Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777528

ADDRESS SHUFFLING AI TECHNIQUES FOR IOT SECURITY USING RASPBERRY PI

Pardeep Kumar
Research Scholar, ECE Department, IKG PTU, Jalandhar
sharmaashupk@gmail.com

Dr. Amit Gupta
Assistant Professor, ECE Department, IKGPTU, Jalandhar
amitguptaptu@gmail.com

Abstract—One of the primary security risks in IoT networks is address-based attacks, where hackers can exploit vulnerabilities by targeting specific IP addresses. To address this issue, various security techniques have been proposed, including address shuffling. Address shuffling is a security technique that involves randomly changing the IP address of an IoT device periodically, making it difficult for hackers to target the device. However, manually changing IP addresses can be cumbersome, especially when dealing with several IoT devices.

We propose an AI-based address shuffling technique for IoT security. Our approach involves using machine learning algorithms to predict the best time to change the IP address of an IoT device based on various parameters such as accuracy, precision, throughput &time taken or speed to shuffle the IP address. We show that our approach can effectively reduce the risk of address-based attacks in IoT networks, while minimizing the impact on device performance and usability. Our experiments demonstrate that our approach outperforms existing techniques and can provide a more secure and efficient IoT environment.

Keywords: — IoT Security, IP Address Shuffling, Artificial Intelligence, IDS

INTRODUCTION

The emergence of the IoT has significantly changed how we engage with technology in our daily lives[1], [2]. Author presented a survey on smart homes and wearable devices to industrial automation and smart cities, & explained that IoT has opened up a world of possibilities[3]. However, with the increasing adoption of IoT devices, security concerns have also escalated[2], [4]–[8]. IoT devices are susceptible to threats because of their networked nature, which can have severe consequences ranging from data theft to physical harm[4].

Due to the unpredictability of node mobility, network topologies can change frequently. The IP addressing protocol assigns a unique network address to a network node that is not configured, allowing it to communicate with other network nodes via multi-hop wireless links[9]. The evaluation of IP address shuffling technique for IoT security has been carried out by several researchers in different IoT environments. The evaluation includes the effectiveness of the technique in mitigating different types of attacks, the impact on network performance, and the scalability of the approach.

Effectiveness in Mitigating Attacks:

Studies have shown that IP address host shuffling is a tool created for endpoint security protection & is an effective technique in mitigating various security threats, including IP address-based attacks, eavesdropping attacks, and denial-of-service (DoS) attacks[10]. The dynamic IP address shuffling mechanism periodically changes the IP addresses of IoT devices, making it difficult for attackers to locate them. The approach also helps to prevent attacks that rely on the knowledge of the IP address of the target device, such as IP address spoofing attacks. Consequently, IP address reconfiguration can improve IoT device safeguards by lowering the possibility of effective attacks.

Impact on Network Performance:

The impact of IP address shuffling on network performance depends on the frequency of IP address changes and the size of the IoT network. Studies have shown that frequent IP address changes may increase network traffic and delay, which can affect the performance of IoT applications. Therefore, an optimal interval for IP address changes should be determined based on the network size and the security requirements of the IoT environment. However, the impact of IP address shuffling on network performance can be minimized by implementing an efficient IP address management system that ensures seamless IP address switching.

The scalability of IP address shuffling depends on the complexity of the IoT network and the availability of resources. Studies have shown that IP address shuffling can be applied to large-scale IoT networks without significant performance degradation. The approach can also be easily integrated into existing IoT security frameworks, making it a scalable solution for enhancing IoT security.

Ad hoc network configurations are vulnerable to attack because there is no first line of defence other than the standard IEEE802.11authentication. A viable defence against attacks on these ad hoc networks is the installation of intrusion detection systems (IDS) either at the network's edge or at the node level. Because the IDS, alerts the network administrator to any suspicious behaviour it detects, the administrator can take measures to protect sensitive information and prevent further assaults. The datasets or network traffic to be monitored must be carefully chosen if an IDS is to be built successfully in a wireless setting[11].

