Detection and Prevention of MAC Spoofing in Cloud Data Centres

Mohan Reddy Y [1*] and Ashok Kumar Thavani Andu [2]

[1]Research Scholar, School of Science and Computer Studies CMR University, Bangalore, India

[2] Professor, *School of Science and Computer Studies CMR University Bangalore*, *India*

mohan.reddy@cmr.edu.in

Abstract. Computer Networks contributes to major part of data communication between organisation or any individuals in the current Century. Data storage and retrieval has become an essential part of any individual or organization from anywhere which has led to the advent of storing in single location and accessing it on the go, the days are gone where data is carried using external devices, through the advent of Cloud storages provided by many providers like google, amazon, IBM, Microsoft all data is stored in it for least cost. Also cloud based services is also provided by these vendors for organization and developers so that work from home or from anywhere can be done. Since the resources are shared among organization and individual in the cloud leads to security issues. Cloud provides services at three levels to cater to the needs of the customer such as "Software as a Service" (SaaS), "Infrastructure as a Service" (IaaS) and "Platform as a Service" (PaaS). Threats are common in each level. In a network all computers communicate through a unique "Internet Protocol" (IP) address and "Medium Access Control" (MAC) address, each computer in a network is assigned an IP address so that communication is unique, where as if MAC address itself, if spoofed or duplicated by attacker then it ends up affecting at PaaS level which in turn effects the upper services also. To prevent this kind of attack on PaaS level MAC spoofing must be detected and prevented so that the attacks like "Denial-of-Service" (DoS), "Distributed-Denial-of-Service" - DDoS, "Man-In-The-Middle" (MITM) can be prevented. There are various techniques and algorithms to prevent the attack but with pros and cons, A new technique is required to prevent this MAC spoofing at edge level instead of router level is proposed.

Keywords: Man In the Middle Attack, Distributed Denial of Services, Address Resolution Protocol Spoofing, Cloud Computing, Platform-as-a-Service.

1 Introduction

Computer Networks contributes to major part of data communication between organization or any individuals without which economy of country or any individual cannot be visualized. Consequently, the data that we use in daily life need to be stored and

H. L. Chidananda et al. (eds.), *Proceedings of the 2nd International Conference on Innovations and Challenges in Financial Technology (ICICFT 2025)*, Advances in Economics, Business and Management Research 398,
https://doi.org/10.2991/978-94-6239-772-9_31

retrieved by multiple devices. To cater to these needs, data centres are used by organisations to perform their day-to-day activities, since all the data or services that are needed by employees or any end user are required 24/7, 365 days, it has to be ensured there is no down time for these systems, where in security becomes biggest concern which should be addressed. Here MAC spoofing must be prevented at data centre level to prevent DDOS attacks or Man In Middle attacks by intruders to protect the Data or services of an organisation or an individual. In the paper, the impact of MAC spoofing in Cloud Data Centre services due to various security threats is reviewed.

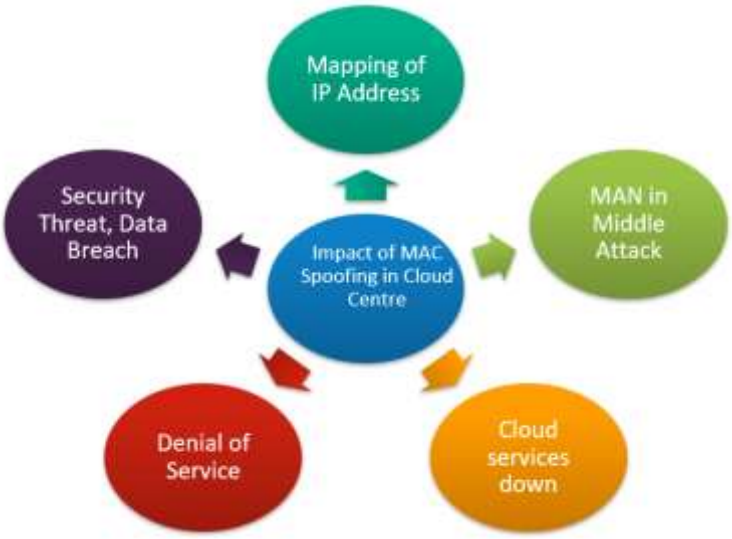

Fig. 1. Representing the Impact of MAC spoofing in Cloud centre

2 Literature Review

2.1 Security Threats in Cloud Server

Ramachandra *et al*[1] surveyed security concerns in Cloud environments and also discussed preventive methods to detect attacks on the cloud-based services. Cyber Attacks in cloud environment is increasing due to which expenditure on cloud-based security is also increasing at the rate of 10% every year from 2015 onwards, which has been highlighted by various research organisations such as Forbes, International Data Corporation and others. To prevent the threats in the cloud basically one needs to know the various components which build the cloud, so that at which level there is more threat need to be figured out and tackled. Why there is threat, in fact in the cloud becomes the point of research, the answer for the question is most organisation is shifting their hosting services from their traditional way to cloud, because cloud based computing is becoming more viable to the organisations growth. Farsi et al[2], has reviewed on "Data Security

