I.J. Wireless and Microwave Technologies, **2024, 2, 1-16**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.02.01

A Novel Framework for Real-Time IP Reputation Validation Using Artificial Intelligence

NW Chanaka Lasantha
IIC University of Technology, Faculty of Graduate Studies, Phnom Penh 121206, Cambodia
E-mail: chanaka.lasantha@gmail.com
ORCID iD: https://orcid.org//0009-0006-3226-7713

Ruvan Abeysekara
IIC University of Technology, Faculty of Graduate Studies, Phnom Penh 121206, Cambodia
E-mail: ruvan@iic.edu.kh
ORCID iD: https://orcid.org//0009-0007-2663-3497

MWP Maduranga*
Department of Computer Engineering, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka
E-mail: pasanwellalage@kdu.ac.lk
ORCID iD: https://orcid.org//0000-0002-0053-4999
*Corresponding author

Received: 13 November, 2023; Revised: 15 December, 2023; Accepted: 13 March, 2024; Published: 08 April, 2024

Abstract: This research paper introduces and discusses deeply an approach to the real-time IP reputation (IPR) concept and its validation process for an Amazon Web Services Web Application Firewall (AWS WAF) backend application safeguarding using intelligence (AI) technologies. Also, the study examines existing IP reputation solutions over AWS WAF which Evaluates methodologies highlighting the difficulties faced and real-world challenges in validating IPR while utilizing OpenAI's generative AI language models the framework aims to automate the extraction and interpretation of IP-related information from AWS S3 real-time log storage sources such as logs, and natural language reports based on JSON structure. These dedicated algorithms developed, and AI model concepts are powered by processing language enabling them to identify incidents and detect patterns of IP behavior that should indicate security risks. Also, models do not directly access databases, as they can analyze data from APIs featured and with local maintenance database such that AbuseIPDB to evaluate the reputation of IP addresses Integrating AI into the process of validating IPs can greatly improve cybersecurity operations by summarizing findings and providing insights ultimately saving time and resources.

Index Terms: Real-time IP Reputation, AWS WAF Security, AI-powered IP Validation, OpenAI Language Models, Cybersecurity Automation.

1. Introduction

Ensuring the validation and credibility of an IP address is crucial for maintaining network security and preventing misuse. It involves assessing the activities and behaviour of an IP address to determine its reputation. If an IP address has been involved in spamming, hosting malware participating in botnets or carrying out cyberattacks its integrity can be compromised. By validating IP reputations organizations can effectively safeguard both their cloud and on-premises networks by limiting access from sources and ensuring the proper utilization of resources [1]. Typically includes checking the IP address against databases and blacklists that keep track of known IP addresses. It's important to keep an eye on the IP reputation (IPR) because it can indicate if there is a possibility of activity or compromise, by threat actors. By monitoring IPR organizations can take measures and precautions to either block or thoroughly investigate traffic from sources before any harm occurs. This helps prevent access, reducing the chances of cyberattacks and protecting data [2]. OpenAIs language models have the potential to enhance IPR analysis capability by automating the extraction and interpretation of information related to IPs from sources such as logs and natural language reports. These models can understand language enabling them to process reports identify incidents and detect patterns or abnormalities, in IP behavior that could indicate threats, while these models cannot directly access databases, they can analyze outputs from

APIs such as AbuseIPDB, which provides data on the IPR of IP addresses [3]. They can also help refine and improve cybersecurity reports by summarizing findings and offering recommendations. By incorporating these AI capabilities into the IPR validation process organizations can streamline their analysis. Save time and resources [4,5]. Additionally, the ML features of these AI models allow them to continuously learn and adapt to activity patterns. The goal of the project is to manage and update lists of IP addresses for protection against hackers [6]. It achieves this by retrieving and analyzing logs from an AWS WAF to verify the IP addresses also by combining the Abuse IP database with Generative AI the project aims to automate the validation process for determining IPR while promptly sending email notifications to report and block attackers, this system has been designed specifically for AWS accounts with options for storing logs [7]. The objectives include maintaining sets of IPs in AWS WAF identifying security threats, from WAF logs and ensuring accurate validation of IPR through advanced abuse detection methods [8]. Also, the objective of this research work is to streamline the process of generating real-time updates, for IPR lists and reporting. The focus is on using AWS WAF as a platform to efficiently fetch logs from S3 object storage buckets across multiple accounts to provide accurate and efficient Bad IP address prevention against form anonymous hacker attempts as well [9].

2. Background of Study

2.1 The Concept of IP Reputation and Its Significance in Cybersecurity

The concept of IPR plays a role in cybersecurity and it refers to the level of trustworthiness associated with an Internet Protocol (IP) address based on its behaviour score determines trust, an IP reputation score helps determine the likelihood of an IP address being involved in malicious activities. Cybersecurity systems rely on this score to make decisions about permitting or blocking traffic from IPs also in Negative IP reputations can arise from activities such as spamming, participating in Distributed Denial of Service (DDoS) attacks, hosting content or being part of botnets [10]. Understanding the significance of IPR lies in protecting networks and services from these activities. An IP address, with a reputation poses a security risk. By monitoring and assessing the reputation of IP addresses organizations can proactively block threats at the network periphery thus reducing risks to systems and safeguarding sensitive data [11].

2.2 Overview of The Existing Methods and Challenges in IP Reputation Validation

The traditional method of validating IPR involves checking an IP address, against databases and real-time blacklists that contain records of IPs. These lists are created using techniques such as honeypots and spam traps and reports of behaviour, Reputation scores are then assigned based on the behaviour of the IP while introducing lots of challenges such as IP reputations can quickly become outdated [12]. Real-time updates are essential to stay out of cyber threats [13], False positives and negatives can occur, resulting in legitimate traffic being blocked or malicious traffic being allowed, as organizations grow, managing and validating several IP addresses can become overwhelming, consolidating data from sources into a cohesive reputation system can be complex and resource intensive [14].

2.3 Overview of The Existing Methods and Challenges in IP Reputation Validation

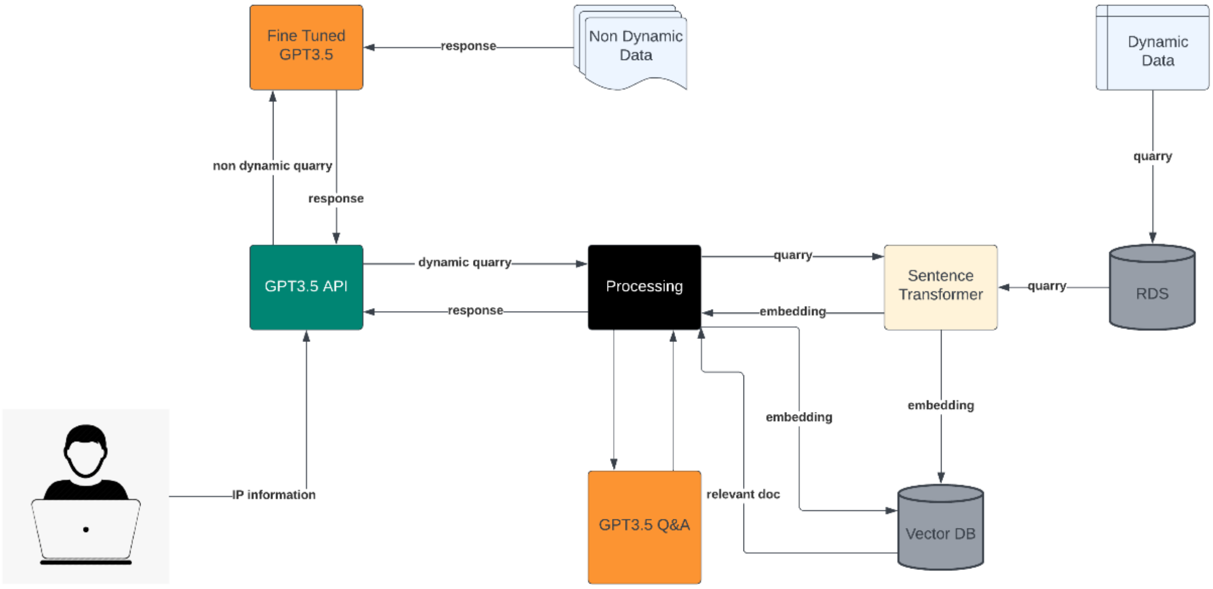


Fig. 1. Basic OpenAI Test Analysis approach.