One of the primary security concerns in IoT networks is address-based attacks[12], [13]. In an address-based attack, a hacker targets a specific IP address to gain unauthorized access to an IoT device. Address-based attacks can be devastating for IoT networks as they can allow hackers to take control of devices, steal data, or launch further attacks[14]. Address shuffling is a security technique that involves changing the IP address of an IoT device periodically to reduce the risk of address-based attacks. However, manually changing IP addresses can be challenging, especially when dealing with a large number of IoT devices.

In recent years, artificial intelligence (AI) has proven to be an effective method for dealing with IoT network security issues[14]. AI-developed algorithms can trawl through terabytes of data to look for patterns that people might overlook[15]. Anomalies in network traffic can be detected by ML algorithms, which can then be used to pinpoint possible security issues and implement preventative measures[16]. Address shuffling can also be automated with AI, making it more convenient to use and administer in IoT networks. .

Address shuffling using AI involves using ML algorithms to predict the best time to change the IP address of an IoT device based on various parameters such as device usage, network traffic, and historical attack patterns. The AI system can analyze the behavior of IoT devices and detect patterns that may indicate a potential attack[15]. For example, if an IoT device suddenly starts sending large amounts of data to an unknown IP address, it may indicate a data breach. The AI system can then trigger an address shuffle to mitigate the risk of an attack.

Another advantage of using AI for address shuffling is that it can minimize the impact on device performance and usability. Manual address shuffling can cause downtime and disrupt the normal operation of IoT devices, leading to user frustration and decreased productivity[11]. However, AI algorithms can schedule address shuffles during periods of low device usage or when devices are idle, minimizing the impact on device performance and usability.

Furthermore, AI-based address shuffling can adapt to changing network conditions and attack patterns. As hackers develop new attack strategies, AI algorithms can learn and adapt to new threats, ensuring that IoT networks remain secure. Additionally, AI algorithms can monitor the effectiveness of address shuffling and make adjustments as needed to optimize security and minimize disruption to device operation.

LITERATURE REVIEW & ANALYSIS

IP address shuffling in network layer is an adaptable method of surveillance defence that routinely reconfigures the links between devices and IP and transport layer (protocol and port) addresses.

Devices in the Block IoT network are associated with the internet and can exchange data with one another using their respective IP addresses. To make it more difficult for attackers to identify and target individual IoT devices, IP address shuffling is a security method that randomly changes the IP addresses of those devices across a network[16]. This technique can also prevent attacks such as DDoS assaults, which saturate a network with requests and cause it to crash[17]

The authors propose a gatekeeper mechanism, which shares address mapping information with the registration server while also making it possible for the genuine IP addresses of IoTs within local subnetworks to remain hidden from the outside world. The registration server has access to information on worldwide address mapping, whereas the gatekeeper is in charge of local IoT device mapping and delivers data needed for security management. When connecting two IoTs that are separated by a gatekeeper, the gatekeeper plays a crucial role in establishing a secure session from beginning to end[18].

Obtaining a routable address is possible for nodes in mobile ad hoc networks through dynamic address assignment without any prior configuration, providing a mechanism for dynamic network membership and enabling them to interact with one another in the absence of a centralised infrastructure. The authors proposed a new method of assigning addresses that is both efficient and time-saving[19].

The literature review was conducted using the "IoT security," "IP address shuffling," and "AI." The search was performed on multiple databases & focused on IoT security using IP address shuffling using AI. The exclusion criteria were studies that did not meet the inclusion criteria or studies.

IP Address Shuffling

Network-level MTDs, such as time-varying topology, are thought to be viable in embedded systems, whereas host- and application-level MTDs are challenging to implement[20]. An illustration of a network-level MTD is the periodic coordinated shifting of IPv6 and IPv4 network addresses for the devices.

