New Generation Computing (2021) 39:599–622
https://doi.org/10.1007/s00354-021-00130-6

Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic

Sudakshina Mandal[1] · Danish Ali Khan[1] · Sarika Jain[2]

Received: 4 December 2020 / Accepted: 15 June 2021 / Published online: 29 June 2021

Abstract

The ubiquitous cloud computing services provide a new paradigm to the work-from-home environment adopted by the enterprise in the unprecedented crisis of the COVID-19 outbreak. However, the change in work culture would also increase the chances of the cybersecurity attack, MAC spoofing attack, and DDoS/DoS attack due to the divergent incoming traffic from the untrusted network for accessing the enterprise's resources. Networks are usually unable to detect spoofing if the intruder already forges the host's MAC address. However, the techniques used in the existing researches mistakenly classify the malicious host as the legitimate one. This paper proposes a novel access control policy based on a zero-trust network by explicitly restricting the incoming network traffic to substantiate MAC spoofing attacks in the software-defined network (SDN) paradigm of cloud computing. The multiplicative increase and additive decrease algorithm helps to detect the advanced MAC spoofing attack before penetrating the SDN-based cloud resources. Based on the proposed approach, a dynamic threshold is assigned to the incoming port number. The self-learning feature of the threshold stamping helps to rectify a legitimate user's traffic before classifying it to the attacker. Finally, the mathematical and experimental results exhibit high accuracy and detection rate than the existing methodologies. The novelty of this approach strengthens the security of the SDN paradigm of cloud resources by redefining conventional access control policy.

Keywords COVID-19 · Coronavirus pandemic · Cloud security · MAC spoofing · Zero trust access control policy

✉ Danish Ali Khan
dakhan.ca@nitjsr.ac.in

Extended author information available on the last page of the article

Introduction

Over the last decades, dependencies on cloud resources have been increased significantly in organizations [1]. The businesses have been transformed enormously with leading cloud vendors like Amazon, Microsoft, and Google [2]. In the Coronavirus pandemic, the usages of cloud resources have escalated when the enterprises have shifted to the work-from-home environment to adjust the computing needs worldwide. Cloud resources ensure seamless work-from-home facility and maintain connectivity with the critical resources beyond the corporate boundary [3]. However, the fast-paced adoption of cloud resources increases network traffic and security issues related to hacking and spoofing. When these cloud resources are accessed from heterogeneous platforms using untrusted home networks, it leads to severe security breaches. These problems cannot be averted with the existing methods in the present dynamic situation, whereas the individual network traffic comes from the untrusted zone beyond the corporate structure [1]. Using this privilege, attackers and hacktivists compromise the critical cloud infrastructures by launching several attacks by spoofing the host. Therefore, the trivial network infrastructures should be modified with emerging needs to protect from spoofing attacks. In this regard, the organizations aim to confirm the safety and reliability of cloud resources as well as the hosts residing and working remotely using untrusted network [4].

In a wireless environment, remote workstations are connected to the enterprise's cloud resources through a personal Wi-Fi hotspot or mobile network. Local network service providers do not possess any special security measures to prevent network spoofing attacks like address routing protocol (ARP) spoofing attacks [2], Internet protocol (IP) spoofing attacks [3], and media access control (MAC) spoofing attacks [3]. Intruders probe through the Internet service providers (ISP) to gain access to the legitimate user. ARP spoofing and IP spoofing attacks are considered to be the significant distributed denial of service (DDoS) attacks in cloud environment when workforces connect from the home network [4]. When an intruder sniffs the network for a valid MAC address and pretends to be the legitimate user of any significant MAC address, it is termed as MAC spoofing attack [5]. Maximum Internet service providers (ISP) bind their network services with the MAC address by embedding it in the network interface card (NIC). ISPs do not grant access to the internet if the MAC address has been altered anyhow. However, the legitimate MAC address can easily be spoofed and can be the bedrock of several attacks mentioned earlier. A large number of literature exist to detect MAC spoofing attacks in wireless networks. Analyzing the sequence number of transmission control protocol (TCP) packets, using hop count filter, by checking the received signal strength indicator (RSSI) signal can detect any network spoofing attacks in wireless network [6]. However, these techniques could not take charge if the spoofing has already happened to the host and authenticated the malicious host as a legitimate one. It is very tricky to detect the attack which is already done in the enterprise's network. When the number of hosts increases to use cloud resources from several remote zones, the chances of spoofing would be accelerated with the significant number of traffic packets. Spoofing associated with the vast amount of heterogeneous traffic coming from untrusted areas to the enterprise's network can be prevented, which increases security [1].

The conventional security concepts to protect cloud resources have been changed radically with the growing number of cybersecurity threats. Interactions with corporate cloud resources and services are often bypassed through the on-premises perimeter-based security models that rely on conventional network firewalls and virtual private networks (VPN) [7]. The new paradigm has eliminated these traditional security barriers where perceptible perimeters are enclaved the corporate on-premises resources. Now, resources have been scattered in distributed essence in the current cloud environment, which does not rely on physical network configuration. Changing the firewall rule in every step would not be feasible for the enterprise strategies for granting access in the remote working environment. To ensure the protection in application endpoints across heterogeneous circumstances, enterprises prefer to shift to the next-generation zero-trust approaches [8].

The zero trust concept has been intended to create a new access control policy that embraces the modern environment and protects individual devices and users beyond their perimeter, which is free from network support micro-segmentation. The fundamental concept of zero trust is "never trust, always verify" [9]. It verifies individual incoming network requests coming from untrusted zones. It redefines the concept of access control security policies over the conventional security boundaries independent of VPN structure [7]. In the present cloud environment, the security policy proposed using the zero trust framework would grant access to significant network traffic for the use of distributed cloud resources [10].

The concept of trusting the network gears up by incorporating the software-defined network (SDN) paradigm in the network model [11]. Most enterprises now have moved to the SDN framework, where the data plane and control plane are separated with fine granular segmentation, which makes the concept more lenient. SDN based zero trust access control policy reduces the burden of network-based firewall policy [8]. Defining the set of access control policies at the enterprise level thwart the SDN cloud parameters [12]. The access control policies give a provision for rule-based validation where unauthorized TCP/IP traffic must be rejected to access the SDN framework of cloud resources. These policies also help to block the known and unknown attacks.

In this present situation, architectural access control policies must be redesigned to support work-from-home-concept for accessing cloud resources seamlessly without human intervention. When the cloud resources are used by limited, and having no knowledge group of people, rule-based access control policies can protect the enterprise's cloud resources from being exposed. This paper proposes a progressive access control policy based on zero trust. The significant contributions of the paper are as follows:

- Proposing of zero trust based access control policy to prevent MAC spoofing by ensuring security to the hosts and cloud services. This approach eliminates the threats before spoofing occurred.

- This approach operates on the open system interface (OSI) layer 3 and layer 4 where an individual TCP packet is captured from the incoming untrusted IP address and retrieves the IP address, port number, and corresponding MAC address of the respective traffic.
- The proposed multiplicative increase and additive decrease algorithm uses the IP trackback and port scanning techniques validation of the TCP packet, which reduces the computational overhead.
- The use of dynamic threshold stamping by our proposed approach rectifies a legitimate user's traffic before classifying it to the attacker, which reduces the rate of false-positive rate significantly.

The rest of the paper is organized as follows. Next section discusses the "Background and Related Work". "Proposed Approach" the architecture of the proposed framework with proof of concept. Experimental analysis and results are reported in "Results and Analysis". Finally, the last section concludes the paper.

Background and Related Work

Significant research proposals for making a defensive approach in the wireless network have been discussed in the following subsections. The subsections contain the major contributions from the rigorous research proposals.

DDoS and MAC Spoofing Strategies Based on Cloud Resources

The researchers in [13] used hop count filtering and sequence number encoding methodologies to protect the cloud resources against denial of service attack (DoS) as well as distributed denial of service attack (DDoS). This approach effectively filters out malicious data packets by analyzing transmission control protocol (TCP) traffic, which uses SYN cookie to prevent the attack. Message authentication code (MAC) generator is used here for authentication of the legitimate host. Another significant work is proposed in [14], where a theoretical framework of the threshold value (ThreV) detects MAC spoofing DDoS attacks in wireless local area infrastructure network (WLAN). This methodology proves the effectiveness to protect resources from DDoS attack occurred in WLAN. Cloud resources may be unreliable due to several wireless mesh network threats (WMN). A novel framework is proposed in [15] to mitigate these drawbacks of WMN from cloud resources. Similarly, an IoT-based method is proposed in [16] to ensure the privacy and security for the heterogeneous platform in the work-from-home cloud. This method can be paired up with any security measurement protocol to prevent cybersecurity attacks in the cloud, edge, and IoT layers.