The above Fig. 1 shows, that the OpenAI models can automate the analysis of log files detect patterns that should indicate activity and even predict threats by using historical data while it’s integrated into cybersecurity workflows OpenAI capabilities can lead to improvements, in areas specialized by OpenAI, that can understand and generate text-to-human language [15]. Also, This allows them to process and analyze amounts of data for enhancing the process of IPR management detail fetching by automating the analysis of IP-related data that can quickly identify threats, and with algorithms, false positives and negatives can be reduced [16], The AI models continuously learn from data to stay ahead of evolving cyber threats [17], Comprehensive and user-friendly reports are generated to assist decision making with supporting the combination of OpenAIs language models with real-time threat intelligence organizations can strengthen their cybersecurity defences [18].

3. Existing IP Reputation Validation Architectures

3.1 Preventing IP Address Targeted Attacks

One of the hardest things about cybersecurity is tracking and stopping cyber-attacks at the IP address levels which was solved by one of researched blacklists and tools such as Automated IP Reputation Analyzer Tool (AIPRA), which combined Machine Learning (ML) with geolocation data to figure out what's not relevant for regions and countries in usual working time range of humans. But problems such as false positives, and maintenance of the fast-changing nature of its enemy continue to an accurate validation process. The challenges of existing methods, in cybersecurity, to prevent attacks through domains and IP addresses and it discusses approaches such that blacklists which are essentially databases of known threats and the AIPRA which enhances this by cross-referencing multiple blacklists and incorporating a weighted security measure by highlighting the application of machine learning techniques including incorporating geolocation data to improve the identification of entities to get easy attack vector classification. It also raises challenges such as the risk of positives, where legitimate domains are mistakenly flagged as threats the need for regular maintenance and updates to blacklists and the difficulties posed by rapidly emerging malicious domains and changing IP addresses that can evade detection. Furthermore, it acknowledges inconsistencies among blacklist databases and the considerable training time required for machine learning models due to datasets. Apart from that, OpenAI expertise in machine learning can have an impact on the advancement of systems such as AIPRA By involving cutting-edge algorithms and robust data processing capabilities OpenAI can assist in refining these models to achieve accuracy, in classifying IP addresses minimizing instances of positive and constantly adapting to emerging cyber threats [19].

ML can help AIPRA systems immensely while cutting-edge algorithms and effective data processing, combined with the optimization of models which increase accuracy while reducing false positives, keep it up to speed on new threats. This strengthens cybersecurity defences on IPR, while the security of the LAN The MAC and IP addresses, computer names, IP conflicts and MAC mismatches are most important to reduce attacks from bad IPR vectors in securing network traffic and assets and spoofing risk over digital infrastructure. Such that, the spoofers forge these identifiers to masquerade as IPR validation systems. MAC and IP addresses, computer names, and the phenomena of IP conflicts and MAC mismatches are integral to understanding the intricacies of LAN security while the act of spoofing, where an attacker masquerades as a legitimate user by falsifying these identifiers, poses a formidable challenge to IPR validation systems. Traditional security infrastructures often falter in the face of such sophisticated attacks, underscoring the necessity for more robust and adaptive security solutions. Additionally, the capabilities of OpenAI's AI models emerge as a beacon of potential. With advanced machine learning algorithms, these models could revolutionize anomaly detection, automate network traffic monitoring, and conduct comprehensive data analyses. Such AI-driven systems promise not only to detect but also to predict and adapt to emerging threats in real-time, thereby fortifying the integrity of IPR validation processes [20].

3.2 Traditional Bot Traffic Tracking Techniques.

The applications of Residential IP Proxy (RESIP) facilities are becoming more and more popular cases of web scraping and other criminal actions such as relocating behind the reserves of residential IPs where the detection is prevented. Two additional datasets indicate the functioning of RESIP where its figures are highlighted only with the four providers but not with differences concerning them. They suggested an operational scheme that can automatically compare accounts with shared characteristics. Besides, overall, five campuses undertook vulnerable RESIPs' investigation, showing attacked hosts and unlawful acts. This study can shed light on and address the security chances that this growing sector is attributed to. RESIPs, which are a new grey-area business, provide a shield from scrutiny by using other people’s computers in their homes to complain about illegalness and recruitment ways. Also, it proposes RETRO detection, a technique that captures the sequences of flows using a compromised device, raising the operational opacity of these services. While it optimizes a server-side detection method for RESIP connections, dropping false negative outcomes that result from mobile proxies.

Web scraping bots that hide behind Residential IP Proxy services are causing difficulties, for BOT measures and, also, are the advanced bots pretending to be traffic by using the IP addresses of individuals making it challenging to detect and block them without accidentally blocking legitimate users. Traditional IP reputation systems struggle to differentiate between customers and bots that exploit services to address this issue OpenAIs advanced AI models can play a role in developing cutting-edge detection strategies while utilizing ML to analyze network traffic patterns AI can identify behaviors that are characteristic of proxy-driven bot traffic. OpenAI models excel at detecting irregularities that may indicate the use of services from clean IP addresses. OpenAIs expertise in Natural Language Processing (NLP) allows them to gather information from sources and use it to uncover emerging threats and improve detection algorithms. These capabilities could greatly contribute to the development of systems that can distinguish between proxy bot traffic and genuine user interactions thereby strengthening the validation processes, for IPR [21].

The incorporation of OpenAIs AI models, into IPR systems has the potential to greatly enhance cybersecurity measures and utilize ML techniques such that pattern recognition and anomaly detection OpenAIs capabilities can effectively navigate the changing landscape of cyber threats. The mentioned research emphasizes the importance of IPR in assessing risks and, also Presents a system that uses cross-protocol analysis to distinguish between malicious and harmless IP addresses during OpenAI models, those handling large network datasets can play a crucial role in improving this system by providing real-time updates on IPR thus keeping up with the agile nature of cyber threats. Furthermore, employing GPT models to analyze data could offer predictive insights into security vulnerabilities. Additionally, this collaborative approach has the potential to address challenges such as the evolution of malicious tactics and complexities associated with data collection for IPR [22].

3.3 NLP for Enhanced Threat Detection Using ML

The growing trend of IoT-devices interconnectedness has resulted in an uptick in intrusions. IDS or IPS systems are a type of security solution that monitors and detects system violations [23]. Nonetheless, a holistic synchronousness in new developments and model limitations means that a new security framework is required. On the part of this survey AI techniques such as machine learning and deep learning seem as most relevant solution with hybrid design efficient intrusion detection/prevention emphasizing. It considers their viability, setbacks, and real-time issues. Securing IoT, ML and big data analytics have profound effects on it. This is where they come in. This investigates IoT vulnerabilities, uses ML for cyber-vulnerability assessment, and analyzes ML-based intrusion detection solutions [24]. It provides an example of a real-world testbed which is used for the design of IDS, demonstrating that Machine Learning is capable of intrusion detection in computer networks [25]. However, this study the literature on the topic of anomaly-based intrusion detection systems driven by ML/DL, pushing the boundaries to unleash the full potential of ML-based AI systems, examining open issues, and proposing evaluation benchmarks. This interactive synopsis suggests a method to enhance intruders' detection systems efficiency [26].

The limitations of traditional methods, such as blacklists and intrusion detection systems (IDS). It emphasizes that blacklists struggle to keep up with evolving cyber threats signature-based IDS struggle to detect attacks and anomaly-based IDS often produce false positives. Additionally, the dynamic nature of cyber threats and the complex obfuscation techniques employed by actors make IPR validation challenging. ML-driven approach that leverages the stability of IP addresses compared to URLs or domain names. By incorporating OpenAIs AI capabilities in machine learning, anomaly detection and NLP this proposed system aims to enhance detection precision and reduce positives. OpenAIs models, trained on datasets can identify patterns indicative of malicious activity. Furthermore, using learning for anomaly detection can uncover unrecognized potential threats while NLP techniques can provide nuanced insights, from data sources to enrich IPR analysis [27].

3.4 The BlackEye IPR Framework

Algorithms Blacklisting malicious IP addresses is an essential tool for IT systems' protection. The decision-making is based on looking at packet traffic data and the behavioural history of users. Still, the holding of domain experts for blacklisting is on but ML is on the way and just awakes to maturity. This is solved by making the BlackEye framework based on which the different ML methods are used accordingly to achieve superior results. The analysis shows that the multistage method, which is achieved by data cleansing and classification with logistic regression or random forest, leads to the best results. Real-world data evidenced a near-90% less incorrect blacklisting compared to the expert performance. By the same token, our model accelerates the time-to-blacklist, significantly cutting the lifetime of malicious IP addresses on average by 27 days. It can be considered a breakthrough in the process of protecting the IT system concerning blacklisting and redesigning the efficiency and accuracy of the system security [28].