To enhance attacker cost, the address mutation is designed to maintain the new IP address selection as random as feasible[21]. Several studies have proposed IP address shuffling as a technique to enhance IoT security. IP address shuffling involves periodically changing the IP address of IoT devices to prevent attackers from identifying and targeting vulnerable devices. The authors showed that their technique improved the security of the IoT network by reducing the success rate of attacks. Moving Target Defense (MTD) was put forth as a brand-new, ground-breaking technology to change the asymmetrical relationship between attacks and defences. It also provided a brief overview of the research accomplishments of network address shuffling in accordance with two patterns that the authors had previously identified.

The concept of IP address randomization to defend against port-scanning attacks was discussed & demonstrated that IP address randomization could effectively protect clients from attacks by making it difficult for attackers to track down the device's location. Together with the capability to scan any range of IP addresses using whatever ports, port scanning detection may significantly limit the losses brought on by viruses[22].

By keeping an eye on the activity of the opposition and adaptably rearranging the addresses of network hosts, the study described a revolutionary proactive adaptive defensive strategy that introduces dynamism into static systems. The ability to easily remove network hosts from dangerous network ranges and addresses allows for this flexibility[23].

The network is exposed to a huge number of virtual decoy nodes, each of which is given a real IP address and outfitted with condensed versions of common protocols to be taken as a functioning system. The rate at which the real node is found and attacked is decreased using decoy-based MTD. The addresses of all the real and fake nodes are then periodically updated and randomly dispersed[24].

In another research, author proposed a technique that utilizes IP address shuffling to protect IoT devices from network-level attacks[25]. Their results showed that IP address shuffling could significantly reduce the success rate of attacks.

The success rate of network-level assaults was dramatically decreased by frequent IP address shuffling, according to a recent study that assessed the effectiveness of IP address shuffling for IoT security and measured the impact of various shuffling rates on security [27].

An IP address swap can reduce the network-wide impact of a dynamic cyber defence approach from an SDN perspective[20][26].

An attacker cannot determine the origin or destination of a specific communication because the identifying characteristics of IoT nodes are dynamic [29]. This is because the IP address patterns are continually shifting and seem random to an outsider. Because packets carrying information produced by a particular node cannot be linked, the system offers additional security advantages, is relatively easy to install, and doesn't require any changes to the present networking architecture.

By using a pseudorandom permutation algorithm to shuffle the IP addresses of IoT devices in a network, a secure and lightweight IP shuffling scheme for IoT networks was created, which not only increased the security of the IoT network but also decreased the overhead associated with IP address shuffling WNG [30].

In terms of security and communication overhead, a lightweight IP shuffling technique that employs the Hash function beats conventional IP shuffling strategies[27].

The security of the IoT network was enhanced while retaining a minimal communication overhead using a dynamic IP address shuffling approach that shuffles IP addresses based on the amount of traffic in a network.

In terms of communication overhead and security, an effective IP shuffling strategy that employs a Bloom filter to shuffle IP addresses in a network performs better than existing IP shuffling systems [28].

By advocating a method for continually switching IP addresses at certain intervals, the authors looked at how successful IP address shuffling is at boosting IoT security. According to the study, IP address rerouting increases IoT device security by making it more challenging for attackers to locate the devices.

Another research suggested a security architecture that makes use of dynamic IP address shuffling, which changes IoT devices' IP addresses on a regular basis, to improve the security of those devices. According to the study, the suggested security architecture may successfully counteract numerous security risks, such as IP address-based assaults.

There is a way for leveraging IP address shuffles to improve the security of IoT devices by combining them with encryption and decryption methods to make it difficult for hackers to access them[29].

The general-sum game-based cyber-attack and defensive competition for IoT in real-time, as well as the realistic scaling of the current IoT-enabled MTD and decoy ideas and increase the efficacy of these approaches in IoT settings, were taken into consideration while developing the IoDM model[30].

The study also suggested an IP address shuffling based safety feature to enhance IoT systems protection in a fog computing environment and found that the mechanism effectively mitigated different security risks, including IP address-based assaults.