Detection of Network Spoofing Using Zero Trust

The concept of the zero-trust mechanism has made a substantial leap for restructuring policies and ensuring security against cybersecurity attacks in the COVID-19 pandemic. In this regard, a significant security awareness framework has been proposed in [17] to secure 5G smart healthcare system, which hosts critical medical data by leveraging zero-trust architecture. Four-dimensional security policies have been proposed for the first time by considering the dimensions named subject, object, environment, and behavior. This methodology supports fine-grained access control, situational awareness, real-time network security, access behavior analysis, and identity authentication for building trust in the proposed system. With a similar note to the zero-trust approach, an access control policy is proposed by the researchers in [8]. A steganography overlay is embedded as an authentication token of the first packet in the respective TCP packet. This defensive mechanism is considered one of the significant approaches to prevent cybersecurity attacks in the cloud environment. In [18], a risk-based access control framework has been proposed based on a zero-trust network. This security framework supports the firewall provisioning smoothly. A well-defined policy language makes this approach more effective.

Threshold-Based Detection Methods

To preserve confidentiality and integrity against an intruder in an untrusted network, a static threshold-based technique has been proposed in [19]. Threshold has been chosen by collecting minimum features for detecting fast attacks from the perspective of the host. Observation and experimental analysis are considered to set the value of the threshold. Another threshold-based MAC spoofing detection in the wireless medium is discussed in [20]. The conventional sequence number of TCP packets is used here to detect MAC spoofing. An artificial neural network (ANN)-based detection method substitutes the limitations of the high rate of false alerts due to the loss of a data packet. This method helps to detect, and distinguish network behavior from noisy and incomplete data sources.

IP Spoofing Detection with Regards to Wireless Network

Significant research works have been proposed so far to detect spoofing in the wireless network. Some of the essential techniques adhere to the existing approaches; namely, the signature-based approach, received signal strength (RSS)-based approach, sequence number-based approaches, analyzing packet frame, hop count filtering, detecting ARP mismatch, checking the physical characteristics, and many more. Some of the following approaches have been discussed below.

An improved version of a rule-based intrusion detection system is proposed in [21], where network classification is done by analyzing malicious and benign traffic. The predictive performance gives significant accuracy without bothering network behavior. It is helpful for encrypted traffic. The method is also efficient for the malware that uses original hosts such as C& C or proxy toward C&C without checking its payload. Similarly, in [22], a system is proposed to learn the behavior of malicious network activities to help in the detection and prevention of several types of attack such as ARP Cache Poising, DDoS, Probing attack, Botnet, Malformed Packets, etc. The malware classification is done by extracting features and classifying abnormal traffic. Hatcher et al. [23] proposed a cloud/edge streaming analysis-based threat detection model where the model collects real-time big-data traffic in an enterprise network with a similar cybersecurity context. Discrimination between normal and abnormal traffic has been evaluated by clustering algorithms. This model has proven the high accuracy and fast performance in a cloud testbed with a significant volume of streaming data. Similarly, El-Alfy and Al-Obeidat [24] proposed a novel security mechanism by collecting historical data to build the attack model with influential parameters. The multi-criterion fuzzy classification-based predictive model helps to classify unknown network traffic. Eidle et al. [25] proposed a cyber-defense model based on dynamic orchestration of authenticated gateway trust level. This model has efficiently detected and blocked DDoS attacks for the cloud data center network. Researchers in [26] contributed to the research by proposing a neural network-based model on long short-term memory (LSTM) network, which checks the aspects of observable network traffic. On the same note, to overcome the shortfall of the signature-based malware detection model, in [27], a method is presented to detect security threats based on the statistical characteristics of HTTP requests. Similarly, researchers in [28] presented malware detection methods by analyzing TCP/IP packets over HTTPS traffic. Wang et al. [29] proposed a seed expanding (SE) method to detect the attack before penetrating the host.

An intrusion prevention approach has been followed for cybersecurity attacks by combining the first packet authentication approach with transport layer access control policy methods in higher education cloud computing environments [30]. The researchers in [31] proposed a method for network administration using clustering techniques. K-means, PAM, and CLARA are the significant techniques considered here for making the threat profile. Another significant approach for mitigation of IP spoofing like Dos/DDoS attack is proposed in [32]. Using the methodology of IP traceback, Patel et al. [32] proposed a lightweight packet marking (LPM) scheme. This approach reduces the number of false-positive rates and packets needed in the spoofed host and the upstream network traffic map requirement compared to the traditional probabilistic packet marking approach (PPM). Multiple hash function is used here to reduce the false-positive rate to 0. It supports incremental deployment in the presence of a legacy router.

A technique is proposed based on RSS (received signal strength) and medoid-based clustering, which is used to detect multiple spoofing attacks in a wireless network environment in [33]. The dynamic MAC address allocation concept is proposed here to prevent multiple spoofing attacks on the host. In a similar context, the authors of [3, 6, 34–36] proposed significant spoofing detection methodologies applicable for IEEE 802.11 network .

Significance of Cloud in the COVID-19 Outbreak

In light of the coronavirus pandemic, telecommuting becomes a necessity for enterprises worldwide. Shifting to work-from-home has instituted by employees across the globe [1]. The cloud computing environment (CCE) is the primary choice for the employees for accomplishing the task in work-from-home culture. CCE is comprised of a pool of numerous resources that can be seamlessly configured and offers uniqueness and easy access to the resources hosted in CCE. In this crisis, the adoption of CCE provides a high demand for services with reduced cost and setup complexities. The attractive and functional features of CCE accommodate a lot of benefits to the users without investing in the network, hardware infrastructure, and cost. It provides a quick deployment environment, personalized features with high flexibility and scalability, and supports rapid data growth with high availability. However, the rapid growth of CCE usage increases the security and privacy risk. The cloud infrastructures hosted in the corporate perimeter are controlled by specific access control policies previously. However, in the present situation, CCE has transformed from its traditional periphery, and the resources are accessed by several employees having limited or no knowledge about security parameters. There is a big security concern when data transmission happens between untrusted devices globally with CCE. This massive amount of untrusted traffic creates room for several cybersecurity attacks, MAC spoofing attacks, as discussed in "DDoS and MAC Spoofing Strategies Based on Cloud Resources", "Detection of Network Spoofing Using Zero Trust", and "IP Spoofing Detection with Regards to Wireless Network". For a long time, a virtual private network (VPN) has been considered for secure transmission with network perimeter security. VPN has been used as the ready-to-go solution for an extended period which worked through SSL tunnels or IPsec. According to Gartner, the concept of VPN has been phased out 60% of the companies [37] and the compatibility with the current infrastructure has been mismatched due to several reasons listed in [7].

As many VPNs are found fake and malicious, the enterprise should limit the use of VPN in the present scenario. To ensure data protection in work-from-home in this crisis, CCE follows cloud access security brokers (CASB) policies for ultimate data security. CASB is a unified platform that supports minimizing data breaches by ensuring data protection in a completely controlled environment [7]. It also increases cloud visibility. Organizations can get a clear insight into the attack surface and the affected applications with the help of CASB policies.

In the present context, a well-defined solution is proposed by our approach for considering the extreme need for restructuring the existing access control policies. When the enterprises have already started to decrease the budget for the upcoming fiscal year 2021, this approach proves the trustworthiness by proposing this intelligent approach, which needs significantly less computational overhead. Henceforth, the novelty of this approach can be used to secure hosts and cloud resources that can detect any spoofing at a very initial stage without falsifying the legitimate host.

Proposed Approach

The proposed approach is based on the wireless network (IEEE 802.11), independent of physical characteristics and location. The use of the threshold stamping technique gives the chance to rectify a legitimate user's traffic before classifying it to the attacker by reducing the false-positive rate (FPR). The self-learning process of the algorithm allows to learn the characteristics of the deployed network on its own. This process helps to anticipate the network and predict the host's characteristics for easy classification of the spoofed traffic. The existence of spoofing could exponentially raise the threshold. However, if the consecutive increment of the threshold is anticipated, it would be marked as a wrong entry or spoofed IP address and would discard that packet. This approach has been decreased the threshold linearly by predicting the balanced network [38]. This process could prevent any unwanted cybersecurity threats from exploiting the cloud resources. It is considered as an effective process to detect any attack in the presence of a stable network.