4. Case Studies and Real-World Examples

In Table 1, the discussion of real-world data fields in artificial intelligence and cybersecurity. The listing also shows information like names of authors, publication year, study title, the exact page where the study was published, the summary of the main results, which technologies or methods were used and some who additional comments or remarks were made. The initial piece of writing talks about a 2021 research work, Usman et al., 'Intelligent Dynamic Malware Detection using Machine Learning' which was published in journal, 'Future Generation Computer Systems'.Comput.Syst.".

Table 1. Case Studies for IP Reputation Validation

Authors	Year	Title	Publication	Pages No.	Contribution	Technology	Remarks
Usman, N., Usman, S., Khan, F., Jan, M., Sajid, A., Alazab, M., Watters, P.	2021	Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics	Future Gener. Comput. Syst.	118, 124-141	Proposes a hybrid approach combining Dynamic Malware Analysis, Cyber Threat Intelligence, ML, and Data Forensics for predicting IP reputation in pre-acceptance stage.	Machine Learning, Big Data Forensics, Cyber Threat Intelligence	Addresses challenges of high management cost and false positives in traditional reputation systems.
Sainani, H., Namayanja, J., Sharma, G., Misal, V., Janeja, V.	2020	IP Reputation Scoring with Geo-Contextual Feature Augmentation	ACM Transactions on Management Information Systems (TMIS)	11, 1-29	Introduces a model for IP reputation scoring that includes geo-contextual information for a more comprehensive threat assessment.	Geo-Contextual Feature Augmentation, Anomaly Detection Model	Empirical evidence suggests combining network and geo-contextual information enhances threat assessment.

The study offers a mix of Dynamic Malware Analysis and Machine Learning with Machine Learning and Big Data Investigations as technical capabilities to detect the threat. The respondents zone encompasses a comment on the overcoming of obstacles, which include but are not limited to high management costs and the modern cyber threats. Every row on the table corresponds to one case study that describes artificially intelligent techniques elaborately along with their methods to reinforce cybersecurity.

In Table 1 being displayed in Table 1 and include such aspects as authors, year of publishing, title of the study, and the name of the journal or conference to feature. For example, the initial entry of Usman and other in 2021, titled "Dynamic malware detection via machine learning," that was published in "Future Generation Computer Systems" is where they explore dynamic malware detection using machine learning. Such detailed mattering’s not only denote the transition and the development of the area of AI-driven cybersecurity, but also give you an overview of the team that is working in different disciplines to develop the cybersecurity research The precise citation of the particular page number is contributing to this and addresses the issue of the location of such studies in their publications.

The "Contribution," "Technology" and "Remarks" columns are the most important in the table. Thus, these pages elucidate the core of the research, briefly describing the main findings, the specific tools and methods employed, and provide additional information to improve the understanding of the effects of the research findings. For instance, the initial investigation brings together a dynamic malware portrayal with machine learning to avoid high running management costs and processing power difficulties in data packet detection. This form of blending captures the inherent problem-solving nature of these cybersecurity experts while tackling complex cybersecurity challenges. Through the investigation of these three main features, the table not only provides current research trends understanding but also suggests the future trend of AI application in cybersecurity area highlighting the fact that the invention must be continuously developed, and the interdisciplinary collaboration has to be maintained in this fast-changing field study.

5. Capabilities and Limitations

5.1 IPR Validation and Prevention Using ML

A list of malignant IP addresses must be compiled to prevent informational systems from being infected. This is the case now due to high reliance on human factors. The recent development has provided an answer to this picture through BlackEye's machine learning capacity. According to research, the steps of data refinement and division result in improving the list of blacklisting by logistic regression or Random Forest that brings the ratio of undesired blacklist down to 15%. Besides, the reason why Ridge regression is used to clean up data to increase the accuracy by 5% is also evident. BlackEye performs autological learning on any log type, above all increasing the preciseness of match and narrowing down the blacklisting process. The remaining tasks in the given process are performing deep learning for such purposes [29].

5.2 IPR Validation of Public Databases using ML

The mere fact that a blacklist has some efficiency is not enough to not consider its weak sides, for instance, false positives and out-of-date data. One of the reasons for the development of AIPRA is to overcome these issues. The application tool, in turn, finds out what is known about domains and IP addresses, by checking the domains for several of the most common indexes. Following this, the AIPRA assigns the weights to the probability of misconduct that is linked to the URLs, for instance. Moreover, an area involving a geolocation-based machine learning algorithm has been added as a part of the AIPRA superpower, which expands its ability to highlight hazards. It has been found through our research that there is NO AIPRA name on the public blacklists lists at all [30].

Table 2. Review Table

Work	Source	Author	Pages	Contribution	Technology	Remarks
Automatic IP Blacklisting Using Machine Learning from Security Logs.	Journal Article	D. Jeon and B. Tak	p937-948	an automated IP blacklisting framework using machine learning techniques.	Logistic regression and random forest Machine learning, logistic regression, random forest.	Significant reduction in incorrect blacklisting and reduced activity period of malicious IPs and Machine learning models can approach the accuracy of experienced agents, reducing reliance on human judgement.
IP Reputation Analysis of Public Databases and Machine Learning Techniques.	Journal Article	J. L. Lewis, G. F. Tambaliuc, H. S. Narman, and W. S. Yoo,	p181-186	Development of the Automated IP Reputation Analyzer Tool, which cross-checks multiple blacklist databases and assigns security scores to domains and IPs.	Use of blacklist databases, possibly neural networks, decision trees, and logistic regression machine-learning techniques	Addresses issues with traditional blacklists, such as false positives and maintenance/updating challenges.
A New Local Area Network Attack through IP and MAC Address Spoofing.	Journal Article	S. Shaw and P. Choudhury	p347-350	a new attack method for gaining unauthorized internet access in a LAN by exploiting IP and MAC address spoofing.	Specific software tools for spoofing such as Advanced IP Scanner and MAC Address Changer.	Discusses motivations for spoofing attacks such as financial constraints and the need for higher bandwidth. The feasibility of the attack relies on knowledge of user IDs and default LAN ISP passwords.
Detect Malicious IP Addresses using Cross-Protocol Analysis	Journal Article	Y. Huang, J. Negrete, A. Wosotowsky et al.	p664-672	Development of a large-scale classification system using cross-protocol telemetry for IP reputation assessment.	Decision trees and random forests Machine learning models, cross-protocol telemetry, real-world IP reputation system.	Challenges include a lack of labeled data, the high cost of false positives, dynamic nature of IP reputation.
Detecting malicious websites by learning IP address features	Journal Article	D. Chiba, K. Tobe, T. Mori, and S. Goto	p29-39	Development of a machine learning-based detection scheme for web-based malware.	Supervised binary classifiers such as the logistic regression model, neural network, Naive Bayes classifier, and support vector machine.	Emphasizes the adaptability of attackers and the limitations of current detection methods.

5.3 MAC Address Spoofing LAN Attack Validation

LAN unit is challenged more in terms of the speed of transmission security and overall networking capabilities. It constitutes the fact that new threats find a specific way to keep the inmate in fear and be always observant. Thus, one of the methods of exploitation, put into practice by the doctors mostly and reversely acting as such users perfectly illegally, is their making a connection of their resources to the internet through the LAN with the help of avoidance of its security measures at all. A resolution could be the investigation of the case and if the offender is caught to face suiting up and finally be put behind bars or MAC Address changer/Advanced IP Scanner and the elimination of the culprit at the roots. Such as MAC addresses, which can be seen to be blocking external damages, and not exposing IP addresses, which can be used in avoiding any form of unauthorized access Two primary factors of the limited amount of money and time may be influenced by the forged attacks of the kinds that take place because of account IDs and default ISP passwords exploitation [31].

5.4 Detecting Malicious IP by Cross-Protocol Analysis

The trust reputation system is based on actual data that also arranges the ML to be comprehensive. The results are promising according to the strong relationship between browser extension and email service. The importance of the algorithms which make this phenomenon possible cannot be understated, and this makes adequate protection from malicious sites a top priority. For security the source code is obfuscated, and encrypted in the same common IP reputation key, across different providers; as well as pre-processing is done, and the feature combination is done in a new way. An understanding of such as False Positives and the false negatives issue follows from an analysis of errors and explainability as well. Besides figuring out the network IP data through port 53, it will be more efficient to take an incremental view of the model and tend toward making the model more flexible. Although they could overcome this disadvantage by fine-tuning large models on small amounts of data, there might be other issues prohibiting the labelling of low data. Another dilemma is the fact that the reputation of investors will be the same as audience patterns as they get older too [32].