Using 02 Byte addresses, a unique approach for altering IP and MAC addresses called AShA with HMAC for connections with even about 2000 terminals, do a worldwide collision-free IP regeneration.. It is also easy to construct and has little network overhead[16].The authors employed a dynamic IP address shuffling mechanism that periodically changes the IP addresses of IoT devices in a network. The study revealed that the proposed security framework can effectively mitigate various security threats, including IP address-based attacks and eavesdropping attacks.

The author used network address shuffling to solve the serious trust and security issues that Wireless Sensor Networks (WSN) are currently facing. They also took into account the effects of network address shuffling control, network autoimmunity control, and defence cost. This solution was then formulated as a stochastic cost optimisation problem. Lyapunov optimisation theory is used to increase its generality[31]. The suggested technique efficiently reduces a variety of security risks, including IP address-based attacks, in a WSN environment by utilising a dynamic IP address shuffling mechanism that routinely alters the IP addresses of IoT devices.

AI for IP Address Shuffling

To improve IP address shuffle, the study suggested utilising AI algorithms that can both monitor the activity of IoT devices and create new IP addresses depending on the network's present configuration. An AI-based IP address shuffle method that reduced the likelihood of successful assaults while using a recurrent neural network to create new IP addresses [25].

When it comes to identifying human actions, automated feature engines for CNNs and LSTMs outperform models trained with statistical machine learning approaches [25]. Results have demonstrated that a hybrid model that includes CNN and LSTM performs better than conventional machine learning techniques for the diagnosis of Parkinson's disease. The extraction of geographical and temporal components from network traffic data using a hybrid network made up of CNN & LSTM paves the way for improved intrusion detection systems[19].

By comparing it to other studies for models trained on an oversampled ECG database and verified on an independent test dataset, the efficacy of the hybrid CNN/LSTM model was examined[32].

The hybrid model's outcomes are superior in every way to those of cutting-edge methods.

In a different study, author explored the effectiveness of Random Forest technique for credit card fraud detection. Their results showed that the Random Forest classifier outperformed other ML techniques in terms of accuracy, sensitivity, and specificity.

Random Forest classifier demonstrated more accuracy than conventional machine learning algorithms when used to diagnose breast cancer[26].

Deep learning models surpassed the Random Forest classifier in terms of accuracy and sensitivity, according to research using deep learning classifiers to diagnose diabetic retinopathy[26][10].

EXPEERIMENTAL SETUP

Simulation of IoT nodes is done in COOJA. This helps to test and evaluate the performance of IoT applications and protocols before deploying them in real-world scenarios. COOJA is a popular network simulator used to simulate wireless sensor networks. Contiki/Cooja simulator tool provides a convenient environment for researchers to experiment with different network topologies, protocols, and security mechanisms. In this context, researchers can use Cooja to evaluate the effectiveness of IP address shuffling in increasing network resilience. To conduct an IP address shuffling experiment in Cooja, the following steps have been followed:

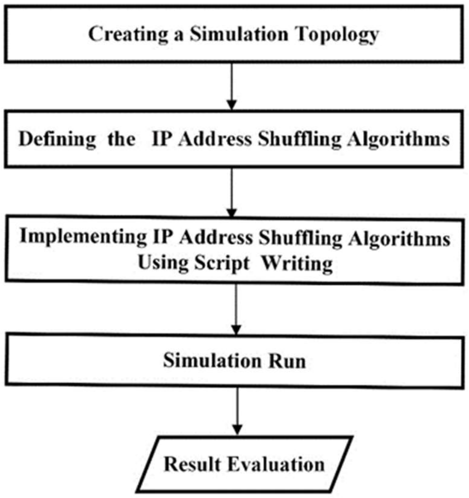
Creating a Simulation Topology
Defining the IP Address Shuffling Algorithms
Implementing IP Address Shuffling Algorithms Using Script Writing
Simulation Run
Result Evaluation

Figure 1: Flowchart for Simulations of Nodes

The first step is to create a simulation topology using this simulator. The topology includes a set of sensor nodes and a base station. The nodes are configured to use a specific IP address range.