The proposed access control policy is based on the transport access control (TAC) layer to extract and analyze the TCP packets of incoming traffic. However, to build a TCP connection with the cloud server/resources, hypertext transfer protocol (HTTP) is used as the application layer protocol [39]. Individual untrusted IP addresses are verified explicitly by the zero-trust network at the time of establishing a session with the cloud resources. The existing identity access management (IDM), such as Amazon Web Services (AWS) or Microsoft Web Directory cloud services, takes the control of the authentication of IP addresses. An explicit trust is established with the IP addresses coming from each host, and IDM allows to create the TCP sessions for accessing the cloud resources further [32]. Validated hosts send the ARP requests with their corresponding IP addresses. The network parameters correspond to the IP addresses have been stored in the ARP table after receiving the ARP responses. Retrieval of MAC address is also carried out by the ARP protocol. Explicit TCP header has been inspected for the port number and destination IP address, instead of the entire TCP packet, which reduces the overhead of checking individual TCP packet content. Henceforth, it preserves high bandwidth with low latency of the network. Authenticated IP addresses should be passed through a virtual security gateway where our access control policy is implemented. Figure 1 illustrates the architecture of the proposed approach. The access control policy takes the responsibility further for granting the access to specified IP traffic. Spoofed IP addresses would automatically be discarded by the policy, and an alert message would be generated.

Structure of the Proposed Access Control Policy

The Proposed access control policy allows inspecting the network traffic by analyzing the port number by assigning certain threshold values [2]. The threshold is dependent on significant global factors, which will be discussed in the next section. Figure 2 describes the flow of the proposed access control policy.

Based on algorithm 1, if the incoming port number is less than the threshold value, the algorithm should perform the following procedures:

- If two different IP addresses come with different port numbers, it increases the threshold by the factor of two, and updates the ARP table of the new incoming IP address.

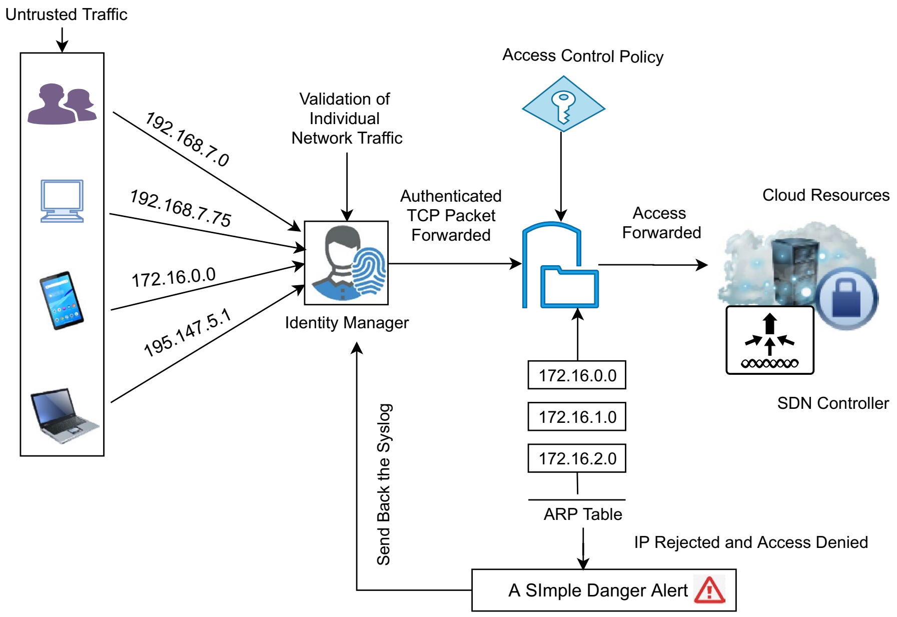


Fig. 1 Block diagram of the proposed architecture

- If the exact mismatch of the IP is found, then the port number is inspected, and the threshold value would be decreased linearly to balance the network traffic [23]. Henceforth, it updates the port number in the ARP table.
- If the new incoming IP address matches with the current IP address, it authenticates for the similarity of the port number, and henceforth, the port number remains unchanged .

If it is found that the incoming TCP port value is much greater than the threshold value, the threshold would be increased by a factor of two to accommodate the new port number by the self-learning process. In this situation, the host gets a chance to correct the incoming traffic without punishment. If the entire process continues and the consistent increment of the threshold is observed, then the host is identified as spoofed. The approach would reject the TCP packet coming from that host automatically.

This algorithm decreases the false-positive rate significantly by giving a chance to decrease the threshold when it goes beyond the maximum limit. Individual scanning of the threshold based on their port number authenticates the particular IP traffic. The traffic would be considered spoofed by this approach without traceback to their respective MAC address. The flowchart of algorithm 1 is illustrated in Fig. 3.