5.5 Detection of malicious traffic by learning IP Reputation

Embracing flexible and scalable solutions in machine learning comprises their lightweight approach that does not change the existing methodologies. Using the list of IP addresses of unsolicited email attacks and traffic of campus network as input, the method of our study higher than other present approaches is further. Good sites are tagged as harmful and bad sites are tagged as malicious, yet the unknown ones are overlooked and therefore, the attacks carried out by these sites continue. Nevertheless, this convenience of harmless identification of such areas on the common hosting might, in turn, result in needed re-profiling to promote better results. While the intelligence agencies strive to gain the upper hand, it is the adaptability and constant evolution of the attackers that is the core challenge. Moreover, the defences are powerless in the hunt for the unknown [33].

6. Methodology

6.1 Methodology for IP Collection

Fig.2 IP Collection sections show that the process of gathering data involves collecting IP addresses from sources, including server logs, user reports and external threat intelligence feeds. Once collected an initial filtering step categorizes these IP addresses based on predefined criteria such as trusted, suspicious, or unknown to optimize resource usage for analysis a deduplication strategy ensures that each IP address is processed individually. The enrichment phase then enhances the IP addresses by adding contexts such as geolocation information, ASN details or historical behaviour to facilitate comprehensive evaluation while it is maintaining effectiveness over time regular updates and maintenance are necessary to incorporate entries and adjust the status of existing IPs in the database. Also, integration, with system components, is established to enable real-time updates and alerts for newly discovered or high-risk IP addresses creating a strong and responsive framework.

6.2 Methodology for Reputation Checking

Fig. 2 shows the process starts by checking IPR addresses against the AbuseIPDB API to gather up-to-date reputation data for analysis it has created a scoring algorithm that assigns reputation scores to the IPs considering both the seriousness and frequency of reported incidents to ensure accuracy and, it examines data for each IP address to identify patterns and changes in behaviour that might impact its reputation score to get and implement decision logic based on these scores to determine what steps should be taken next such as whether to escalate for investigation and activate automated defences while establishing a feedback loop that continuously improves the reputation-scoring process by learning from actions and decisions .

6.3 Methodology for Log Analysis

Fig. 2 shows the first step is to analyze the logs generated by AWS WAF and extract IP addresses and relevant metadata after that, we use algorithms to detect anomalies and identify patterns that may indicate security risks while correlating this data with IPR information, gaining a rounded understanding of threats. It also performs analysis to uncover emerging threats that may not be immediately apparent, ensuring a comprehensive view of security. This system generates reports as well as event-triggered reports providing actionable insights to security personnel for informed decision-making in the event of potential security incidents.

6.4 Methodology for Communication

Fig.2 Notification templates are carefully designed to be personalized for scenarios ensuring that the messages sent are easily understandable and prompt the required action while the system determines who should receive these notifications based on the seriousness of the alert and the roles of the recipients to protect these communications measures, such that encryption and authentication are put in place to ensure that the messages remain confidential and intact. The system is also designed with resilience and redundancy features so even if there are system failures

notifications will still be delivered without any issues. Additionally, automated response protocols are established to respond to alert types by taking immediate actions such as updating firewall rules and isolating compromised systems to enhance security without any delay.

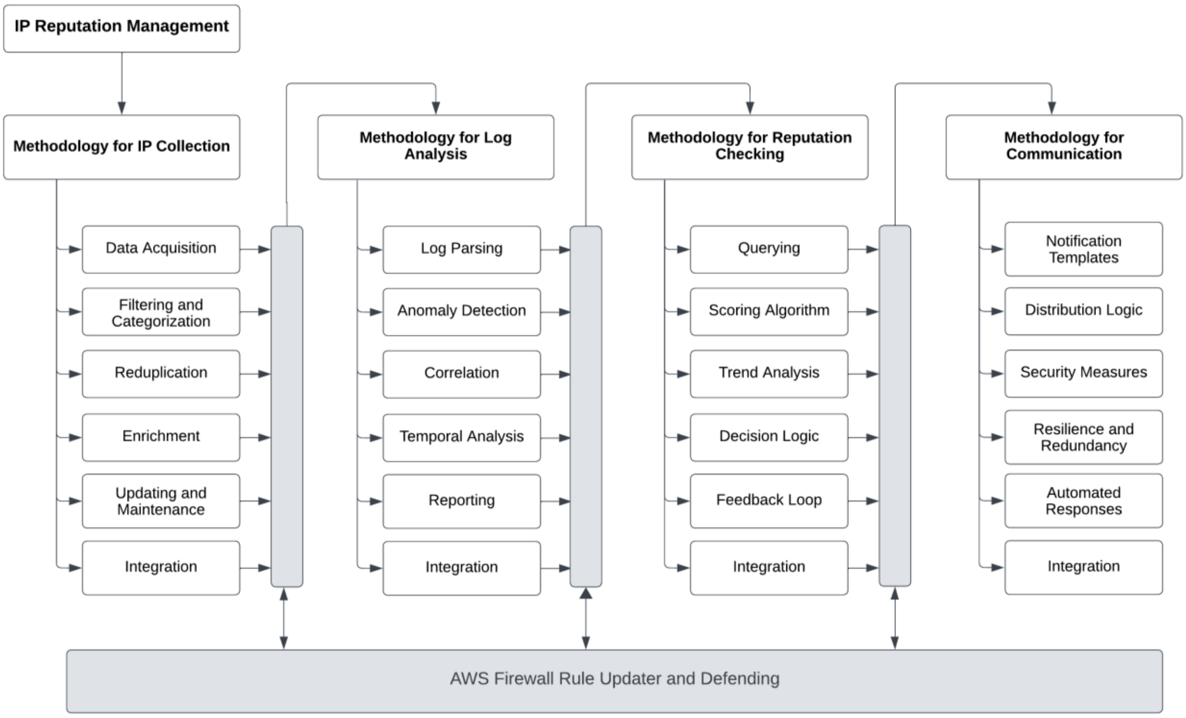


Fig. 2. Methodology

7. Algorithms Applied in the Solution

Incorporating the AI technology developed by OpenAI into the existing security algorithm brings a new level of potential which is started with the algorithm extracts configurations, helps in interpreting and understanding settings reducing errors and optimizing system setup while the secure retrieval of credentials through AWS Secrets Manager remains unchanged ensuring adherence to security practices. The next phase involves leveraging OpenAIs GPT for log analysis while the AI analyzes AWS WAF logs with an understanding of context enabling it to identify patterns and threats that might be missed by traditional rule-based systems. When it comes to interacting with the AbuseIPDB API, OpenAI models automate queries, assess responses, and refine the process of evaluating IPR addresses to give support and lead to an approach to managing threats. Additionally, AI generates human text to help transform data into actionable intelligence, making decision-making on IP blocking more efficient. The integration of AI also proves beneficial in error handling. By utilizing OpenAIs language models the system can diagnose issues, interpret error logs accurately and provide solutions for resolution. This proactive mechanism significantly reduces downtime. Improves system reliability. Furthermore, communication, within the algorithm is revolutionized through AI-generated email summaries by using terminology individuals receive clear and concise summaries of WAF activities that have been carefully crafted by GPT while improving the clarity and efficiency of security updates.

8. Experimental Setup

The IP Collecting module in the above Fig.3 explains that the IP Collection module plays a role in the IPR validation mechanism, and it gathers information from sources, such as network logs and external feeds to maintain an up-to-date list of IPs. These IPs are then categorized based on whether they belong to customers, internal systems or facing networks and while doing this targeted categorization the module ensures validation, removes any duplicate entries and to streamline the process further the module filters out known IPs [36]. Whitelisted ones before conducting reputation checks. This pre-filtering step makes subsequent checks easier and more effective, and the module also keeps a repository updated with the data acting as the system’s primary source of accurate information. Scheduled updates ensure that the module remains current and relevant. Additionally, its integration with systems allows for real-time response to threats and it enhances IP data by providing details such as geolocation information and historical behaviour patterns enabling analysis that is designed to handle large volumes of IPs efficiently the module is scalable and employs parallel processing techniques along with optimized data structures for optimal performance. The fault tolerance of this module is crucial for ensuring functionality within the IPR validation during outages or errors in data sources, it continues to operate.