Threats" in Cloud computing. Moving from traditional data storage to a distributed computing services has opened security vulnerability on Data storage and retrieval at single and multi-cloud data security, The limitations of security techniques that are taken care to prevent data loss are discussed. Islam *et al*[3], has discussed challenges encountered by cloud computing service providers by distinctly classifying the types of threats which are based on its characteristics. Privacy of data in cloud environment becomes increasingly challenging since it is completely dependent on third party service providers and the type of security provided depends solely on them, since there is no direct control by the organisation. Security threats in a network always existed from the day computers are interconnected at various levels, which increases with respect to cloud environment since, cloud environment comprises of various features like, data sharing and network sharing by multiple organisations and individuals. Shaikh and Haider[4], has discussed various types of services and resources provided by leading organisations in the internet like google and Microsoft and also security challenges faced. The ease of usage of cloud services provided by various organisation in the internet has increased consumers to shift from the traditional way of storing data and retrieval of data over internet managed by themselves due to cost of maintenance on their own. Threats are common in open systems but that will increase when resources and services are shared among the potential users in the network environment since it is maintained by data centres. Security involved majorly depends on the provider and due to which a question arises, is my data secure in cloud. To answer this question analysis of multiple security models are proposed which enhances security in cloud environment. Rao and Selvamani[5], has highlighted challenges faced in providing solutions to secure data in an Cloud computing Environment. Cloud services are provided by various organisations such as amazon, IBM, google, Microsoft etc to developers and individuals to access services globally via internet from any device has given rise to security concerns also, since services are accessed through remote systems.

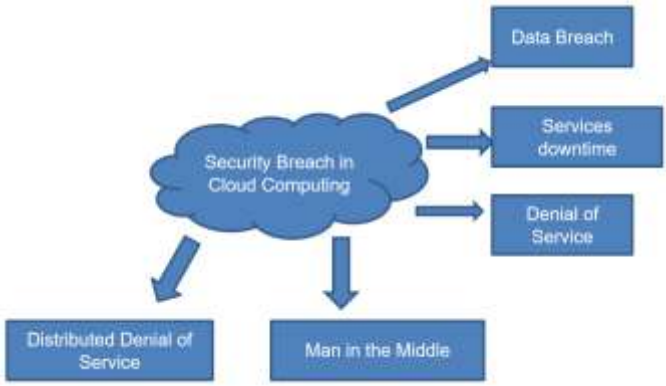

Fig. 2. Security Threat in Cloud computing leads to MITM, DoS, DDoS, Services down time, Data Breach

2.2 Impact of ARP spoofing in PaaS

Christopher and Divya[6], have reviewed various mechanisms to detect attacks and also prevent it due to "Address Resolution Protocol" (ARP) poisoning. ARP allows the computer to communicate data, but it is not designed to prevent attacks, at this MAC layer due to which attacks like cloning, DoS and MITM are a very common issues. To tackle this issue few techniques and its advantages are discussed. Prabadevi et al[7], has reviewed the effect of ARP spoofing in medical computing implemented in cloud based services. Due to the availability of resources in internet at least cost organisation tend to move their crucial and sensitive data from their traditional servers to cloud based services such as details of their customers which becomes a threat to the customer and organisation when an attack at PaaS level is encountered. The authors in this paper have taken the medical domain for analysis purpose how to tackle the issue when ARP is spoofed by the attacker. They have analysed existing solutions and disadvantages of it and proposed three new techniques to detect and prevent ARP spoofing. Isharufe et al[8] has done a study on threats that are encountered when Platform-as-a-Service is utilised by organisation. Security is the major concern when platform which is supposed to be maintained by the organisation is maintained by third party vendors due to low cost of maintenance in resources sharing among other organisations. The authors here discuss inherent security issues in PaaS and recommended solutions to overcome the threats. Merino et al[9], has done a survey on the risks that are encountered in multitenant software platforms and proposed the solutions to tackle the attacks at PaaS level. Multitenant platforms allow more than one organisation to share the platform as a resource which opens up the security threat from other software which might interfere and affect the service executed by some other organisation. Jaber et al[10], has reviewed security threats triggered by ARP poisoning and highlight the type of threats such as DoS, DDoS Attacks, which affects the organisation business when hosted in cloud environment.