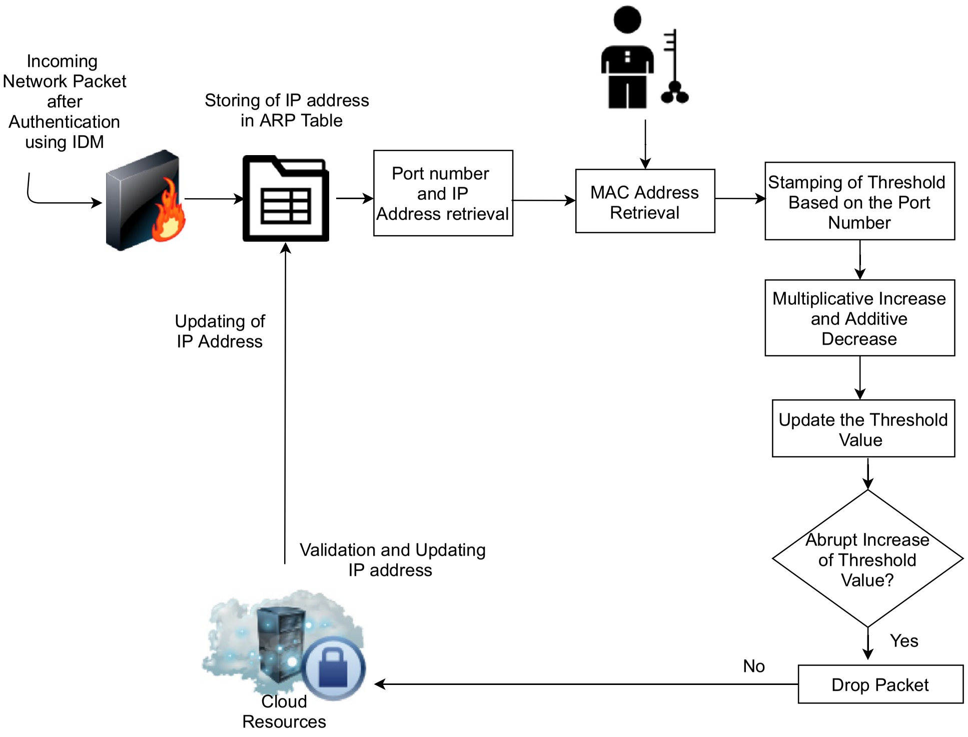


Fig. 2 Flow diagram of the proposed zero-trust-based access control policy

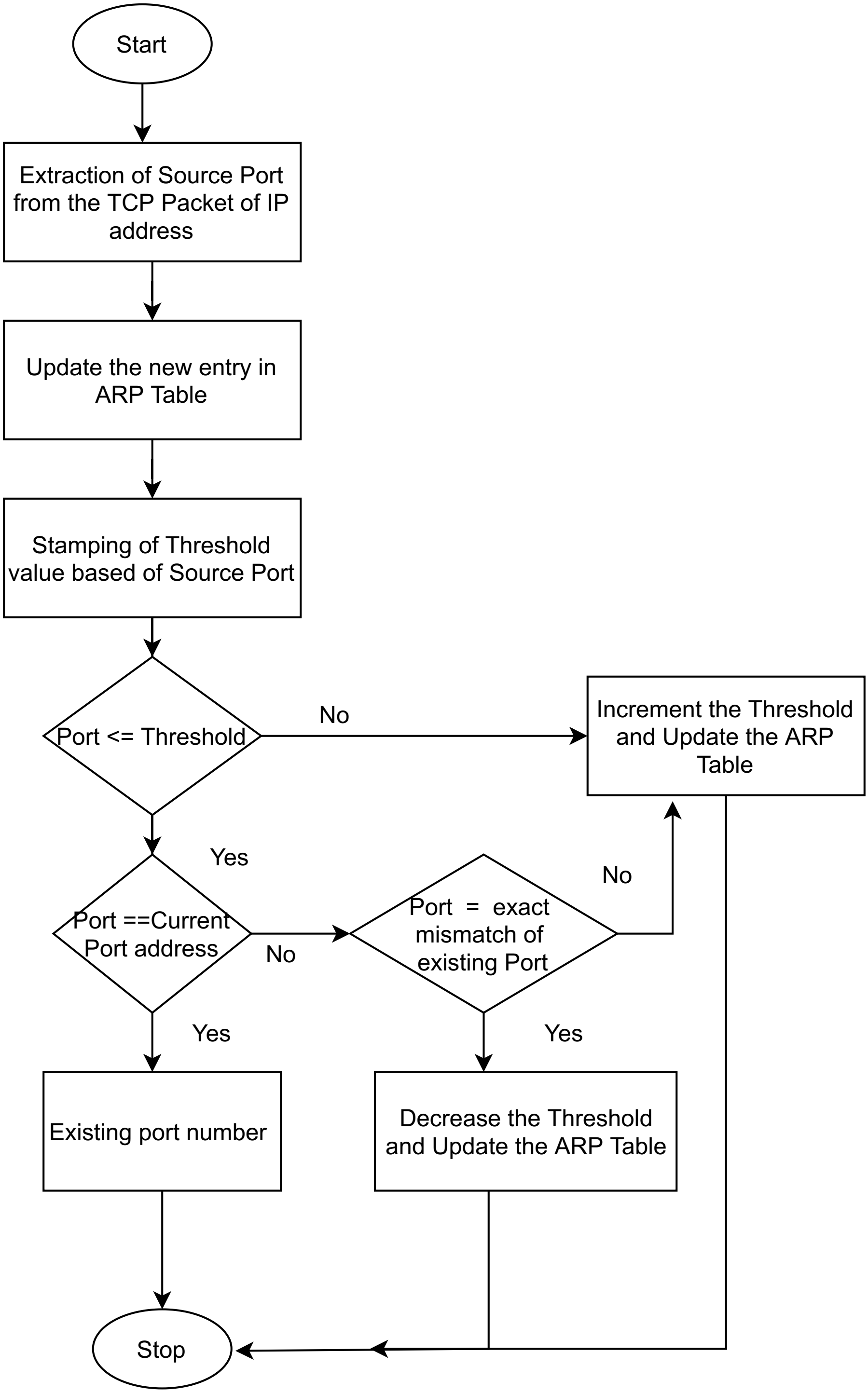

Start
Extraction of Source Port from the TCP Packet of IP address
Update the new entry in ARP Table
Stamping of Threshold value based of Source Port
Port <= Threshold
No
Increment the Threshold and Update the ARP Table
Yes
Port ==Current Port address
No
Port = exact mismatch of existing Port
No
Yes
Yes
Existing port number
Decrease the Threshold and Update the ARP Table
Stop

Fig. 3 Flowchart of algorithm 1

Algorithm 1 Multiplicative Increase and Additive Decrease

```
Input: TCP Port Address
Output:Updated Port Number, Updated Threshold value
For TCP Port number
Begin
Scan Port number and assign threshold
Monitoring Phase:
if $Port\ number \leq Threshold\ value$ then
    Then
    if $Port\ number == Current\ Port\ number$ then
        Then Print Port is already exist
    else
        if $Port\ number == exact\ mismatch\ of\ existing\ Port\ number$ then
            Then
            Decrease the threshold linearly
            Set Current Port Number = = Updated Port number
else
    Increase the threshold by factor 2
    Current Port Number = = Updated Port number
if $Port\ number \geq Threshold\ value$ then
    Then
    Increase the threshold by a factor of 2 according to the Port Number
    Set Old threshold value = Updated threshold value
End
```

Proof of Concept

Consider a network space N with available users (R_a) with TCP traffic packets (T_p), which have specific network requirements (A^*) stored in ARP table (T_b). Network attributes can be represented as $A_i^* = A_1^*, A_2^*, A_3^*, \dots A_n^*$ which can be extracted from each T_p. Source Port number, Destination Port number, IP address, and MAC address are the required network traffic attributes here [40]. Network parameters (P) can be retrieved from the network requirements (A^*) of individual T_p by the function P_k.

U is represented the IP addresses of existing users' by R_a with corresponding TCP traffic packet T_p in Eq. (1). Equation (2) retrieves the required network parameters (P_k) for each user corresponds to the Eq. (1). Equation (3) calculates the number of existing users in a specified time frame

$$U =(R_a * T_p) \in N, \tag{1}$$

$$P_k =P[(R_a * T_p) \ * \ (A_i^*)] \in N, \tag{2}$$

$$N(U_A^*) = \sum_{i=0}^{n} \frac{\delta(P_k)(A_i^*)}{\delta(t)} \text{ where } A_i \subset A \ \forall A_i \subset U, \ t\,[0, 1]. \tag{3}$$

Dynamic users (R_d) can be incorporated into this network space N in the specified time interval $[t, 0]$. In Eq. (4), the representations of all the hosts are described as U. Parameters' calculations (P_k) for cumulative users like existing users and new dynamic users are described in Eq. (5). The number of cumulative users in a specified period is defined by Eq. (6) where $P_i \leq n_i$ and $A_i \subset A$ for all $A_i \subset U$ [41]

$$U =[(R_a * T_p)\,(R_d * T_p)] \in N, \tag{4}$$

$$P_k =P(U * A_i^*) \in N, \tag{5}$$

$$N(U_A^*) = \sum_{i=0}^{n} \frac{\delta(P_k)(A_i^*)}{\delta(t)} \text{ where } A_i \subset A\ \forall A_i \subset U,\ t\,[0, 1]. \tag{6}$$

The incoming source IP address and the required destination IP address are represented by A_{sip} and A_{dip} . Total number of source (U_s) and destination (U_D) port numbers in a specified time interval are calculated in Eqs. (7) and (8), respectively

$$U_s = \int_{i=0}^{n} \sum_{i=0}^{n} \frac{\delta(A_{\text{sip}})}{\delta(t)}, \tag{7}$$

$$U_D = \int_{i=0}^{n} \sum_{i=0}^{n} \frac{\delta(A_{\text{dip}})}{\delta(t)}. \tag{8}$$

The requisite information regarding source and destination port addresses can be retrieved from the network parameters (A_i^*) and stored in the ARP table (T_b) defined in Eq. (9). The value of T_b would to be used further by the proposed approach for MAC address verification and granting the access to cloud resources

$$T_b(U_S + U_D) = \int_{i=0}^{n} \sum_{i=0}^{n} \frac{\delta(A_{\text{sip}})}{\delta(t)} + \int_{i=0}^{n} \sum_{i=0}^{n} \frac{\delta(A_{\text{dip}})}{\delta(t)}. \tag{9}$$

Calculation of Threshold Value

The selection of a proper threshold value helps to prevent any attack at a very early stage. It is hard to stamp a suitable threshold value to distinguish between normal and abnormal traffic. The inaccurate threshold will not only increase the false-positive rate of network traffic, but it increases the chances of intrusion by considering the malicious activity as regular traffic. In this paper, the static threshold approach is applied using the port scanning method of the respective TCP packets of incoming network traffic [42]. The threshold will be helpful to detect the constant or dramatic increase in the network flow [19].

Threshold (P_{tr}) is calculated by investigating the network traffic (P_i) statistics over a fixed period considered as t [43]. For normal traffic, $P_i \leq P_{\text{tr}}$, should be validated by the proposed approach. Depending upon the port number, the threshold value is assigned for authentication. If $P_i \geq P_{\mathrm{tr}}$, an anomalous network state is likely to be occurred. According to the algorithm proposed, it is impossible to know the spoofed MAC address without prior knowledge of the threshold value. The threshold can be calculated based on some specific network parameters.

a. Number of incoming traffic request coming from the router at the time period (t).
b. Count the number of incoming active traffic request and analyzing log.
c. Type and rate of incoming traffic (type such as TCP, UDP, and ICMP).
d. Extraction of destination port number.