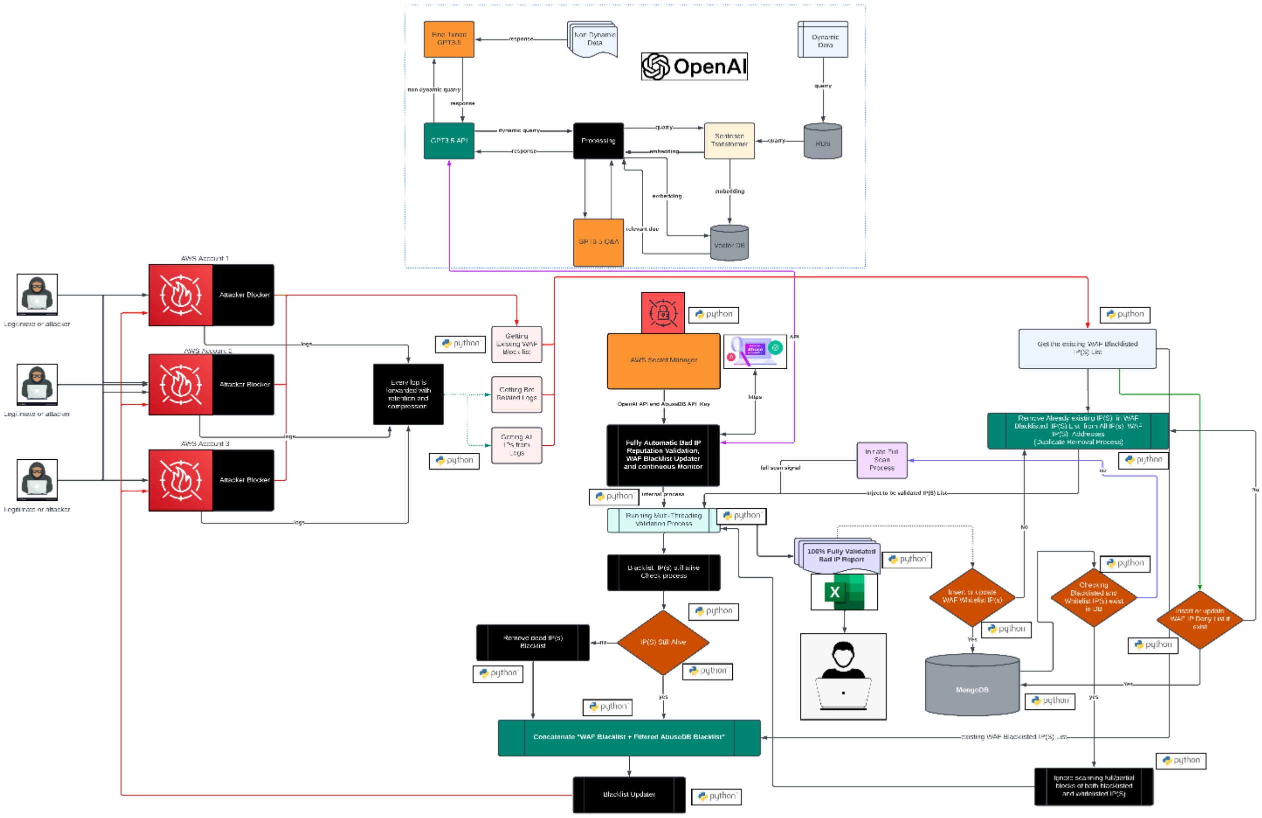

Fine Tuned GPT3.5
response
Non Dynamic Data
OpenAI
Dynamic Data
non dynamic query
response
query
GPT3.5 API
dynamic query
response
Processing
query
embedding
Sentence Transformer
query
RDS
embedding
embedding
relevant doc
GPT3.5 Q&A
Vector DB
AWS Account 1
AWS Account 2
AWS Account 3
Attacker Blocker
Attacker Blocker
Attacker Blocker
Legitimate or attacker
Legitimate or attacker
Legitimate or attacker
logs
logs
logs
Every log is forwarded with retention and compression
Getting Existing WAF Block list
Getting Bot Related Logs
Getting All IPs from Logs
AWS Secret Manager
API
https
OpenAI API and AbuseDB API Key
Fully Automatic Bad IP Reputation Validation, WAF Blacklist Updater and continuous Monitor
internal process
Running Multi-Threading Validation Process
Blacklist IP(s) still alive Check process
IP(S) Still Alive
no
Remove dead IP(s) Blacklist
yes
Concatenate "WAF Blacklist + Filtered AbuseDB Blacklist"
Blacklist Updater
Get the existing WAF Blacklisted IP(S) List
Remove Already existing IP(S) in WAF Blacklisted IP(S) List from All IP(s) WAF IP(S) Addresses (Duplicate Removal Process)
Initiate Full Scan Process
full scan signal
Inject to be validated IP(S) List
no
No
No
100% Fully Validated Bad IP Report
Insert or update WAF Whitelist IP(s)
Yes
Checking Blacklisted and Whitelist IP(s) exist in DB
Insert or update WAF IP Deny List if exist
Yes
yes
MongoDB
existing WAF Blacklisted IP(S) List
Ignore scanning full/partial blocks of both blacklisted and whitelisted IP(S)
python

Fig. 3. Experimental Setup

The IPR validation module is shown in Fig.3 shown, The Reputation Checking component, which is a part of the IPR validation framework connects with AbuseIPDB to evaluate the reliability of IP addresses by analyzing their reputation scores and historical data. It carries out queries, in bulk efficiently processing batches of IP addresses and retrieving abuse reports from AbuseIPDB. These reports provide information about the types and frequencies of incidents associated with each IP address. This valuable data allows for the assignment of nuanced IPR scores to IPs reflecting risks based on incidents. A sophisticated algorithm implemented in this component can distinguish the severity of incidents. It prioritizes offences such as DDoS attacks over ones such as spam and adjusts risk scores accordingly. These scores are customizable to align with an organization's risk profile while tracking the reputation of IPs over time. This component can identify patterns or trends that may indicate IP addresses turning malicious or undergoing rehabilitation. It interprets reputation data to make decisions, such as updating firewall rules or flagging IPs for review. The system continually evolves through a feedback loop process that learns from past decision outcomes to improve assessments. If a blocked IP address is found to be safe or an allowed IP address causes trouble this information helps recalibrate the scoring process. The module has been designed while considering AbuseIPDBs API limitations and includes features such as rate limiting and retry strategies to prevent the use of services.

The Log Analysis module is shown in Fig.3, The Analysis component functions, as the unit within the IPR validation framework. Its role is to examine data from WAFs and extract information such as IP addresses, timestamps, and request details from WAF logs. By cross-referencing this data with reputation information obtained from AbuseIPDB the module refines reputation scores based on behavior patterns. Utilizing algorithms, this module can identify activities by detecting anomalies and patterns that indicate malicious behaviour. It looks for indicators like repeated failed login attempts and known attack signatures using both techniques and machine learning methods to stay off emerging threats. One of its strengths lies in its ability to uncover slow-paced attacks by analyzing data trends over time allowing for early intervention. In addition to analyzing WAF logs, this module integrates the findings with server logs and intrusion detection systems to provide a view of network interactions. This integrated approach assists incident response teams in dealing with security incidents. The design of this module ensures scalability by processing volumes of log data through optimized pipelines utilizing big data technologies. It generates reports that highlight activities, for compliance purposes auditing procedures and security policy development. The detailed analysis of WAF logs significantly enhances IPR validation efforts reinforcing the security framework of an organization.

The IPR Communication module shown in Fig.3 serves as the hub for alerting in the IPR validation to inform stakeholders, such as network administrators and security analysts, about any issues related to IPR reputation. This is achieved using SMTP, which enables tailored notifications to be sent out whenever threats are detected by the reputation checking and log analysis modules. This module offers flexibility and intelligence by allowing alerts to be configured based on varying levels of urgency. Whether it’s providing summaries or immediate warnings the alerts can be customized to match the threat level associated with an IP address. The email templates used for these notifications can also be personalized to include information about IPR scores, related traffic incidents and recommended actions. The integration of data from modules ensures that communication is not only informative but also actionable. Furthermore, the Communication module automates incident responses like updating firewalls or isolating systems to swiftly mitigate threats. Security is a priority sensitive data is protected through encryption and authentication measures. Also, to ensure the delivery of messages, in cases of communication disruptions this module features queuing capabilities and fallback options. It acts as a communication backbone that guarantees threat information reaches the appropriate parties promptly. Ultimately this facilitates decision-making processes that are both effective and efficient.

9. Outcome and Results

9.1 Sample section of validated data

Table 3. shows the results of the main solution using a framework, for validating IPR has conducted an analysis on the dataset provided in the Report which was auto generated by the solution to evaluate the reliability of reported IP addresses. Our process involved gathering report data and assigning reputation scores to each IP address based on factors such as the number of associated reports, recency of the report and abuse confidence rating. While it enhances this scoring system, we cross-referenced our dataset with established whitelists and blacklists to ensure that none of the high-risk IPs had been previously classified as safe.

During our examination of traffic behaviour, we discovered a correlation between reported IPs and malicious activities such as port scanning and brute force attacks. IP Abused DB API Models trained these IPs as high risk through a perfect abuse confidence score aligning with this dataset’s ratings this is to ensure up-to-date accuracy we integrated real-time threat intelligence feeds while validating findings against global security incidents including The final validation of our solution has showcased a massive success rate, in identifying IP addresses highlighting its effectiveness in proactively detecting and addressing cyber threats originating from suspicious IP address such that its comprehensive analysis is supported by techniques and threat intelligence emphasizing the strength of our approach.