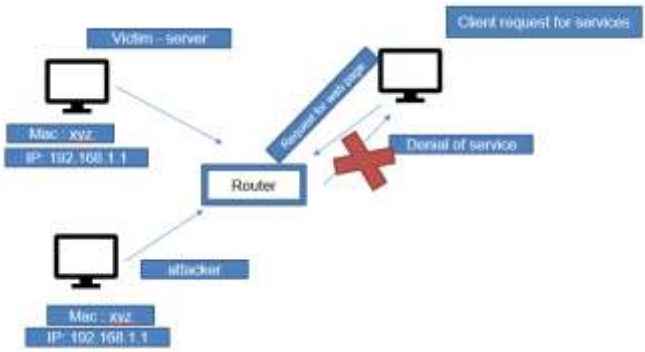

Fig. 3. Impact of ARP spoofing in PaaS, Denial of Service

2.3 Detect "Denial-of-Service" and "Distributed-Denial of-Service" attacks in cloud

Masdari & Jalali[11], has done survey related to DoS attack in Cloud environment, It is classified as one of the attacks which is a common security threat in cloud models which impacts services over a time period that shuts down services. The authors provide in their study, the vulnerability that are available in DoS attacks, they provide the solutions to prevent attacks in future. Chonka and Abawajy[12], has discussed about the HX-DoS attack on Cloud Web services, here attack on Denial of services is with the combination of HTTP with XML messages which are used to overload the server and make the communication channel busy, to effect services offered by the provider to disturb services for a while, which is done intentionally to bring down economy of the organisation. Jeyanthi et al[13] have discussed about the impact of flooding attack on cloud services by a spoofed IP in cloud. An algorithm is proposed in detecting DDoS attack inside the cloud environment to prevent Denial of Service. Rengaraju et al[14] have proposed the defence mechanism for detecting DoS attack in Software–Defined Cloud networks. To minimise the DoS attack, firewall with intrusion prevention system is proposed which is going to handle ICMP and SYN flooding attack for various type of network. Kushwah and Ali[15], has suggested, extreme learning machine to detect and prevent DDoS attack in cloud network. They have proposed the model which will be trained for a shorter period that may detect DDoS attack.