To find the lower value (α) and the upper value (β) of the threshold, Eq. (10) is used where n_1 and n_0 are considered the two threshold coefficients here. After defining the threshold based on essential network parameters, regular calculations of the coefficients are carried out. If any coefficient's value is considerably greater than other, irregular network states can be found. As the TCP packet rates vary across TCP ports ranging from 0 to 65k, a threshold value for the single port must be greater than 1023

$$P_{\mathrm{tr}}(n1) = \frac{\beta}{\alpha}, \; P_{\mathrm{tr}}(n0) = \frac{1-\beta}{1-\alpha}. \tag{10}$$

From the set of network parameters (A^*) extracted from the TCP packet (T_p), we need the discrete source port address (U_s), from the set of all source IPs referred as $s : S \in A_i^*$ [44]. A_i^* must be updated for a distinguished source IP address (U_s). If U_s exceeds a certain threshold value (P_{tr}), the source IP address (s) is labeled as a spoofed according to the hypothesis $S1$ [33]. Based on the hypothesis $S0$, if U_s falls below a significant threshold (P_{tr}), then the source IP address (s) is labeled as benign. In either case, the algorithm monitors the source IP address (s) for categorization [41]. A_i^* is computed as follows in the likelihood ratio in Eq. (11):

$$\prod_{i=1}^{n} \frac{\Pr[A_i|S1]}{\Pr[A_i|S0]}. \tag{11}$$

To calculate the conditional probability, Eqs. (12) and (13) are used hereunder

$$\begin{cases} \Pr[A_i = 0|S0] = \theta_0 \\ \Pr[A_i = 0|S1] = \theta_1, \end{cases} \tag{12}$$

$$\begin{cases} \Pr[A_i = 1|S0] = 1 - \theta_0 \\ \Pr[A_i = 1|S1] = 1 - \theta_1. \end{cases} \tag{13}$$

Concerning Eqs. (12) and (13), the value of A_i is considered with two Boolean values where 0 represents success, and 1 is for failure; it gives the number of success or failure of connecting to the specific target IP addresses. θ_0 exhibits the regular traffic where θ_1 is responsible for malicious traffic. Here, the port number (U_s) of the TCP packet (T_p) is taken as a primary network parameter (A^*). Probability of the respective port number (U_s) is calculated in Eq. (14)

$$P_r(U_S) = \frac{\text{No. of packet with } A_i \text{ as src port address}}{\text{Total packet in } (t)}. \tag{14}$$

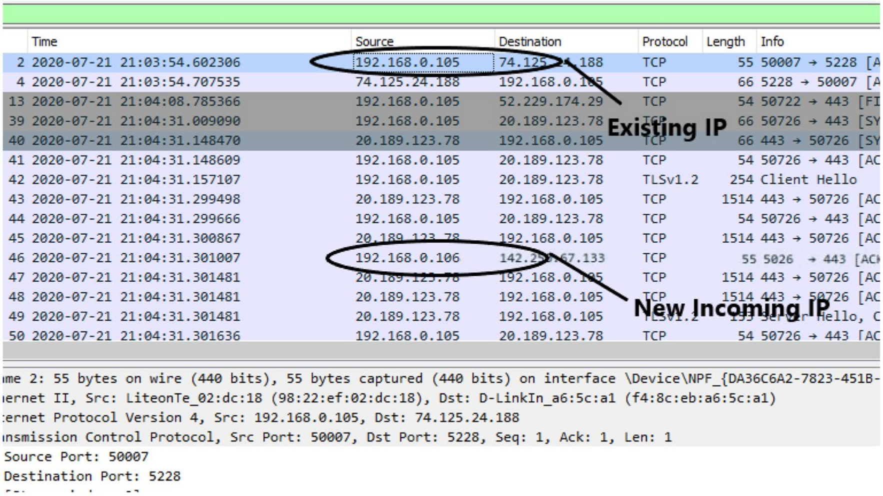
Based on this calculation, spoofed profile (suspect factor) is detected from in Eq. (15)

$$S_0 \leq \text{Spoofed Host} \geq S_1. \tag{15}$$

Results and Analysis

Wireshark version 3.2.5 is used to capture the network traffic with a configuration of 1.10 GHz Intel Pentium processor with 4 GB RAM, 1 TB HDD, and Intel HD Graphics card. Wireshark is a leading open-source network capturing tool that simultaneously captures all kinds of network traffic packets from network interface cards (NIC's) and provides traffic analysis and monitoring options. PCAP detects the network traffic on a fixed amount of time interval in a wireless network environment and filters out the TCP traffic.

From the snapshot of the Wireshark PCAP traffic analysis in Fig. 4, it is visible that the two highlighted IP addresses, namely 192.168.0.105 and 192.168.0.106, are utilized for analyzing MAC spoofing. Tables 1 and 2 have been validated mathematically according to our algorithm by observing the two IP addresses and their corresponding threshold values. Table 1 corresponds to the legitimate host. Based on our algorithm, the legitimate host is considered an authorized one and has got



	Time	Source	Destination	Protocol	Length	Info
2	2020-07-21 21:03:54.602306	192.168.0.105	74.125.24.188	TCP	55	50007 → 5228 [A
4	2020-07-21 21:03:54.707535	74.125.24.188	192.168.0.105	TCP	66	5228 → 50007 [A
13	2020-07-21 21:04:08.785366	192.168.0.105	52.229.174.29	TCP	54	50722 → 443 [FI
39	2020-07-21 21:04:31.009090	192.168.0.105	20.189.123.78	TCP	66	50726 → 443 [SY
40	2020-07-21 21:04:31.148470	20.189.123.78	192.168.0.105	TCP	66	443 → 50726 [SY
41	2020-07-21 21:04:31.148609	192.168.0.105	20.189.123.78	TCP	54	50726 → 443 [AC
42	2020-07-21 21:04:31.157107	192.168.0.105	20.189.123.78	TLSv1.2	254	Client Hello
43	2020-07-21 21:04:31.299498	20.189.123.78	192.168.0.105	TCP	1514	443 → 50726 [AC
44	2020-07-21 21:04:31.299666	192.168.0.105	20.189.123.78	TCP	54	50726 → 443 [AC
45	2020-07-21 21:04:31.300867	20.189.123.78	192.168.0.105	TCP	1514	443 → 50726 [AC
46	2020-07-21 21:04:31.301007	192.168.0.106	142.250.67.133	TCP	55	5026 → 443 [ACK
47	2020-07-21 21:04:31.301481	20.189.123.78	192.168.0.105	TCP	1514	443 → 50726 [AC
48	2020-07-21 21:04:31.301481	20.189.123.78	192.168.0.105	TCP	1514	443 → 50726 [AC
49	2020-07-21 21:04:31.301481	20.189.123.78	192.168.0.105	TLSv1.2	155	Server Hello, C
50	2020-07-21 21:04:31.301636	192.168.0.105	20.189.123.78	TCP	54	50726 → 443 [AC

```
ıme 2: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{DA36C6A2-7823-451B-
ıernet II, Src: LiteonTe_02:dc:18 (98:22:ef:02:dc:18), Dst: D-LinkIn_a6:5c:a1 (f4:8c:eb:a6:5c:a1)
:ernet Protocol Version 4, Src: 192.168.0.105, Dst: 74.125.24.188
ınsmission Control Protocol, Src Port: 50007, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
Source Port: 50007
Destination Port: 5228
```

Fig. 4 PCAP snapshot of Wireshark network traffic with filtering TCP traffic

Table 1 Authorized user

IP address	Port number	Threshold value	Timing	Status info
192.168.0.105	50007	50007	2020-7-21 21:03:54	Existing
192.168.0.106	5026	9000	2020-7-21 21:04:31	Incoming new IP address
192.168.0.106	9252	18000	2020-7-21 21:04:31	Mismatch: Increment
192.168.0.106	10252	17920	2020-7-21 21:04:32	Exact mismatch: Decrement
192.168.0.106	11598	17800	2020-7-21 21:04:33	Exact mismatch: Decrement
192.168.0.106	12454	17650	2020-7-21 21:04:34	Exact mismatch: Decrement
192.168.0.106	13569	17400	2020-7-21 21:04:36	Exact mismatch: Decrement
192.168.0.106	12690	17070	2020-7-21 21:04:38	Exact mismatch: Decrement
192.168.0.106	14920	16850	2020-7-21 21:04:41	Exact mismatch: Decrement
192.168.0.106	15526	16610	2020-7-21 21:04:45	Exact mismatch: Decrement

