EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Mobile Security Operation Centre (mSOC)

Sudhir Walia [1,*], Qazi Mustafa Kaleem[2] and Shinu Abhi[3]

[1, 2, 3] REVA Academy for Corporate Excellence, REVA University, Bengaluru, India

Abstract

Attacks on the internet are becoming increasingly threatening. For naïve home users, who are poorly protected, there is always an imminent danger of getting cyber attacked.
This paper is aimed to design and build an IoT-based Network Security device that would run as an access point for users to connect to the Internet in a home setting. The paper discusses a standalone perimeter security solution with Incident Response (IR) life cycle management and controls through an IoT device – Raspberry PI. Enterprise-level features such as Next Generation Firewall (NGFW), Network Intrusion Detection System (NIDS), Domain Control for Ad/Spam blocking, Security Information and Event Management (SIEM) for Log Co-ran System on Chip (SoC), which can be installed anywhere and carried for mobile operations. Hence, the name, Mobile Security Operation Centre (mSOC).
This solution intends to protect the user when browsing the internet and blocking or providing visibility to the malicious connections made to or from users. The mSOC can filter domains based on whitelist/blacklist and Regex Pattern. It can also identify the domains that are blocked or allowed. It also provides visibility to traffic, application statistics, and IP reputation. IP reputation and Malicious Domains then can act as input to the iptables for L3/L4 blocking. A Software User Interface is developed to integrate and manage multiple Open-Sourced applications like dnsmasq/ elk/ graylog/ SQlite3/ Iptables/ adminlte as a single product that could serve as a complete security solution for a home or Small Medium Business (SMB). Thus, the proposed solution secures naïve users from security exploitations.

Keywords: Internet, NIDS, IoT, NGFW, Raspberry Pi, SIEM

Received on 08 December 2023, accepted on 02 December 2023, published on 13 December 2023

doi: 10.4108/eetiot.4586

1. Introduction

By 2022, the global count of internet users had risen to 5.95 billion, marking an internet penetration rate of 62.5% within the entire world's population [1]. The numbers provide a valuable context for digital adoption and growth. With this digital growth, new cybersecurity issues are constantly emerging, with new viruses and malware being discovered daily. To prevent future attacks, it is important to know the most common types of attacks and their causes.

While organisations have the budget and resources to protect users from cyber threats, individual users lack the resources and skills to protect themselves. Among the top attacks on home internet users, 9% of malware were emails and more than 80% of reported security incidents were phishing attacks. Globally, each day sees around 14.5 billion messages that are classified as spam/phishing makes up for 45% of all emails, of which at least 20% of home users fall victim to [2]. Some of the most prevalent cyber threats are phishing,, social engineering, ransomware, and Distributed Denial of Service (DDoS).

Most of the technology deployment involves the protection of assets in an organisation. However, the studies show that it is not just the organisations that are prone to cyber-attacks, but everyone connected to the internet is vulnerable.

There is limited literature available on the implementation of IoT-based security solutions for Small and Medium Enterprises (SMEs) and Small Offices/Home offices

*Corresponding author. Email: sudhir22e@gmail.com

(SOHOs). Feasibility studies of implementing Raspberry Pi-based Domain Filtering, SIEM, and IP reputation for SOHOs and SMEs are hardly available in the extant literature.

The need for security is at the forefront today for all. Constructing an intelligent home brings convenience, yet it comes with the demands of securing sensitive areas that contain a wide range of IoT devices. With the increase in cybercrimes, network security is a must-have for businesses and SOHOs. Employees must constantly be linked to the home network to work for users to work from home. Updating home network security, minimizing vulnerabilities, and implementing additional security measures are essential. Strengthening security is also necessary due to the increasing number of IoT devices that can connect to the home network. The network serves as the main point of entry for hacking IoT, making it crucial to enhance security. In a research study conducted on RPi as a packet analyzer and honeypots [3], RPi has been utilized as an affordable, energy-efficient, and practical home network security system. This includes implementing IDS Suricata, deploying several honeypots, and utilizing a tshark packet analyzer. The performance of the device is also evaluated while the system is in operation. To visualize log data from the four sensors, the ELK stack is employed.