Table 3. Sample section of validated final test data

aws account id	region	ip address	total reports	usage type	isp	abuse confidence score	is white listed	breach details
xxxxxx	ap-southeast-1	106.75.177.81	10	Data Center/Web Hosting/Transit	Shanghai UCloud Information Technology Company Limited	31	0	The IP address 106.75.177.81 is located in China. It is assigned to Alibaba Cloud and is likely being used by a server or network device.
xxxxxx	ap-southeast-1	103.72.217.126	3	Fixed Line ISP	Soibam Technology Private Limited	13	0	The IP address 103.72.217.126 is a public IP address that is assigned to a device on a network. This IP address is used for communication and identification purposes on the internet.
xxxxxx	ap-southeast-1	104.131.170.150	0	Data Center/Web Hosting/Transit	DigitalOcean LLC	0	1	The IP address 104.131.170.150 is assigned to a server or device on the internet. It is a public IP address and can be used to identify the location and network of the device it is assigned to.

9.2 Top Reported Domains Illustration

Fig. 4 pie chart shows how abuse reports are divided among the five domains that have a confidence score of 100 indicating a level of certainty in the accuracy of the reported abuse. This information is especially important for cybersecurity and network management professionals as it highlights domains that are frequently associated with behaviour or malicious activity. Each segment of the chart represents a domain with a confidence score drawing attention to areas that require intervention or monitoring. By examining the pie chart stakeholders can easily identify which domains are most involved in these reports that need investigation or action while maintaining the clear visual representation of the chart allows for an understanding of how reports are distributed across these high-risk domains.

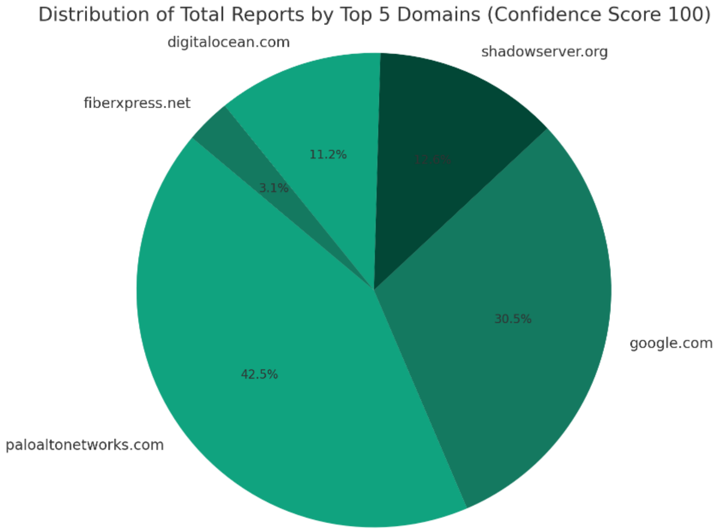


Fig. 4. Top Reported Domains

9.3 Top Reported ISPs Illustration

Fig. 5 is a bar graph that presents a comparison of the number of abuse reports associated with the top five Internet Service Providers (ISPs) for entries that have received a full confidence score of 100. The vertical bars represent the quantity of reports for each ISP allowing for an examination to identify which ISPs are linked to the volumes of verified abuse reports. This visual representation holds importance for network administrators, regulators, and security teams as it can indicate which ISPs may be hosting several individuals engaging in abusive or malicious activities as evidenced by their high confidence scores. It assists in identifying any patterns or trends within the data, such as whether specific ISPs have a high number of abusive IP addresses. This information could imply that these ISPs should strengthen their monitoring and security measures to reduce the risk associated with hosting activities. These charts serve as tools for making data-informed decisions and prioritizing cybersecurity resources. They condense datasets into understandable visuals offering clear insights into areas where network abuse is most concerning and reliable.

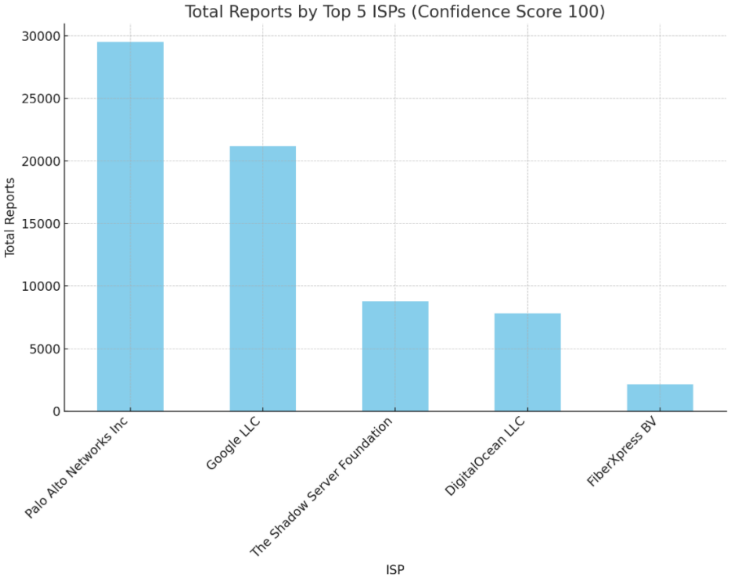


Fig. 5. Top Reported ISPs

9.4 Validated IP Abuse Score

Fig. 6 shows that the DB API models were ratified to be IP Abused, Plotting the virtual curve of Abuse Confidence Score that began with 80 and ended with 100 proves that our reporting system is intensified with the passing days. Confidence of reports increases especially from credible sources. This rises very possibly because the algorithm relates more highly to reported unusual IP addresses, severe admins taking greater weight. IPs with the high risk may end up with a loop of additional monitoring when the system fails to achieve a good level of attack-reducing mechanisms for these IPs. Organizations, with a cushion effect, may opt for such formulas that give higher results to the IP nearing the maximum with the scores being concentrated at the top end, or 100, signifying a strong consensus about the risk of a given IP. Therefore, it is expected that the frequency of scores at the upper end of the scale will rise sharply.

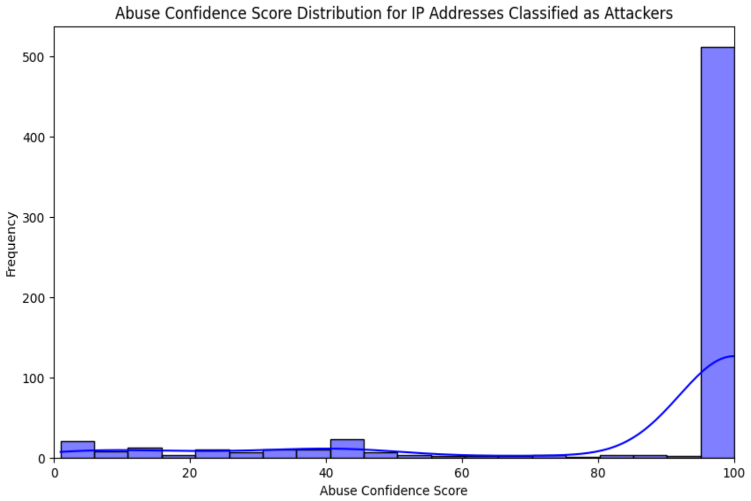
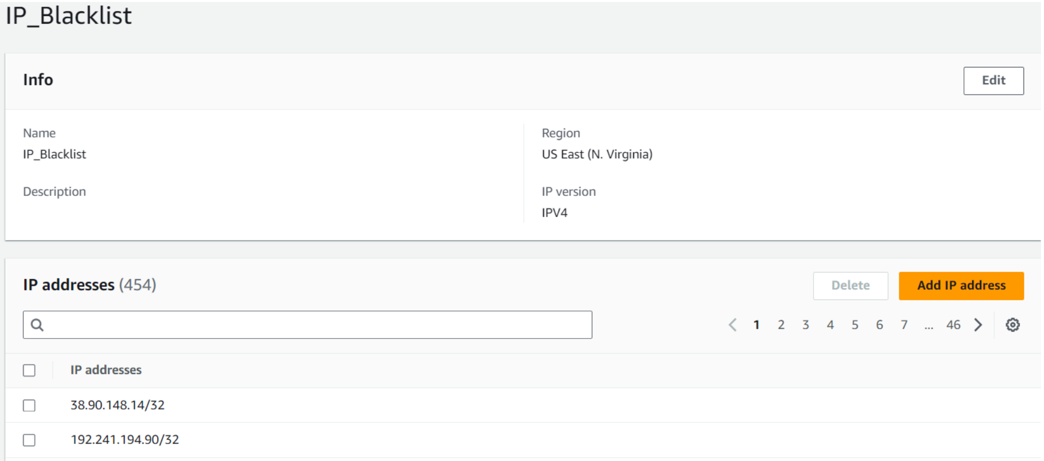


Fig. 6. Abuse score.