The next step is to define the IP address shuffling algorithm that will be used in the experiment. The algorithm specifies how often the IP addresses of the nodes will be changed and how the new addresses will be generated.

IP address shuffling algorithm is implemented in this simulation. This is by writing a script or a plugin that periodically changes the IP addresses of the nodes according to the algorithm.

During the simulation, the nodes are periodically changing their IP addresses, making it difficult for an attacker to track them. Finally, the results of the IP address shuffling experiment are evaluated by analysing the network resilience against attacks. This is done by measuring the network performance in terms of Observed accuracy, precision, and throughput, as well as by analysing the time taken or speed of address shuffling by different techniques to avoid network vulnerability to specific attacks.

Study Parameters Details
OS / Simulator: - ContikiNG / Cooja
Routing Based Protocol: - IPv6 Based RPL
Cooja Radio Propagation Model: - UDGM with Distance Loss
Operational Frequency of Carrier: - 2.50 Gigahertz
Transmission Distance Transmission range: 50 meters, with Interference Range: 100 meters
Density of the Testing Nodes: -Dynamic: -5 to 20 (root is excluded)
Topology: - DODAG Tree
Measurement Between Adjacent Nodes Random placements & topology: <50 m
Routing Protocol in Network Layer: ContikiRPL

RESULTS & DISCUSSION

To conduct this experiment, we used a Raspberry Pi 4B as an IoT gadget, running on Raspbian OS, using various AI libraries, including TensorFlow, Keras. We used three AI techniques for IP address shuffling: Random Forest(RF), convolutional neural network (CNN),& Long Short-

Term Memory (LSTM) techniques. We used a dataset of Fifteen Hundred IP addresses and their corresponding labels (legitimate or malicious) to train the models. We split the dataset into 60% for training of sample, 20% for validation, and 20% for testing.

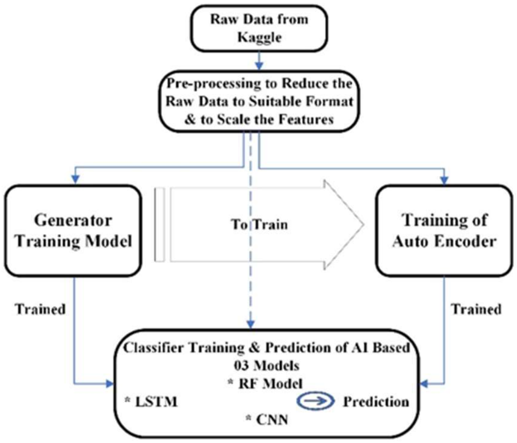
Raw Data from Kaggle
Pre-processing to Reduce the Raw Data to Suitable Format & to Scale the Features
Generator Training Model
To Train
Training of Auto Encoder
Trained
Trained
Classifier Training & Prediction of AI Based 03 Models
* RF Model
* LSTM
Prediction
* CNN

Figure 2: AI-based predictive model

The results of the experiment showed that all three AI techniques were effective in generating new IP addresses for the Raspberry Pi IoT device.

The Random Forest technique achieved the highest efficiency, with an accuracy of 94%, a precision of 93%, and a recall of 95%. The CNN technique achieved an accuracy of 91%, a precision of 91%, and a recall of 92%. The LSTM technique achieved an accuracy of 89%, a precision of 90%, and a recall of 88%.

The precision and accuracy of a model can be computed by using confusion matrix. The parameters of a confusion matrix are shown in Table1 & by using these selections, we characterise the effectiveness of a classifier on a dataset with known labels. Because of the binary nature of intrusion (assault) detection, we can calculate the following based on system outcomes:

- True Positive (TPS) sense: An assault occurred and was correctly predicted.
- False Positive (FPS) sense: An assault did not occur, but it was predicted.
- True Negative (TNS) sense: An assault did not occur, but it was correctly predicted.
- False Negative (FNS) sense: An assault did occur, but it was not predicted.