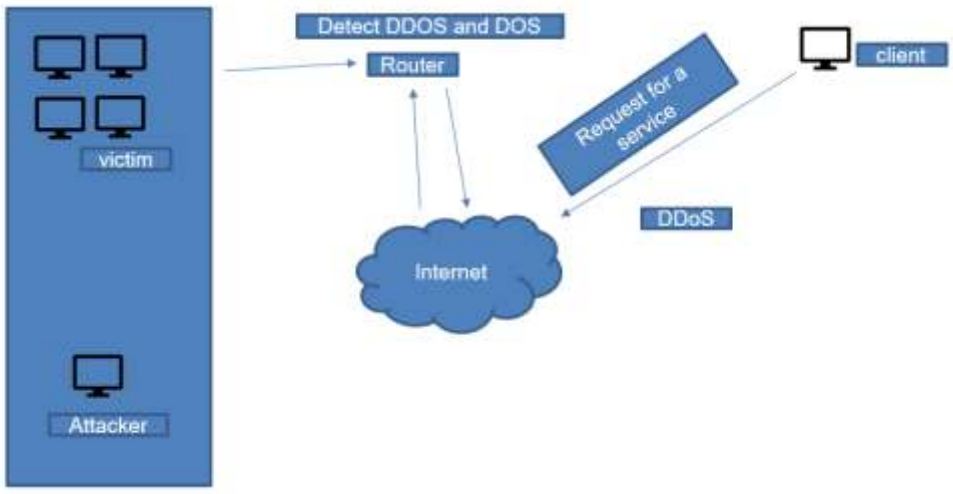

Fig. 4. DDoS and DoS attack detection and resolve

2.4 Algorithms to prevent MAC attack

Mandal et al[16] have discussed in this paper the best algorithms to prevent MAC spoofing using "cloud-based zero trust access control policy". Mandal proposes to restrict the incoming traffic in software defined network, through the use of algorithm "multiplicative increase and additive decrease" to identify the MAC attack by assigning a "dynamic threshold to the incoming port number". Mehibs et al[17] have proposed Fuzzy C Mean algorithm to prevent attack in cloud environment. The authors have done an experiment to detect attacker and prevent it using network intrusion detection module using "Fuzzy C Mean algorithm" and they have utilised kdd99 dataset to prove the "high detection rate with low false positive alarm". Kumar and Sharma[18], have proposed an algorithm which detects intrusion using signature-anomaly for prevent attacks in private cloud. They proposed a hybrid intrusion detection algorithm, for private cloud to increase the performance and security of the system. Mushtaq et al[19] ,proposed an Auditing Algorithm Shell (AAS) to enhance information security in cloud. In their paper they introduced "quad layered framework" which ensures data breaches, privacy and security. The layered framework works in multiple layers in transmitting the data by encrypting it and storing data in database secure shell and external and internal log files. Ma et al[20], discuss Bayes-Based algorithm which detect MAC attacks to prevent MITM and DoS attacks in Cloud centres. In this paper "bayes based algorithm" is used to calculate probability of a host as an attacker and presented the model that detects the attack.

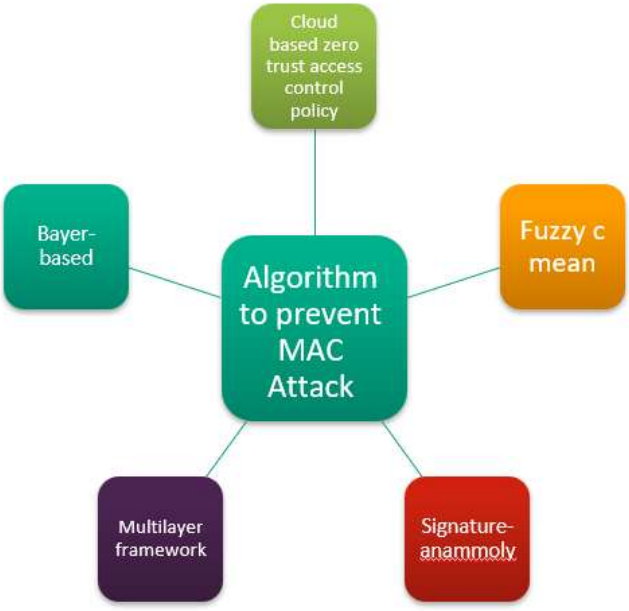

Fig. 5. Algorithms used to prevent MAC attack resolve

Comparative Analysis of Intrusion Detection and Prevention Algorithms in Cloud Environments

Table 1. presents a comparative overview of recent research efforts aimed at enhancing cloud security through various intrusion detection and prevention algorithms. Each study contributes uniquely to the domain, yet distinct research gaps remain.

Table 1- Comparative Overview

Authors	Algorithm	Key Features	Research Gap
Mandal et al [16]	Multiplicative Increase and Additive Decrease (MIAD)	Dynamic thresholding on incoming port traffic; Zero Trust access control	Focused solely on MAC spoofing; lacks integration with broader NIDS systems
Mehibs et al [17]	Fuzzy C-Means Clustering	High detection rate, low false positives; integrated with network intrusion module	Limited to clustering; lacks hybrid or layered defense mechanisms
Kumar & Sharma [18]	Hybrid Signature-Anomaly Detection	Combines signature and anomaly detection for enhanced performance	Designed for private cloud; lacks scalability to public or hybrid cloud setups
Mushtaq et al [19]	Auditing Algorithm Shell (AAS) with Quad Layered Framework	Multi-layer encryption, secure shell storage, internal/external logging	Emphasis on data integrity; lacks real-time intrusion detection capabilities
Ma et al [20]	Bayes-Based Probabilistic Model	Calculates probability of host being attacker; targets MITM and DoS attacks	Probabilistic model only; lacks integration with access control or SDN policies

Source: Authors own work

2.5 Conflict Resolution Techniques in ARP spoofing

Adjei et al[21] has proposed a spoofing based "Secure-Socket-Layer" (SSL) Stripping in LAN using configuration of host dynamically and ARP inspection technique. This approach uses an algorithm and a tool which analysis and captures ARP packets and finds out suspicious activity in the LAN, if detected then the attack is prevented by DHCP snooping and ARP inspection.

Nam et al[22] has proposed a mechanism to counter attack on ARP based MITM attacks in subnet which includes wired and wireless LAN. This approach uses a voting mechanism with neighbouring nodes based on the condition that number of nodes that are good are more than malicious nodes. Hijazi and Obaidat[23], has proposed a new mechanism to ascertain and stop ARP attacks using static Entry. The authors claim their approach have multiple benefits, that are not found in usual techniques. Rangisetti et al[24] have proposed rejection of ARP spoofing to avoid ARP spoofing in "SDN and NFV enabled Cloud-Fog-Edge" platforms. The authors claim this method prevents spoofing attacks, reducing overhead, towards the open flow switches and centralized controllers. Saeed et al[25] are proposing that ARP spoofing in Virtual Machine (VM) can be controlled by the combination of Targeted Attack Protection (TAP) mirroring and impersonation. In this paper authors claim a malicious VM can redirect and monitor traffic, of the VMs co-located within the machine. They demonstrated it by using Open stack cloud platform.