9.5 AWS WAF IP-Deny List for Blocked IP Address

Fig. 7 shows that an automated IP was blacklisted by The IP Reputation validation system accurately minimizing False Positive IP blocking to allow legitimate services not been getting blocked by the AWS WAF in the corresponding IP List section. Also, this solution successfully blocks these kinds of bad attacks by bad actors and automatically blacklines all relevant addresses based on machine learning-in effectively, those related to checking ML-Driven signatures verification process while the solution uses the IP-List section of AWS WAF to automatically blacklist attacks from bad IP addresses.



IP_Blacklist

Info

Name
IP_Blacklist

Region
US East (N. Virginia)

Description

IP version
IPV4

IP addresses (454)

□ IP addresses

□ 38.90.148.14/32

□ 192.241.194.90/32

Fig. 7. Blacklist over AWS WAF

10. Discussion

The solution showcased exhibits significant advantages, in the realm of cybersecurity operations and It streamlines the process of validating IPR, which is crucial for network security while connecting with AbuseIPDB the framework accesses a database of abuse reports related to IP addresses ensuring that its assessments are based on up-to-date information. With AbuseIPDB integration, the framework can get the sport of assessments done from the basis of reports of abuses related to IP addresses, the responsibility of being updated to comply with the information of those reports always lies with the framework. It is the capability of the solution to retrieve, and structure analyzed data responses that are praised since it helps analyses and integrates other systems to accomplish the whole process as well. Furthermore, its ability to gauge and cater to IP address volumes is the key point here, as to the extent IPs originate the threats, IP addresses can be fed into the automated IP monitoring system.

Along with all the other advantages of the solution, one should not skip mentioning the compliance with widely accepted best practices, specifically, adhering to rate limits given that the interactive with the third-party APIs is occurring. This helps the organization maintain its long-term service relationship and keeps the consumers using the service in line with the prescribed usage policy. The effective communication of technological assistance able with empathy and thoughtfulness is another factor. Also, it is apparent that the integration of OpenAI services into the framework could make AI-driven analysis and decision-making possible, at least as described in the information provided that is not completely clear. While it is creditable to have certain advantages, the solution still comes along with some shortcomings that may cause detraction from its efficient implementation. The major issue will be the overly simplistic way the algorithm deals with API rate limits, what may further delay the response, and this may not be ideal, particularly if I have many IPs whose access to the network must be managed. Also, if I must handle many IP addresses during the peak moments of network it is very hard to handle such kind of delay. There could be a case where bottlenecks will become a stumbling block for these organizations that do not have prompt enough responses to such threats.

Also, weaknesses of the error handling mechanism are another problem to be clarified. It fails to conveniently log on both emergencies and normal errors while the solution is not very sophisticated in terms of dealing with a different type of API errors. An important weakness is the main role of the AbuseIPDB database; in case this database isn't available, the system's capability to check and evaluate IP reputations will fail, leading the network to be open to threats. This data dependence indicates the need for resilience in the drawn solution. For instance, the issues of the IPR validation method need to be considered when primary data sources are not available. One of the ways can be the employ of alternative reputation services, based on heuristic analysis or on the cached data. Integration issues prevention is not less critical if the solution is to be used in practice and is planned for the real applications. Developing more mature error handling and response techniques, designing plan B in case data sources do not work, and optimizing the solution to process large amounts of data effectively are the key points that should be refined. Moreover, providing a vivid illustration of the integration of OpenAI services in addition to highlighting the role of AI-driven abilities making the solution as robust and useful as possible for complex cybersecurity scenarios is also an important element of our work.

11. Future Work

The process of feature engineering involves creating characteristics, from raw data to enhance the classifiers' ability to differentiate between harmless and malicious IP addresses while achieving this, we will examine reports of abuse, traffic patterns and other relevant metadata to identify traits that strongly correspond to activities such that for instance, This project will consider factors such as the frequency and recentness of attacks associated with an IP address, the variety of services targeted and the consistency of the origins of the traffic. Also, after transforming data into insights our model will become better at detecting sophisticated cyber threats. Additionally, it will utilize feature selection algorithms to remove redundant characteristics to optimize the classifiers' efficiency while reducing overhead to the IPR validation process to enable better focus on the most informative attributes to enhance this set of features, on the Random Forest (RF) model will be able to provide accurate and timely evaluations of IP reputation [34].

The RF classifier remains up to date and effectively integrating real-time data streams is an aspect of IPR detection work. This integration entails subscribing to threat intelligence feeds that provide up-to-the-minute information, on emerging threats and recent behaviours associated with IP addresses while analyzing real-time data the model will adapt to the changing landscape of threats ensuring that its evaluations of IPR are based on the up, to date information available. This dynamic approach allows for a defence strategy foreseeing and responding to threats as they emerge to handle a volume of data while maintaining the model's performance ensuring that the speed of validation does not compromise the accuracy or responsiveness of the system [35].

Also, the real-time data will not be used for evaluations but will also contribute to refining future predictions through training the model while this continuous learning process is crucial for maintaining an updated and effective cybersecurity defence mechanism. In future, the solution will optimize the model to efficiently handle datasets without compromising its performance. This optimization will ensure that the model can scale effectively as the volume of IP reputation queries increases while minimizing response time, which is crucial for real-time applications by Adjusting the configuration of the RF model to ensure it can quickly process queries while maintaining a level of predictive accuracy to safeguarding cybersecurity infrastructure [36]. The future ensemble models will go through cross-validation to make sure they are dependable while gathering predictive information will be utilized to improve security protocols strengthening the resilience of the system against cyber threats such that a comprehensive method of validating IPR guarantees that the cybersecurity solution remains strong and efficient, in countering types of threats.

12. Conclusion

In conclusion, this paper presents an approach for real-time validation of IPR that harnesses the power of AI and ML. Also, with cyber threats becoming increasingly complex it is vital to have mechanisms in place to ensure network security. Validating IPR is an aspect of this effort while the proposed solution addresses the challenge of assessing the credibility of an IP address by utilizing AI models developed by OpenAI, which automate data extraction and interpretation based on this research it has found that integrating AI capabilities related to NL processing and ML significantly improves accuracy in identifying and responding to threats. By employing algorithms such as regression and random forests along with data cleansing methods we have observed a decrease in false positives during blacklisting processes as well as a notable reduction in the active duration of malicious IPs. The significance of this framework lies in its potential to revolutionize cybersecurity. Also, automating security log analysis and strengthening the validation process of this solution not only streamlines workflows but also enhances the reliability of security infrastructures. The learning and adaptive features embedded within AI models ensure that the system evolves alongside changing patterns of cyber threats.

References

[1] J. Porenta and M. Ciglarič, “Empirical comparison of IP reputation databases,” *ACM Int. Conf. Proceeding Ser.*, no. December, pp. 220–226, 2011, doi: 10.1145/2030376.2030402.

[2] Safitra, M.F.; Lubis, M.; Fakhrurroja, H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability 2023, 15, 13369. https://doi.org/10.3390/su151813369

[3] M. Lyu, H. H. Gharakheili, C. Russell, and V. Sivaraman, “Hierarchical Anomaly-Based Detection of Distributed DNS Attacks on Enterprise Networks,” *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 1, pp. 1031–1048, 2021, doi: 10.1109/TNSM.2021.3050091.

[4] P. Vitliemov and K. Markov, "An Approach to Design a Haptic and Autonomous Multi-mission Incident Response Robot," 2022 8th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE), Ruse, Bulgaria, 2022, pp. 1-4, doi: 10.1109/EEAE53789.2022.9831391.

[5] S. H. Ahn, N. U. Kim, and T. M. Chung, “Big data analysis system concept for detecting unknown attacks,” *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 269–272, 2014, doi: 10.1109/ICACT.2014.6778962.

[6] E. D’Andréa, J. Francois, O. Festor, and M. Zakroum, “Multi-label Classification of Hosts Observed through a Darknet,” *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. 2023, NOMS 2023*, 2023, doi: 10.1109/NOMS56928.2023.10154356.

[7] K. Gaur, M. Diwakar, K. Gaur, P. Singh, T. Sachdeva and N. K. Pandey, "SQL Injection Attacks and Prevention," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-4, doi: 10.1109/ISCON57294.2023.10112156.