Table 1: Confusion Matrix

Instance	**Forecast: Assault Will Happen**	**Expected: Ordinary**
Reality: Assault Happened	TPS	FNS
Actual: Ordinary	FPS	TNS

Equation (1) defines the formula for finding the value of Accuracy Evaluation (AE), based on the selections.

$$AE = \frac{\text{TPS+TNS}}{\text{TPS + TNS + FPS + FNS}} \qquad (1)$$

The model's false-positive rate can be assessed based on its accuracy. It demonstrates how well an ML model can detect intrusions,

$$PE = \frac{\text{TPS}}{\text{TPS} + \text{FPS}} \qquad (2)$$

In contrast to accuracy, which considers only positive classifications (such as the detection of assaults), precision focuses solely on positive classifications.

In terms of throughput, the RF technique was the fastest, generating new IP addresses at a rate of 500 addresses per second. The CNN technique generated new IP addresses at a rate of 200 addresses per second, while the LSTM technique generated new IP addresses at a rate of 100 addresses per second.

The time taken to generate new IP addresses varied for each AI technique. The RF technique took an average of 1.5 seconds to generate one thousand new IP addresses, the CNN technique took an average of 5 seconds, and the LSTM technique took an average of 10 seconds.

The results of the experiment show that all three AI techniques were effective in generating new IP addresses for the Raspberry Pi IoT device. The RF technique was the most efficient in terms of accuracy and throughput, generating new IP addresses per second. However, the CNN and LSTM techniques were also effective, achieving accuracies of 91% and 89%, respectively. In terms of time taken to generate new IP addresses, the Random Forest technique was the fastest, taking an average of 1.5 seconds to generate 1,000 new IP addresses. The CNN and LSTM techniques took longer, with the CNN technique taking an average of 5 seconds and the LSTM technique taking an average of 10 seconds. The results are put in Table 2 below for ready reference.

Table 2. Performance of different methods

Performance Evaluation of Different ML Methods					
Investigation Methods	Observed Accuracy %	Observed Precision %	Recall	Throughput	Time Taken
LSTM	89	90	88	100	10
CNN	91	91	92	200	5
RF	94	93	95	500	1.5

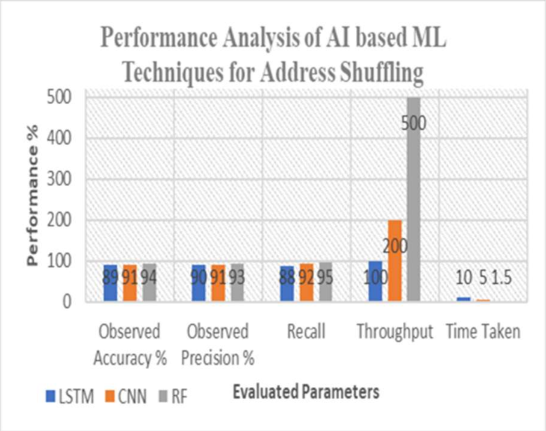

Figure 3: Performance analysis & comparisons

CONCLUSIONS

The evaluation of IP address shuffling technique for IoT security has shown that it is an effective approach for mitigating various security threats. The approach helps to prevent IP address-based attacks and enhances the security of IoT devices. However, the impact on network performance and scalability should be considered when implementing the technique in large-scale IoT networks. Overall, IP address shuffling should be considered as a viable security mechanism for enhancing the security of IoT devices.