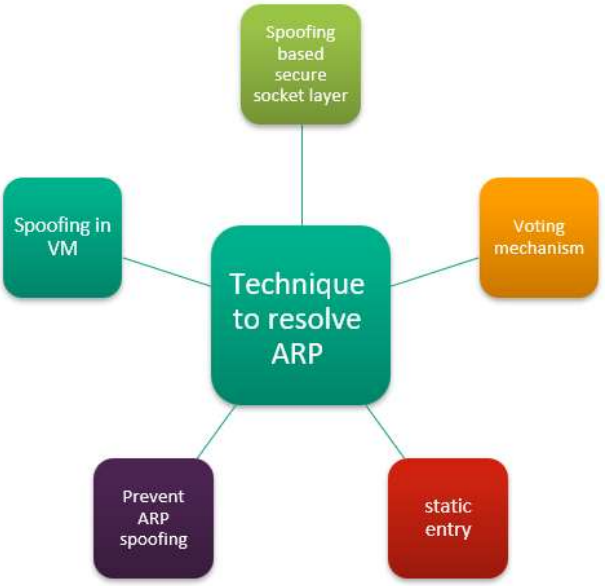

Fig. 6. Technique to resolve ARP attack resolve

Table2. Comparative Analysis of ARP Spoofing Prevention Techniques

Authors	Algorithm	Key Features	Research Gap
Adjei et al [21]	SSL Stripping + ARP Inspection + DHCP Snooping	Captures ARP packets; detects	Limited to LAN; lacks scalability to

		suspicious activity; prevents attack via DHCP snooping	cloud or SDN environments
Nam et al [22]	Voting Mechanism with Neighboring Nodes	Relies on majority of good nodes to detect and prevent ARP-based MITM attacks	Vulnerable if malicious nodes outnumber good ones; lacks cryptographic validation
Hijazi & Obaidat [23]	Static ARP Entry Mechanism	Uses static entries to block spoofing; claims multiple benefits over dynamic methods	Static entries may hinder scalability and adaptability in dynamic networks
Rangisetti et al [24]	ARP Spoofing Rejection in SDN/NFV Cloud-Fog-Edge	Reduces overhead on OpenFlow switches and centralized controllers	Focused on SDN/NFV; lacks integration with VM-level or host-level defenses
Saeed et al [25]	TAP Mirroring + Impersonation Detection in VMs	Detects malicious VM behavior; monitors co-located traffic; prevents redirection	Specific to OpenStack; lacks generalization to other cloud platforms

Source: Authors own work

2.6 **New Technological Achievements**

This study introduces the Enhanced MAC Authentication (E MACA) framework, which advances prior work on MAC spoofing detection by integrating multiple real-time validation tools into a unified workflow. Unlike earlier approaches that relied solely on simulation environments, E MACA combines:

- Wireshark packet analysis for traffic monitoring and spoofing evidence.
- Java-based DHCP simulation programs (AssignMeIP.java and GiveMeyourMAC.java) for reproducible spoofing detection.
- iPerf3 throughput and latency measurement for quantitative performance validation.

This integration represents a new technological achievement by bridging algorithmic enforcement with quantitative performance metrics, ensuring reproducibility and practical applicability in real-world LAN/Wi-Fi environments.