[8] H. Alejos, “DDOS Mitigation Analysis of AWS Cloud Network,” *Univ. Nusant. PGRI Kediri*, vol. 01, pp. 1–7, 2017.

[9] N. Novaes Neto, S. E. Madnick, A. Moraes G. de Paula, and N. Malara Borges, “A Case Study of the Capital One Data Breach,” *SSRN Electron. J.*, no. January, pp. 0–24, 2020, doi: 10.2139/ssrn.3542567.

[10] Naila Samad Shaikh, Affan Yasin, Rubia Fatima, "Ontologies as Building Blocks of Cloud Security", International Journal of Information Technology and Computer Science(IJITCS), Vol.14, No.3, pp.52-61, 2022.

[11] S. Achar, “Compliance Challenges for cloud firewall,” *World Acad. Sci. Eng. Technol. Int. J. Comput. Syst. Eng.*, vol. 16, no. 9, pp. 379–384, 2022, doi: 10.5281/zenodo.7084251.

[12] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, “Intrusion detection system in cloud computing: Challenges and opportunities,” *Conf. Proc. - 2013 2nd Natl. Conf. Inf. Assur. NCIA 2013*, no. December, pp. 59–66, 2013, doi: 10.1109/NCIA.2013.6725325.

[13] A. Rath, B. Spasic, N. Boucart, and P. Thiran, “Security Pattern for Cloud SaaS : From System and Data Security to Privacy Case Study in AWS and Azure,” 2019, doi: 10.3390/computers8020034.

[14] S. Yasser hashemi and P. Sheykhi Hesarlo, “Security, Privacy and Trust Challenges in Cloud Computing and Solutions,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 8, pp. 34–40, 2014.

[15] P. Kumar Sharma, P. Singla, V. Gupta, Paras and P. Garg, "An Era of ChatGPT: Systematic Analysis of Utility and Challenges," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 897-902, doi: 10.1109/ICECAA58104.2023.10212359.

[16] V. Le and H. Zhang, “Log Parsing : How Far Can ChatGPT Go ?”.

[17] V. Le and H. Zhang, “Log Parsing with Prompt-based Few-shot Learning”.

[18] E. Pyyny, “Mikko Lempinen CHATBOT FOR ASSESSING SYSTEM SECURITY,” no. June, 2023.

[19] J. L. Lewis, G. F. Tambaliuc, H. S. Narman, and W. S. Yoo, “IP Reputation Analysis of Public Databases and Machine Learning Techniques,” *2020 Int. Conf. Comput. Netw. Commun. ICNC 2020*, pp. 181–186, 2020, doi: 10.1109/ICNC47757.2020.9049760.

[20] S. Shaw and P. Choudhury, “A new local area network attack through IP and MAC address spoofing,” *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 347–350, 2015, doi: 10.1109/ICACEA.2015.7164728.

[21] E. Chiapponi, M. Dacier, O. Thonnard, M. Fangar, and V. Rigal, “BADPASS: Bots Taking ADvantage of Proxy as a Service,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13620 LNCS, pp. 327–344, 2022, doi: 10.1007/978-3-031-21280-2_18.

[22] Y. Huang *et al.*, “Detect Malicious IP Addresses using Cross-Protocol Analysis,” *2019 IEEE Symp. Ser. Comput. Intell. SSCI 2019*, pp. 664–672, 2019, doi: 10.1109/SSCI44817.2019.9003003.

[23] A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,” Knowledge-Based Syst., vol. 189, p. 105124, 2020, doi: 10.1016/j.knosys.2019.105124.

[24] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, “Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things,” IEEE Internet Things J., vol. 6, no. 4, pp. 6822–6834, 2019, doi: 10.1109/JIOT.2019.2912022.

[25] R. Ganeshan, C. S. Kolli, C. M. Kumar, and T. Daniya, “A Systematic Review on Anomaly Based Intrusion Detection System,” IOP Conf. Ser. Mater. Sci. Eng., vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022010.

[26] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, “Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset,” IEEE Access, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[27] D. Chiba, K. Tobe, T. Mori, and S. Goto, “Detecting malicious websites by learning IP address features,” *Proc. - 2012 IEEE/IPSJ 12th Int. Symp. Appl. Internet, SAINT 2012*, pp. 29–39, 2012, doi: 10.1109/SAINT.2012.14.

[28] D. Jeon and B. Tak, “BlackEye: automatic IP blacklisting using machine learning from security logs,” *Wirel. Networks*, vol. 28, no. 2, pp. 937–948, 2022, doi: 10.1007/s11276-019-02201-5.

[29] D. Jeon and B. Tak, “automatic IP blacklisting using machine learning,” Wirel. Networks, vol. 28, no. 2, pp. 937–948, 2022, doi: 10.1007/s11276-019-02201-5.

[30] N. Usman et al., “IP Reputation for Forensics Data Analytics,” Futur. Gener. Comput. Syst., vol. 118, no. January, pp. 124–141, 2021, doi: 10.1016/j.future.2021.01.004.

[31] S. Shaw and P. Choudhury, “MAC address spoofing,” Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015, pp. 347–350, 2015, doi: 10.1109/ICACEA.2015.7164728.

[32] Y. Huang et al., “Graph neural networks and cross-protocol analysis for detecting malicious IP addresses,” Complex Intell. Syst., vol. 9, no. 4, pp. 3857–3869, 2023, doi: 10.1007/s40747-022-00838-y.

[33] D. Ocampo, F. B. C, D. Castillo, T. M. L, and M. A. N, “A New Local Area Network Attack through IP and M,” pp. 198–205, 2013.

[34] F. Livingston, “Implementation of Breiman’s Random Forest Machine Learning Algorithm,” *Mach. Learn. J. Pap.*, pp. 1–13, 2005.

[35] D. D. Anton, “Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests”.

[36] J. Alonso, L. Belanche, and D. R. Avresky, “Predicting software anomalies using machine learning techniques,” *Proc. - 2011 IEEE Int. Symp. Netw. Comput. Appl. NCA 2011*, pp. 163–170, 2011, doi: 10.1109/NCA.2011.29.

Authors’ Profiles

NW Chanaka Lasantha, a seasoned Cyber & Information Security Architect, holds a Bachelor of Information Technology from the University of Colombo and a Master of Science from Kingston University, UK. Currently pursuing a Ph.D. at IIC Technological University, Cambodia, he has over 20 years of experience in the field. His expertise covers a wide spectrum including Data Protection, Risk Mitigation, Compliance, and Cloud & Linux Security. Presently a Security Architect at Kerner Norland, Chanaka is also skilled in SecDevOps and is a Defense Python Developer. He has developed numerous security solutions for cloud computing and Linux systems. Committed to promoting security awareness, he is an active speaker and contributor to security blogs and forums, sharing his extensive knowledge in cybersecurity.

Ruvan Abesekara obtained his Ph.D. in Computer Science and Technology from Dalian Maritime University, China, and holds an MSc in Computer Science from the University of Colombo School of Computing. He is currently a professor in Computer Science and the Vice Chancellor of the British College of Applied Studies, Sri Lanka. He also serves as an adjunct faculty member at the IIC University of Technology, Cambodia. In addition to his academic qualifications, Ruvan holds several industry and professional certifications. He is a member of several organizations such as The Institute of Doctors, Engineers and Scientists, the Institution of Engineering and Technology, the Institute of Electrical and Electronics Engineers, the British Computer Society, the Chartered Institute for IT, the Computer Society of Sri Lanka, and the Australian Computer Society, among others. Furthermore, he is a Microsoft Certified Peer Coach and a Cisco Certified Instructor. His current research interests include IoT, AI for cybersecurity, data mining and algorithms, and privacy-preserving techniques.

MWP Maduranga obtained his BSc.Eng. in Electronic Engineering degree in 2013 from the Asian Institute of Technology (AIT), Thailand, and an MSc.Eng. in Electrical and Electronic Engineering degree from the University of Peradeniya, Sri Lanka, in 2017. He earned his PhD degree in Computing from the IIC University of Technology, Cambodia, in 2022. Currently, he is a lecturer in Computer Engineering at the General Sir John Kotelawala Defence University, Sri Lanka. He is a senior member of IEEE and received an Engineering Charter in Electronics and Telecommunication Engineering from the Engineering Council, the UK, in 2020. He has co-authored numerous indexed journal articles and served as a member for several IEEE conferences in the region. His current research interests include Machine Learning-based indoor localization, AI/ML in IoT Applications, and wireless communication.

How to cite this paper: NW Chanaka Lasantha, Ruvan Abeysekara, MWP Maduranga, "A Novel Framework for Real-Time IP Reputation Validation Using Artificial Intelligence", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.2, pp. 1-16, 2024. DOI:10.5815/ijwmt.2024.02.01