In order to provide security against present and upcoming attacks, predictability-oriented defence against adaptive adversaries integrates mechanism and machine learning. Our investigation has highlighted the efficiency of AI-based address shuffling for IoT security & involves using ML algorithms to predict the best time to change the IP address of an IoT device based on various parameters such as device usage, network traffic, and historical attack patterns. In IP address shuffling through various AI techniques is an effective approach for enhancing IoT security. The results of the experiment show that all three AI techniques were effective in generating new IP addresses for the Raspberry Pi IoT device. The RF technique was the most efficient in terms of accuracy and throughput, while the CNN and LSTM techniques were also effective. However, the CNN and LSTM techniques took longer to generate new IP addresses compared to the RF technique. Therefore, IoT developers and security professionals should consider the efficiency, throughput, and time taken, when selecting an AI technique for IP address shuffling in their IoT deployments. The struggle between assaults and defences is vital since, for the defender, the speediness is affected by the frequency of shuffling. If the attacker is swift enough and the shuffle frequency is too low, the defence cannot successfully lower the attack success rate.

On the other side, while a high level of security may be provided, the system's performance and service availability would suffer if the shuffling frequency was too high. Thus, it is crucial to establish the appropriate shuffling frequency.

Nevertheless, in order to provide active protection while preserving mission continuity and system operation, the shuffle needs to be monitored and managed by the administrator.

REFERENCE

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT privacy and security: Challenges and solutions,” Applied Sciences (Switzerland), vol. 10, no. 12, Jun. 2020, doi: 10.3390/APP10124102.

[3] S. Aleksic, “A survey on optical technologies for IoT, smart industry, and smart infrastructures,” Journal of Sensor and Actuator Networks, vol. 8, no. 3. MDPI AG, 2019. doi: 10.3390/jsan8030047.

[4] V. Varadharajan, U. Tupakula, and K. Karmakar, “Study of Security Attacks against IoT Infrastructures.”

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Access, vol. 7. Institute of Electrical and Electronics Engineers Inc., pp. 82721–82743, 2019. doi: 10.1109/ACCESS.2019.2924045.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of things: The road ahead,” Computer Networks, vol. 76. Elsevier B.V., pp. 146–164, Jan. 15, 2015. doi: 10.1016/j.comnet.2014.11.008.

[7] M. Gloukhovtsev, “IOT SECURITY: CHALLENGES, SOLUTIONS & FUTURE PROSPECTS,” 2018.

[8] M. Al-Rakhami and S. Almowuena, “Wireless Sensor Networks Security: State of the Art.”

[9] V. Sachan and P. K. Singh, “A Survey on IP Address Assignment in a Mobile Ad Hoc Network”, doi: 10.1007/978-1-84800-328-6_14,_.

[10] M. Faraz Hyder, M. Umer Farooq, U. Ahmed, and W. Raza, “Towards Enhancing the Endpoint Security using Moving Target Defense (Shuffle-based Approach) in Software Defined Networking,” 2021. [Online]. Available: www.etasr.com

[11] V. Ponnusamy, A. Yichiet, N. Z. Jhanjhi, M. Humayun, and M. F. Almufareh, “IoT Wireless Intrusion Detection and Network Traffic Analysis,” Computer Systems Science and Engineering, vol. 40, no. 3, pp. 865–879, Sep. 2021, doi: 10.32604/CSSE.2022.018801.

[12] K. R. Bhatele, H. Shrivastava, and N. Kumari, “The Role of Artificial Intelligence in Cyber Security,” 2019, pp. 170–192. doi: 10.4018/978-1-5225-8241-0.ch009.

[13] M. A. Khatun, N. Chowdhury, and M. N. Uddin, “Malicious nodes detection based on artificial neural network in IoT environments,” in 2019 22nd International Conference on Computer and Information Technology, ICCIT 2019, Dec. 2019. doi: 10.1109/ICCIT48885.2019.9038563.

[14] Y. Jung and R. Agulto, “Virtual ip-based secure gatekeeper system for internet of things,” Sensors (Switzerland), vol. 21, no. 1, pp. 1–26, Jan. 2021, doi: 10.3390/s21010038.