Table 2 Spoofed user

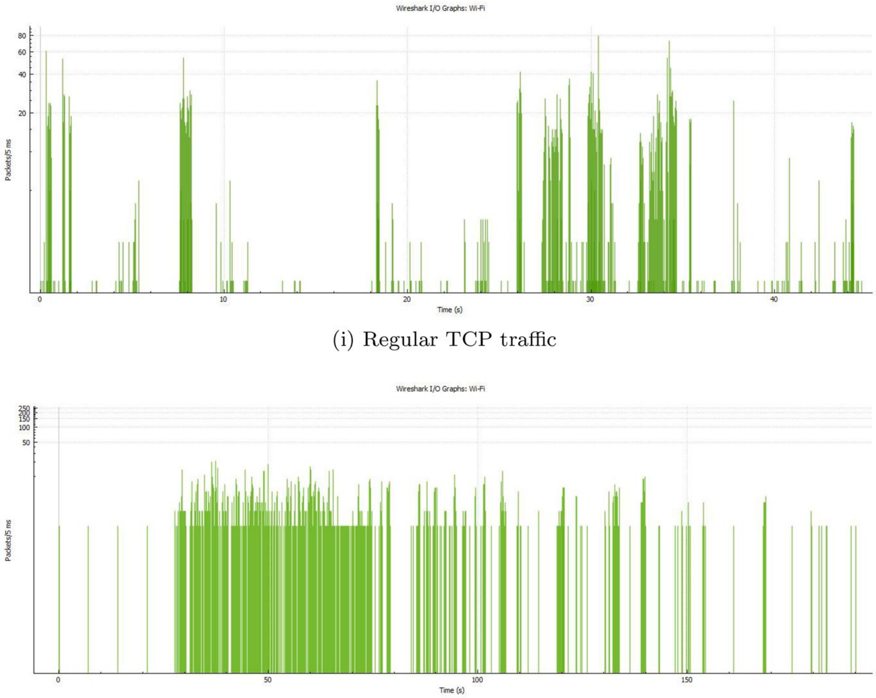
IP address	Port number	Threshold value	Timing	Status info
192.168.0.105	50007	50007	2020-7-21 21:03:54	Existing
192.168.0.106	5026	9000	2020-7-21 21:04:31	Incoming new IP address
192.168.0.106	20400	18000	2020-7-21 21:04:31	Mismatch: Increment
192.168.0.106	27911	36000	2020-7-21 21:04:32	Increment of threshold
192.168.0.106	36515	35980	2020-7-21 21:04:33	Exact mismatch: Decrement
192.168.0.106	41240	71960	2020-7-21 21:04:34	Increment of threshold
192.168.0.106	49189	70458	2020-7-21 21:04:36	Exact mismatch: Decrement
192.168.0.106	50456	69296	2020-7-21 21:04:38	Exact mismatch: Decrement
192.168.0.106	76525	69076	2020-7-21 21:04:41	Exact mismatch: Decrement
192.168.0.106	99892	138152	2020-7-21 21:04:45	Exact mismatch: Decrement Reject packet

the access to the SDN framework of cloud architecture. It is also clear from Table 2 that the spoofed already happened to the new IP address; thus, it needs to discard the TCP packet.

Figure 5 represents the Wireshark PCAP I/O graph considering the TCP packet based on the above two cases on a fixed amount of time interval. The I/O graph represented in Fig. 5i corresponds to the legitimate IP addresses where consistency is maintained. However, from the abrupt increment of TCP traffic exhibited in Fig. 5ii, our algorithm has considered it as spoofed traffic.

Figure 6 is illustrated hereunder, by analyzing the values of Tables 1 and 2 in these regards. The red line shows the threshold value, and the green line indicates the corresponding port number.

It is visible from Fig. 6ii that for the spoofed user, the threshold value is beyond the maximum limit, and the abrupt changes break the linearity where the authorized user's graph is linear in fashion in Fig. 6i. All the existing algorithms predict a legitimate user as a spoofed one, which increases the false-positive rate where our



(i) Regular TCP traffic

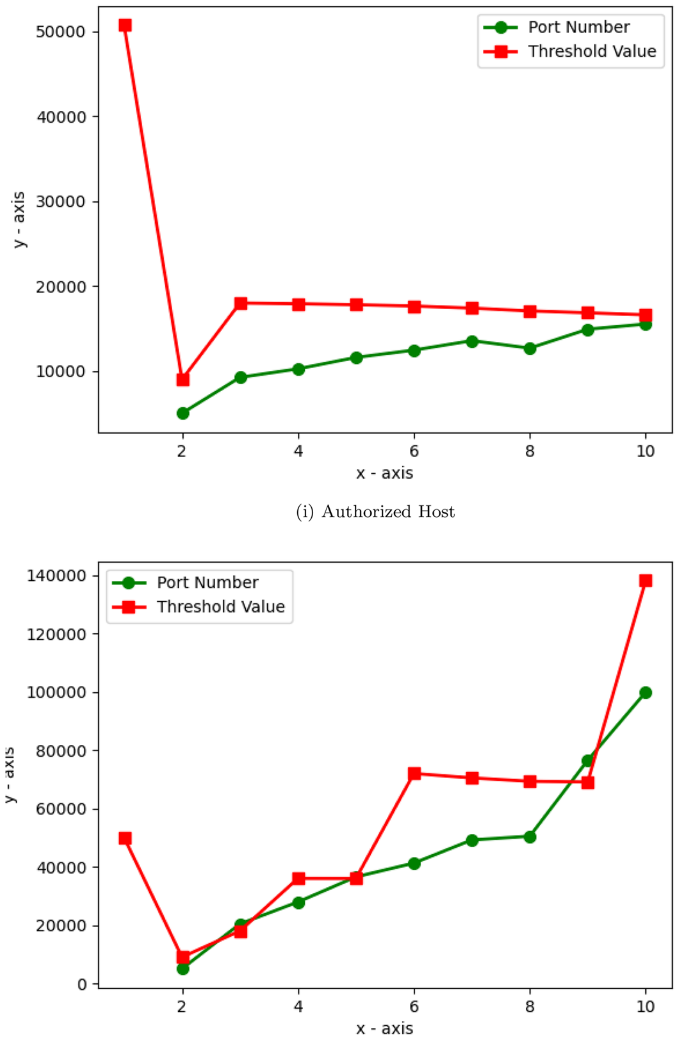
(ii) Spoofed TCP traffic

Fig. 5 Wireshark PCAP I/O graph considering TCP packet

algorithm outperforms among the existing algorithms by its self-learning nature to set an optimal threshold by considering several parameters.

Calculation of Entropy

Entropy is calculated in this section to analyze the randomness of malicious incoming traffic [45]. Entropy is considered a familiar and valuable concept of information theory for the measurement associated with the uncertainty of randomness. The degree of randomness is termed as a concentration of distribution [46]. Entropy can be used to analyze the distribution of randomness collected from the attributes of the TCP packet over a certain period. Attributes can be referred to as source IP, destination IP, source port, destination port, and many more. If there are N incoming packets, then the value of entropy will vary from 0 to $\log_2 N$. Entropy is zero where all distribution values are identical and highest when all the values are different [47]. We have used Wireshark simulation for experimental purposes and captured the network traffic over 1 h time. As per the definition, if there is N number of TCP traffic coming from a particular source IP port, the entropy will give a clear analysis if the traffic is beyond the threshold or not. The entropy of the random variable X is defined as $H(X)$ in Eq. (16).



(i) Authorized Host

(ii) Spoofed Host

Fig. 6 Threshold according to the Port Number representation for authorized host and for spoofed host

$$H(X) = -\sum_{i=1}^{n} P(x_i)\log_2(P(x_i)). \tag{16}$$

The random variable $X = x_1, x_2, \dots x_n$ is considered as possible realizations and $p(x_i)$ be the corresponding probabilities in Eq. (17).

$$P_i = -\frac{\text{No. of time of } x_i \text{ of } X}{\text{Window size}} \tag{17}$$

$$\begin{cases} \text{if}\,, H_0, < \text{Threshold} : \text{Suspected as spoofing} \\ \text{if}\,, H_0, > \text{Threshold} : \text{No attack detected} \end{cases} \tag{18}$$

$$\text{Normalized Entropy} : H_0 = \frac{H(x)}{\log_2(n)} \tag{19}$$

By considering Eq. (18), the performance of our algorithm could be enhanced. The incremental value of the entropy H_0 could be normalized using Eq. (19).

Performance Evaluation

For the assessment of our proposed method, we have compared the approach with the existing approaches of [20, 33–36]. All these chosen researches are considered to be the best performing methods for ensuring MAC spoofing defensive mechanism by capturing the TCP/IP network traffic. Most of the existing researches of [20, 35, 36] are based on the physical characteristics of the wireless network, i.e., RSS values, wherein the framework of [34] is based on eliminating MAC spoofing from blacklisted MAC address from the network. We have evaluated the accuracy of the existing methods of [20, 33–36] along with our proposed approach.

The proposed method attained an accuracy rate of 97.75%, wherein in [34], the accuracy rate is calculated as 96.28%. Researchers in [20] achieved an accuracy rate of 95.28%. Vijayakumar et al. [33] and Alotaibi et al. [35] detected the similar accuracy rate of 94.83% from their proposed work. From the research of Jokar et al. [36], 94.75% accuracy rate is calculated. It is evident that our proposed method outperforms the existing researches in terms of accuracy. Figure 7 illustrates the overall accuracy compared to previously proposed methods.