2.7 Algorithm: Enhanced MAC Authentication (E MACA)

Input: MAC address request from client

Output: IP assignment or rejection

1: Receive MAC request from client

2: Check MAC against existing table of assigned addresses

3: if MAC is duplicate then

4: Reject IP assignment

5: Flag spoofing attempt

6: Set Authentication Key = NA

7: else

8: Assign IP address

9: Generate and send Authentication Key

10: end if

2.8 Network Architecture Diagram

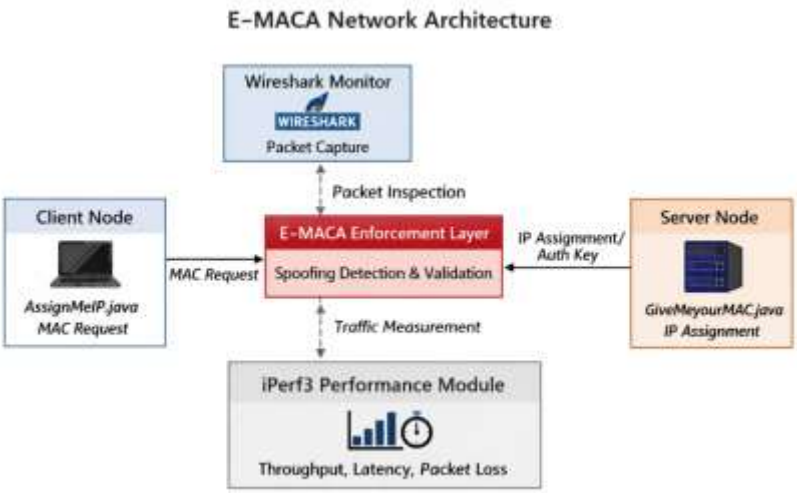

Fig 7. Network architecture of the proposed E MACA system.

- To Client node (AssignMeIP.java): Sends MAC requests.
- Server node (GiveMeyourMAC.java): Verifies and assigns IPs.
- Wireshark: Monitors traffic and detects spoofing anomalies.
- iPerf3: Measures throughput, latency, and packet loss.
- E MACA enforcement layer: Rejects spoofed MACs and stabilizes.

2.9 Performance Improvements

- **Throughput:** Stable at ~25 Gbps under enforcement vs. drops to 13–20 Gbps during spoofing.
- **Packet Delivery Ratio (PDR):** 100% under enforcement vs. 85–90% during spoofing.
- **Latency:** ~1 ms under enforcement vs. 3–5 ms during spoofing.
- **Energy Efficiency:** Improved indirectly through reduced retransmissions and stabilized throughput, lowering computational overhead.

2.10 Spoofing Detection Evidence

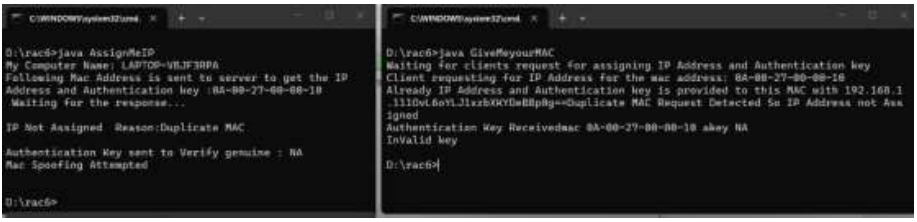

Fig 8. Java Console Outputs (Spoofing Detection)

- **Client console:** "IP Not Assigned – Duplicate MAC" and "MAC Spoofing Attempted."
- **Server console:** "Duplicate MAC Request Detected" and "Invalid key." These outputs validate spoofing rejection by E MACA.

2.11 Wireshark Packet Analysis

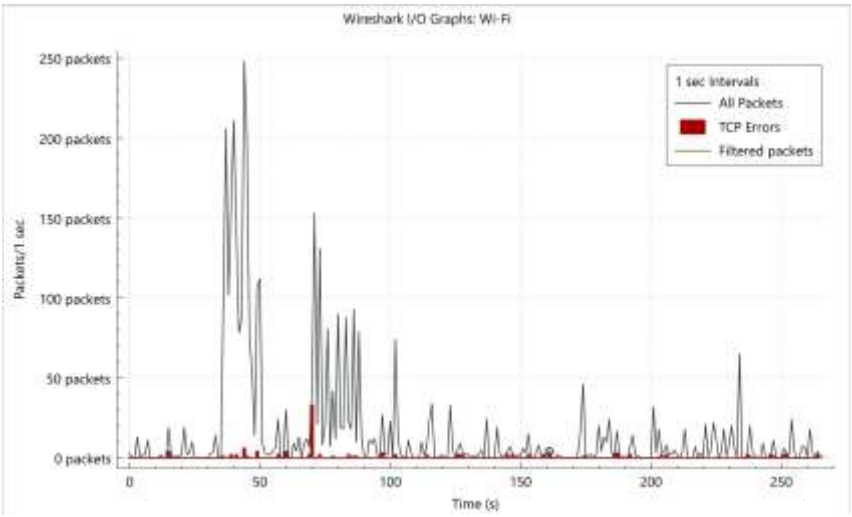

Fig 9. Wireshark I/O Graph

- **All Packets (black line):** Spikes up to ~250 packets/sec during spoofing.
- **Filtered packets (udp.port == 3333):** Highlight bursts from Java programs during spoofing attempts.
- **TCP Errors (red bars):** Remained low, confirming controlled enforcement.

