martínez-García, "How AI-enabled SDN technologies improve the security and functionality of industrial IoT network: Architectures, enabling technologies, and opportunities," *Digital Communications and Networks*, 2022.

[25] S. Yoo, S. Kim, S. Kim, and B. B. Kang, "AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification, Information Sciences," *Information Sciences*, vol. 546, pp. 420-435, 2021.

[26] F. Guenane, M. Nogueira and A. Serhrouchni, "DDOS Mitigation Cloud-Based Service," in *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015.

[27] A. Balobaid, W. Alawad, and H. Aljasim, "A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques," in *International Conference on Computing, Analytics and Security Trends (CAST)*, 2016.

[28] P. Szynkiewicz, "Signature-Based Detection of Botnet DDoS Attacks," *Cybersecurity of Digital Service Chains*, vol. 13300, 2022.

[29] N. T. Dinh and V. T. Hoang, "Recent advances of Captcha security analysis: a short literature review," *Procedia Computer Science*, vol. 218, pp. 2550-2560, 2023.

[30] V. Prakash, N. Bharathiraja, R. D. Nayagam, R. Thiagarajan, R. Krishnamoorthy, and J. Omana, "EB Algorithm for Effective Privacy and Security of Data Processing in MCC," in *International Conference on Electronic Systems and Intelligent Computing (ICESIC)*, India, 2022.

Chaima Ishak graduated in 2023 from the Higher Institute of Applied Science and Technology of Mateur (ISSAT Mateur), where she obtained her International Master's degree in Cyber-Physical Systems. In 2019 she obtained an Applied Master's degree in Networks and Telecommunication specializing in services and security of networks. Her research activities consist of developing network security solutions. She especially focuses on using Machine Learning techniques to secure network environments.

Yosra Ben SAIED, PhD graduated from Telecom SudParis, France in 2013. She is now working as an assistant professor at Carthage University, Tunisia. She is also a member of the committee program of the IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN). Her main topics of interest are related to network security and privacy in the Internet of Things, wireless sensor networks, and Cloud Computing.