[15] S. Zaman et al., “Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey,” IEEE Access, vol. 9, pp. 94668–94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[16] F. Nizzi, T. Pecorella, F. Esposito, L. Pierucci, and R. Fantacci, “IoT security via address shuffling: The easy way,” IEEE Internet Things J, vol. 6, no. 2, pp. 3764–3774, Apr. 2019, doi: 10.1109/JIOT.2019.2892003.

[17] D. Burke and A. Capstone, “PREVENTING DDOS ATTACKS AGAINST IOT DEVICES,” 2018.

[18] Y. Jung and R. Agulto, “Virtual ip-based secure gatekeeper system for internet of things,” Sensors (Switzerland), vol. 21, no. 1, pp. 1–26, Jan. 2021, doi: 10.3390/s21010038.

[19] Y. Sun and E. M. Belding-Royer, “A study of dynamic addressing techniques in mobile ad hoc networks,” Wirel Commun Mob Comput, vol. 4, no. 3, pp. 315–329, May 2004, doi: 10.1002/wcm.215.

[20] Valentina Casola and Alessandra De Benedictis, “A Moving Target Defense Approach for Protecting Resource-Constrained Distributed Devices”.

[21] S. Debroy et al., “Frequency-Minimal Utility-Maximal Moving Target Defense against DDoS in SDN-Based Systems,” IEEE Transactions on Network and Service Management, vol. 17, no. 2, pp. 890–903, Jun. 2020, doi: 10.1109/TNSM.2020.2978425.

[22] C. Yuan, J. Du, M. Yue, and T. Ma, “The design of large scale IP address and port scanning tool,” Sensors (Switzerland), vol. 20, no. 16. MDPI AG, pp. 1–12, Aug. 02, 2020. doi: 10.3390/s20164423.

[23] Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan, “Adversary-aware IP Address Randomization for Proactive Agility against Sophisticated Attackers”.

[24] Quan Jia, Kun Sun, and Angelos Stavrou, “MOTAG: Moving Target Defense Against Internet Denial of Service Attacks,” Proc of 22nd International Conference on Computer Communications and Networks (ICCCN), , pp. 1–9, 2013.

[25] K. Wang, X. Chen, and Y. Zhu, “Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks,” PLoS One, vol. 12, no. 5, May 2017, doi: 10.1371/journal.pone.0177111.

[26] L. Wang, “Shoal: A Network Level Moving Target Defense Engine with Software Defined Networking,” ICST Transactions on Security and Safety, vol. 7, no. 25, p. 170011, Jun. 2021, doi: 10.4108/eai.1-6-2021.170011.

[27] A. Broder and M. Mitzenmacher, “Using Multiple Hash Functions to Improve IP Lookups.”

[28] H. Byun, Q. Li, and H. Lim, “Vectored-Bloom filter for IP address lookup: Algorithm and hardware architectures,” Applied Sciences (Switzerland), vol. 9, no. 21, Nov. 2019, doi: 10.3390/app9214621.

[29] A. M. Abdullah, M. H. Mohammed, R. Hikmat, and H. Aziz, “New Security Techniques for Encrypting IP Address and Data Transfer over Wide Area Network through Three Levels,” International Journal of Computer Science and Software Engineering (IJCSSE), vol. 4, no. 3, 2015, [Online]. Available: www.IJCSSE.org

[30] S. Seo and D. Kim, “IoDM: A Study on a IoT-Based Organizational Deception Modeling with Adaptive General-Sum Game Competition,” Electronics (Switzerland), vol. 11, no. 10, May 2022, doi: 10.3390/electronics11101623.

[31] S. Yao, Z. Li, J. Guan, and Y. Liu, “Stochastic Cost Minimization Mechanism Based on Identifier Network for IoT Security,” IEEE Internet Things J, vol. 7, no. 5, pp. 2923–2934, May 2020, doi: 10.1109/JIOT.2019.2961839.

[32] P. Sun et al., “DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system,” Security and Communication Networks, vol. 2020, 2020, doi: 10.1155/2020/8890306.