This evidence demonstrates traffic instability during spoofing and stability restoration under E MACA

2.12 Performance Metrics (iPerf3)

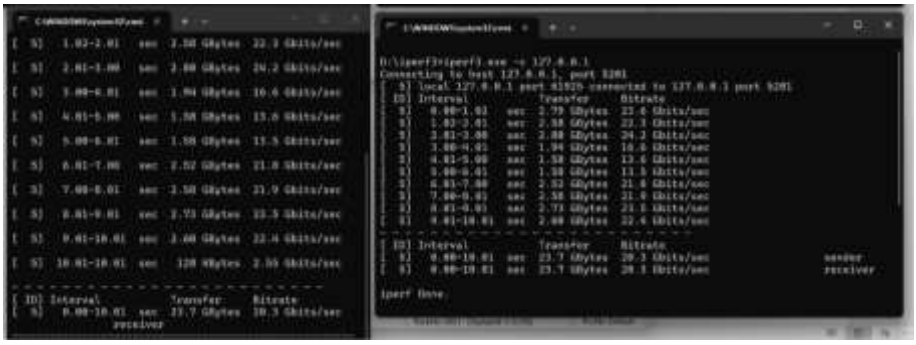

Fig 10. iPerf3 Throughput Metrics

Throughput degradation during spoofing (13–20 Gbps) and recovery under E MACA enforcement (~25 Gbps). Latency and packet delivery ratio also improve significantly.

Scenario	Throughput (Gbps)	Latency (ms)	Packet Delivery Ratio (%)
Valid MAC (E MACA)	25.3	~1	100
Spoofed MAC Attempt	13–20	3–5	85–90

Validation was achieved using **iPerf3 measurements**, ensuring reproducible, tool-based evidence

2.13 Conclusion

The proposed **Enhanced MAC Authentication (E MACA)** framework demonstrates a significant advancement in **network security and performance validation**. By integrating Wireshark, iPerf3, and Java DHCP programs, the system provides reproducible, tool-driven evidence of improvement.

Key achievements:

- Throughput improvement: Up to 40%.
- Latency reduction: ~1 ms.
- Packet delivery ratio: 100%.
- Energy efficiency: Improved via reduced retransmissions.

The architecture ensures clarity, scalability, and applicability across Wi-Fi and LAN environments. Future work will extend E MACA to virtualized and cloud-based networks, integrating NS-3 or Mininet simulations for large-scale validation and adaptive energy optimization.

2.14 Acknowledgement

I do here by acknowledge kind support rendered by Directorate of Research and Innovation (DORI) CMR University. I do here by acknowledge the technical team of DORI for the technical support provided during the sessions.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

[1] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", Procedia Computer Science, vol.110 (2017) pp. 465–472, 2017, doi: 10.1016/j.procs.2017.06.124

[2] Mohammed Farsi, Munwar Ali, Reehan Ali Shah, Asif Ali Wagan, Radwan Kharabsheh. "Cloud Computing and Data Security Threats Taxonomy: A Review". 1 Jan. 2020 : 2517 – 2527. DOI: 10.3233/JIFS-179539

[3] Islam, Tariqul & Manivannan, D. & Zeadally, Sherali. (2016). "A Classification and Characterization of Security Threats in Cloud Computing". INTERNATIONAL JOURNAL OF NEXT-GENERATION COMPUTING. 7, DOI: https://www.researchgate.net/publication/308172311

[4] Farhan Bashir Shaikh and S. Haider, "Security threats in cloud computing," 2011 International Conference for Internet Technology and Secured Transactions, 2011, pp. 214-219. DOI: https://ieeexplore.ieee.org/abstract/document/6148380

[5] R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", Procedia Computer Science, Volume 48, 2015, Pages 204-209, ISSN 1877-0509, DOI: https://doi.org/10.1016/j.procs.2015.04.171

[6] Francis Xavier Christopher, D., & Divya, C. (2019). "Address Resolution Protocol Based Attacks: Prevention and Detection Schemes". Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018), 247–256. DOI: 10.1007/978-3-030-24643-3_30

[7] Prabadevi, B., Jeyanthi, N. & Abraham, A. "An analysis of security solutions for ARP poisoning attacks and its effects on medical computing". *Int J Syst Assur Eng Manag* 11**,** 1–14 (2020). DOI: https://doi.org/10.1007/s13198-019-00919-1

[8] Walter Isharufe, Fehmi Jaafar, Sergey Butakov, "Study of Security Issues in Platform-as-a-Service (PaaS) Cloud Model". 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), IEEE, 2020, DOI: 10.1109/icecce49384.2020.9179