For evaluating the performance of our approach more rigorously, we have used the receiver-operating characteristic (ROC) curve which is illustrated in Fig. 8. This curve plots the detection rate (true positive rate) against the false-positive rate (FPR) of the computed values from the methods. It is visible from Fig. 8 that the approach

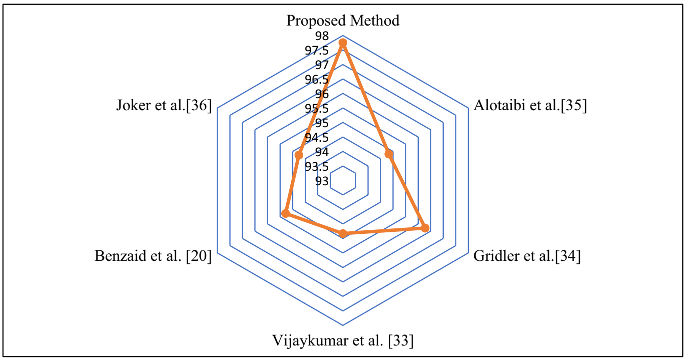


Fig. 7 Overall accuracy (%) of the proposed method compared to other methods

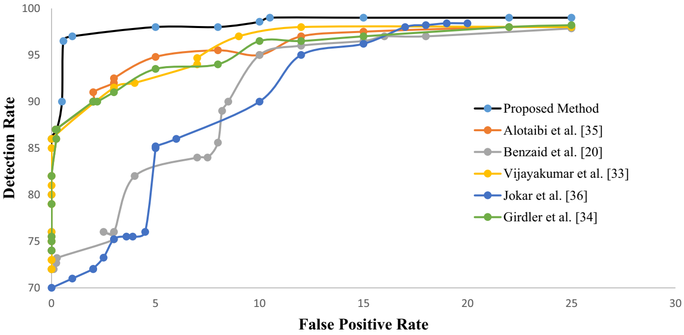


Fig. 8 ROC curve of the proposed method compared to other methods

exhibits a low false-positive rate and significantly high detection rate compared to other methods. At 0.5% FPR, our proposed method has achieved a 96.5% detection rate, which is considered upstanding. Furthermore, the detection rate has been calculated explicitly by comparing with other existing methods in Fig. 9.

Comparing the throughput analyses by the researchers in their existing work, our proposed approach has achieved 98.87%, which is very effective rate compared to other methods. Figure 10 exhibits the analysis of throughput in the bar graph.

Conclusion

The permanent shift towards work-from-home has adhered by the corporate structure to contain the virus undoubtedly in this coronavirus outbreak. The dependency on cloud resources has dramatically elevated due to the present COVID-19 pandemic. The fast-paced adoption of the cloud enables the workforce to keep the enterprise's revenue growth straight and avoid any financial loss. However, the change in work culture would also increase the chances of a cybersecurity attack, MAC spoofing attack,and DDoS/ DoS attack due to the divergent incoming traffic from an untrusted network.

This paper introduces a novel access control policy based on a zero-trust network by creating a defensive mechanism against MAC spoofing in the software-defined network (SDN) framework of cloud architecture. When the access control policies of the corporate structure need a change, our approach exhibits higher accuracy by collecting the individual network traffic from untrusted zones by checking their source TCP/IP traffic and corresponding MAC address. The use of multiplicative increase and additive decrease algorithm helps to detect the advanced MAC spoofing attack before penetrating SDN-based cloud resources. The dynamic threshold value is stamped based on the incoming port number using the ARP protocol policy. The threshold stamping gives the chance to rectify a legitimate user's traffic before classifying it to the attacker, which reduces the false-positive rate. The self-learning nature of the threshold stamping system helps to anticipate the network's characteristics for the spoofed traffic

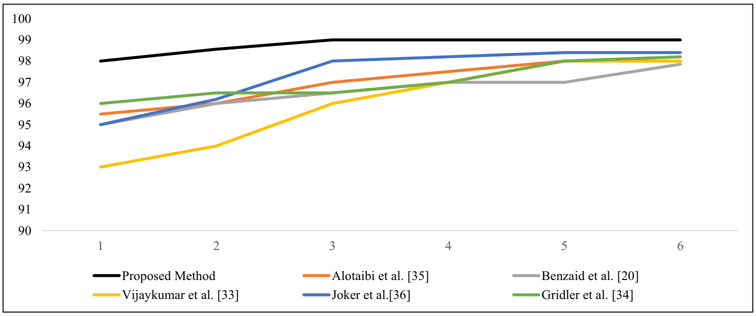


Fig. 9 Detection rate of the proposed method compared to other methods

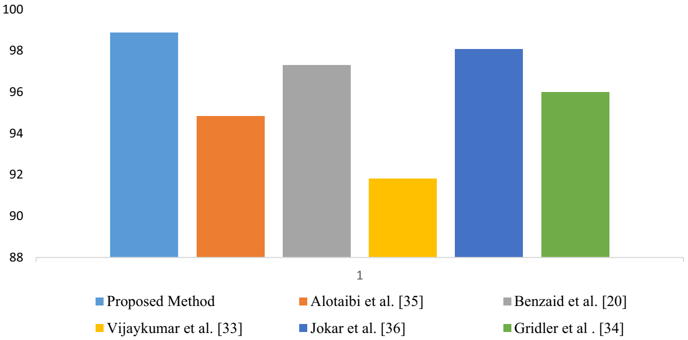


Fig. 10 Comparison of throughput analysis

classification. When the network sees a rapid rise, our AI-based model helps to decrease the threshold and normalizes the traffic. However, in an adverse scenario, the highly skilled attacker's presence does not allow the threshold to decrease, making the TCP packet rejected by the algorithm itself and does not allow the spoofed user to penetrate the SDN framework of cloud architecture. It is observed that our proposed method outperforms the existing literature by achieved a high detection rate and throughput. As we cannot deliberately prevent this preconceived security threat, however, with the help of this approach, seamless threats can be eliminated and prevent the attacker from using the cloud resources. In a software-defined-network paradigm, the elimination of threats ensures the cloud resources' optimized security. However, analyzing the traffic and removing a spoofed user are time-consuming procedures that can be enhanced by further research work.

Funding Not applicable.

Data Availability The authors confirm that the data supporting the findings of this study are available within the article.

Code Availability The datasets analyzed in the specified software during the current study are available in the article only.

Declarations

Conflict of Interest This is to declare that we, the authors of the paper titled "Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic", submitted to the special issue "AI in Global Epidemics" in the Journal "New Generation Computing" for review and possible publication share no conflict of interest with any probable experts in the field who might be potentially reviewing the aforesaid paper. Sudakshina Mandal, Prof (Dr.) Danish Ali Khan, Dr. Sarika Jain.

References

1. Alashhab, Z.R., Anbar, M., Singh, M.M., Leau, Y.B., Al-Sai, Z.A., Alhayja'a, S.A.: Impact of coronavirus pandemic crisis on technologies and cloud computing applications. J. Electron. Sci. Technol. **19**(1), 100059 (2021)
2. Song, M.S., Lee, J.D., Jeong, Y.S., Jeong, H.Y., Park, J.H.: DS-ARP: a new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments. Sci. World J. **2014**, 1–7 (2014)
3. Yu, J., Kim, E., Kim, H., Huh, J.: A framework for detecting MAC and IP spoofing attacks with network characteristics. In: 2016 International conference on software security and assurance (ICSSA), pp. 49–53 (2016)
4. Osanaiye, O.A.: Short paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. In: 2015 18th International conference on intelligence in next generation networks, pp. 139–141 (2015)
5. Jian, T., Rendon, B. C., Gritsenko, A., Dy, J., Chowdhury, K., Ioannidis, S.: MAC ID spoofing-resistant radio fingerprinting. In: 2019 IEEE global conference on signal and information processing (GlobalSIP), Ottawa, ON, Canada, pp. 1–5 (2019)
6. Gajbhiye, Y., Daruwala, R.D.: RSS-based spoofing detection and localization algorithm in IEEE 802.11 wireless networks. In: 2016 International conference on communication and signal processing (ICCSP), Melmaruvathur, Tamil Nadu, India, pp. 1642–1645 (2016)
7. Ahmad, S., Mehfuz, S., Beg, J.: Securely work from home with CASB policies under COVID-19 pandemic: a short review. In: 2020 9th International conference system modeling and advancement in research trends (SMART), pp. 109–114 (2020)
8. DeCusatis, C., Liengtiraphan, P., Sager, A., Pinelli, M.: Implementing zero trust cloud networks with transport access control and first packet authentication. In: 2016 IEEE international conference on smart cloud (SmartCloud), New York, NY, USA, pp. 5–10 (2016)
9. Scott, B.: How a zero trust approach can help to secure your AWS environment. Netw. Secur. **2018**(3), 5–8 (2018)
10. Sivaraman, R.: Zero trust model. Technical report, S3telInc. (2015)
11. Casado, M., Foster, N., Guha, A.: Abstractions for software-defined networks. Commun. ACM **57**(10), 86–95 (2014)
12. Perrin, S.: Making networks SDN-ready with segment routing. Technical report, Cisco Systems Inc. (2017)
13. Aishwarya, R., Malliga, S.: Intrusion detection system- an efficient way to thwart against Dos/DDos attack in the cloud environment. In: 2014 International conference on recent trends in information technology, pp. 1–6 (2014)
14. Durairaj, M., Persia, A.: Theoretical framework of the algorithm to thwart MAC spoofing DoS attack in wireless local area infrastructure network. In: Padma Suresh, L., Dash, S.S. Panigrahi, B.K. (eds.) Artificial intelligence and evolutionary algorithms in engineering systems. Advances in Intelligent Systems and Computing, pp. 99–107. Springer India, New Delhi (2015)