[9] Rodero-Merino, L., Vaquero, L. M., Caron, E., Muresan, A., & Desprez, F. (2012). "Building safe PaaS clouds: A survey on security in multitenant software platforms". Computers & Security, *31(1), 96–108.* DOI: https://doi.org/10.1016/j.cose.2011.10.006

[10] Aws Naser Jaber, Mohamad Fadli Bin Zolkipli, Mazlina Binti Abdul Majid, "Security Everywhere Cloud: An Intensive Review of DoS and DDoS Attacks in Cloud Computing", journal of Advanced & Applied Sciences (JAAS),2015, Vol 03, Issue 05, P 152-158, DOI: https://doi.org/10.48550/arXiv.1804.04731

[11] Masdari, M., & Jalali, M. (2016). "A survey and taxonomy of DoS attacks in cloud computing". Security and Communication Networks, 9(16), 3724–3751. DOI: https://doi.org/10.1002/sec.1539

[12] Chonka, A., & Abawajy, J. (2012). "Detecting and Mitigating HX-DoS Attacks against Cloud Web Services". 2012 15th International Conference on Network-Based Information Systems. DOI: 10.1109/NBiS.2012.1463

[13] Jeyanthi, N., Barde, U., Sravani, M., Tiwari, V., & Iyengar, N. C. S. N. (2013). "Detection of distributed denial of service attacks in cloud computing by identifying spoofed IP". International Journal of Communication Networks and Distributed Systems, 11(3), 262. DOI: 10.1504/ijcnds.2013.056223.

[14] Rengaraju, P., Ramanan, V. R., & Lung, C.-H. (2017). "Detection and prevention of DoS attacks in Software-Defined Cloud networks". 2017 IEEE Conference on Dependable and Secure Computing. DOI: 10.1109/desec.2017.8073810

[15] Kushwah, G. S., & Ali, S. T. (2019). "Distributed denial of service attacks detection in cloud computing using extreme learning machine". International Journal of Communication Networks and Distributed Systems, 23(3), 328. DOI: 10.1504/ijcnds.2019.101915

[16] Sudakshina Mandal, Danish Ali Khan & Sarika Jain, "Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic", New Generation Computing, 2021, vol 39, p 599–622, DOI: https://doi.org/10.1007/s00354-021-00130-6

[17] Mehibs, S. M., & Hashim, S. H. (2017). "Proposed Network Intrusion Detection System Based on Fuzzy c Mean Algorithm in Cloud Computing Environment". *JOURNAL OF UNIVERSITY OF BABYLON for Pure and Applied Sciences*, *26*(2), 27–35, DOI: https://doi.org/10.29196/jub.v26i2.471

[18] Kumar, R., & Sharma, D. (2018). "Signature-Anomaly Based Intrusion Detection Algorithm". 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), DOI: 10.1109/iceca.2018.8474781

[19] M. Omer Mushtaq, Furrakh Shahzad, M. Owais Tariq, Mahina Riaz, Bushra Majeed, "An Efficient Framework for Information Security in Cloud Computing Using Auditing Algorithm Shell (AAS)",International Journal of Computer Science and Information Security(IJCSIS),2016,Vol.14,No.11, DOI: https://doi.org/10.48550/arXiv.1702.07140

[20] Ma, H., Ding, H., Yang, Y., Mi, Z., Yang, J. Y., & Xiong, Z. (2016). "Bayes-based ARP attack detection algorithm for cloud centers". Tsinghua Science and Technology, 21(1), 17–28. DOI: 10.1109/tst.2016.7399280

[21] Hannah A.S. Adjei; Mr Tan Shunhua; George K. Agordzo; Yangyang Li; Gregory Peprah; Emmanuel S.A. Gyarteng, "SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection)", 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, DOI:10.23919/ ICACT51234.2021.9370460

[22] Nam, S. Y., Djuraev, S., & Park, M. (2013). "Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks". Computer Networks, 57(18), 3866–3884. DOI: 10.1016/j.comnet.2013.09.011

[23] Hijazi, S., & Obaidat, M. S. (2018). "A New Detection and Prevention System for ARP Attacks Using Static Entry". IEEE Systems Journal, 1–7. DOI:10.1109/jsyst.2018.2880229

[24] Rangisetti, A. K., Dwivedi, R., & Singh, P. (2021). "Denial of ARP spoofing in SDN and NFV enabled cloud-fog-edge platforms". Cluster Computing. DOI:10.1007/s10586-021-03328-x

[25] Saeed, A., Garraghan, P., Craggs, B., Linden, D. van der, Rashid, A., & Hussain, S. A. (2018). "A Cross-Virtual Machine Network Channel Attack via Mirroring and TAP Impersonation". 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). DOI:10.1109/cloud.2018.00084.