15. Li, R., Liu, Q., Wang, M., We, X.: A novel framework for application of cloud computing in wireless mesh networks. In: 2014 Ninth international conference on P2P, parallel, grid, cloud and internet computing, pp. 448–452 (2014)
16. Ravi, N., Shalinie, S.M.: Learning-driven detection and mitigation of DDoS attack in IOT via SDN-cloud architecture. IEEE Internet Things J. **7**(4), 3559–3570 (2020)
17. Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., Zhai, Y.: A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. In: IEEE Internet of Things Journal, p. 1 (2020)
18. Vanickis, R., Jacob, P., Dehghanzadeh, S., Lee, B.: Access control policy enforcement for zero-trust-networking. In: 2018 29th Irish signals and systems conference (ISSC), Belfast, pp. 1–6 (2018)
19. Faizal, M.A., Zaki, M.M., Shahrin, S., Robiah, Y., Rahayu, S. Siti, Nazrulazhar, B.: Threshold verification technique for network intrusion detection system. arXiv:0906.3843 [cs] (2009)
20. Benzaïd, C., Boulgheraif, A., Dahmane, F.Z., Al-Nemrat, A., Zeraoulia, K.: Intelligent detection of MAC spoofing attack in 802.11 network. In: Proceedings of the 17th international conference on distributed computing and networking, ICDCN '16, New York, NY, USA, Association for Computing Machinery, pp. 1–5 (2016)
21. Bekerman, D., Shapira, B., Rokach, L., Bar, A.: Unknown malware detection using network traffic classification. In: 2015 IEEE conference on communications and network security (CNS), Florence, Italy, pp. 134–142 (2015)
22. Indre, I., Lemnaru, C.: Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things. In: 2016 IEEE 12th international conference on intelligent computer communication and processing (ICCP), Cluj-Napoca, Romania, pp. 175–182 (2016)
23. Hatcher, W.G., Yu, W., Nguyen, J.H., Wei, S., Chen, Z.: A cloud/edge computing streaming system for network traffic monitoring and threat detection. Int. J. Secur. Netw. **13**(3), 169 (2018)
24. El-Alfy, E.-S.M., Al-Obeidat, F.N.: Detecting cyber-attacks on wireless mobile networks using multicriterion fuzzy classifier with genetic attribute selection. Mob. Inf. Syst. **1–13**, 2015 (2015)
25. Eidle, D., Ni, S.Y., DeCusatis, C., Sager, A.: Autonomic security for zero trust networks. In: 2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference (UEMCON), New York City, NY, pp. 288–293 (2017)
26. Prasse, P., Machlica, L., Pevný, T., Havelka, J., Scheffer, T.: Malware detection by analysing network traffic with neural networks. In: 2017 IEEE security and privacy workshops (SPW), pp. 205–210 (2017)
27. Li, K., Chen, R., Gu, L., Liu, C., Yin, J.: A method based on statistical characteristics for detection malware requests in network traffic. In: 2018 IEEE third international conference on data science in cyberspace (DSC), Guangzhou, pp. 527–532 (2018)
28. Prasse, P., Gruben, G., Machlika, L., Pevny, T., Sofka, M., Scheffer, T.: Malware detection by HTTPS traffic analysis. In: 2017 Institutional Repository of the Potsdam University, p. 12 (2017)
29. Wang, J., Yang, L., Wu, J., Abawajy, J.H.: Clustering analysis for malicious network traffic. In: 2017 IEEE international conference on communications (ICC), Paris, France, pp. 1–6 (2017)
30. DeCusatis, C., Liengtiraphan, P., Sager, A.: Advanced intrusion prevention for geographically dispersed higher education cloud networks. In: Auer, M.E., Zutin, D.G. (eds.) Online engineering & internet of things, vol. 22, pp. 132–143. Series Title: Lecture Notes in Networks and Systems. Springer International Publishing, Cham (2018)
31. Bajtoš, T., Gajdoš, A., Kleinová, L., Lučivjanská, K., Sokol, P.: Network intrusion detection with threat agent profiling. Secur. Commun. Netw. **1–17**, 2018 (2018)
32. Patel, H., Jinwala, D.C.: LPM: a lightweight authenticated packet marking approach for IP traceback. Comput. Netw. **140**, 41–50 (2018)
33. Vijayakumar, R., Selvakumar, K., Kulothungan, K., Kannan, A.: Prevention of multiple spoofing attacks with dynamic MAC address allocation for wireless networks. In: 2014 International Conference on Communication and Signal Processing, Melmaruvathur, India, pp. 1635–1639 (2014)
34. Girdler, T., Vassilakis, V.G.: Implementing an intrusion detection and prevention system using software-defined networking: defending against ARP spoofing attacks and blacklisted MAC addresses. Comput. Electr. Eng. **90**, 106990 (2021)
35. Alotaibi, B., Elleithy, K.: A new MAC address spoofing detection technique based on random forests. Sensors **16**(3), 281 (2016)

36. Jokar, P., Arianpoo, N., Leung, V.C.M.: Spoofing detection in IEEE 802.15.4 networks based on received signal strength. Ad Hoc Netw. **11**(8), 2648–2660 (2013)
37. Lawson, C., MacDonald, N.: How to evaluate and operate a cloud access security broker (2015)
38. Anathi, M., Vijayakumar, K.: An intelligent approach for dynamic network traffic restriction using MAC address verification. Comput. Commun. **154**, 559–564 (2020)
39. Dacosta, I., Chakradeo, S., Ahamad, M., Traynor, P.: One-time cookies: preventing session hijacking attacks with stateless authentication tokens. ACM Trans. Internet Technol. **12**(1), 1–24 (2012)
40. Ahmed, S.T., Sandhya, M., Sankar, S.: TelMED: dynamic user clustering resource allocation technique for MooM datasets under optimizing telemedicine network. Wirel. Pers. Commun. **112**(2), 1061–1077 (2020)
41. Liu, S.: MAC spoofing attack detection based on physical layer characteristics in wireless networks. In: 2019 IEEE international conference on computational electromagnetics (ICCEM), Shanghai, China, pp. 1–3 (2019)
42. Port Scanning: Detect Malicious Network & Port Scanner Requests | ExtraHop. Library Catalog. http://www.extrahop.com
43. Sukhov, A.M., Sagatov, E.S., Baskakov, A.V.: Rank distribution for determining the threshold values of network variables and the analysis of DDoS attacks. Proc. Eng. **201**, 417–427 (2017)
44. Mell, P., Harang, R.: Limitations to threshold random walk scan detection and mitigating enhancements. In: 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, pp. 332–340 (2013)
45. Nychis, G., Sekar, V., Andersen, D.G., Kim, H., Zhang, H.: An empirical evaluation of entropy-based traffic anomaly detection. In: Proceedings of the 8th ACM SIGCOMM conference on Internet measurement conference - IMC '08, Vouliagmeni, Greece, p. 151. ACM Press (2008)
46. Sharma, S., Sahu, S.K., Jena, S.K.: On selection of attributes for entropy based detection of DDoS. In: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1096–1100 (2015)
47. Wagner, A., Plattner, B.: Entropy based worm and anomaly detection in fast IP networks. In: Proceedings of IEEE International Workshop on Enabling Technologies, Infrastructures for Collaborative Enterprises (2005)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Sudakshina Mandal[1] · Danish Ali Khan[1] · Sarika Jain[2]

Sudakshina Mandal
2018rsca002@nitjsr.ac.in

Sarika Jain
jasarika@nitkkr.ac.in

[1] Department of Computer Applications, National Institute of Technology Jamshedpur, Jamshedpur, Jharkhand 831014, India

[2] Department of Computer Applications, National Institute of Technology Kurukshetra, Kurukshetra, Haryana 136119, India