RPi-based security solutions can take on the event of a data breach [4]. It is the hardware that supports Debian based OS which provides utility features like Vulnerability Analysis, Network Analysis, Security Policy measures, IPtables, DHCP Service, and DNS proxy to intercept queries and filter domains. The main priority of small companies is to protect the data. However, making a Single touch security solution is extremely difficult with a restricted budget. The company's credibility and reputation are in danger if they disregard security. This cannot be solved with a mostly one-touch i.e., an expensive system that is costly for a small business. The intended solution considers the needs of such an organisation. This cost-effective solution can be viable for a small organisation.

RPi-based Invasion Detection Systems use open-source code to detect intrusions on SOHO networks [5]. Some of the malware looks for fields such as port numbers and packets that are encoded especially, but snort IDS can detect files that contain Malware embedded codes. Small Office Home Office (SOHO) networks, use some Intrusion Detection Systems (IDS) that can be activated to monitor possible attacks. Intrusion Detection Methods (IDM) are a convenient, in-home, inexpensive form of network security. Visible IDMs use software and hardware implementations to packet filter, signature-based detection programs, to detect cyber-attacks in real-time, or to record information and then send it to 24 hours online reporting service.

Senior management must always be aware that the security specialist at the company is useful in implementing a virtual security stack; however, the basic premise of their security service must be economically developed since the budget is limited and RPi can be used as a low-cost option [6].

There is an ever-increasing need to make our networks more secure and to ensure against breaches, leaks, and risks from bad Internet actors. Adding security features to homes connected to the cloud can make it more stable, with minimal downtime. Modern-day insecurity has many risks; cybercrime, hacking, network attacks, and Distributed Denial of Service (DDoS) [7]. Therefore, the authors have produced this guide for a secure home network. It provides an overview of using an Intrusion Detection System IDS, network security system, network intrusion prevention system, or IT security device. The hand-held device is used by a guardian to check an area and to keep an eye.Ghosh et al. (2023) embarked on a comprehensive study to assess water quality through predictive machine learning. Their research underscored the potential of machine learning models in effectively assessing and classifying water quality. The dataset used for this purpose included parameters like pH, dissolved oxygen, BOD, and TDS. Among the various models they employed, the Random Forest model emerged as the most accurate, achieving a commendable accuracy rate of 78.96%. In contrast, the SVM model lagged behind, registering the lowest accuracy of 68.29%[12].Alenezi et al. (2021) developed a novel Convolutional Neural Network (CNN) integrated with a block-greedy algorithm to enhance underwater image dehazing. The method addresses color channel attenuation and optimizes local and global pixel values. By employing a unique Markov random field, the approach refines image edges. Performance evaluations, using metrics like UCIQE and UIQM, demonstrated the superiority of this method over existing techniques, resulting in sharper, clearer, and more colorful underwater images[13].Sharma et al. (2020) presented a comprehensive study on the impact of COVID-19 on global financial indicators, emphasizing its swift and significant disruption. The research highlighted the massive economic downturn, with global markets losing over US $6 trillion in a week in February 2020. Their multivariate analysis provided insights into the influence of containment policies on various financial metrics. The study underscores the profound effects of the pandemic on economic activities and the potential of using advanced algorithms for detection and analysis[14].

Another study tested the performance of Raspberry Pi in context to network performance, latency, throughput, and CPU and memory usage. RPi-3 based design with a Snort-based IDS implemented on it. Packet Sniffer is also utilised to examine network traffic, and the SHA based hashing technique is employed to generate the hash value regularly [8]. There are five types of assaults implemented in this paper: RDP Brute Force, ICMP flooding, SMTP Brute Force, SYN Flood, and Web Phishing. 'htop' utility was

used to do performance testing, and 'sha-sum' program was used to run the test vector method. The Raspberry Pi detected 100 per cent of threats with less than 50 per cent CPU and 10 per cent RAM. As a result, the system may be used on home networks as a viable and low-cost alternative for implementing cybercrime security.

A novel solution like mSOC – Mobile Security Operation Center based on IoT devices like Raspberry Pi can provide a Web-based user interface to configure domain filtering, IP reputation, traffic filtering, and Data Visualization.

2. Solution Phases

The objective of the study is to secure home users with IoT devices like a Raspberry Pi, customised to provide a security solution. This study mimics the basic SOC – Security Operational Centre functionalities at the home level and controls at the fingertips of the user.

At its center, mSOC is a small, transportable tool, pre-packaged with the capability of mSOC. The tool can be seamlessly deployed everywhere (called as Plug & protect): As proven in Fig. 1 users in a clever home ought to use it to guard their clever gadgets. it's far correctly a transportable, on-call for, tool that protects customers from attacks or suspicious activities.

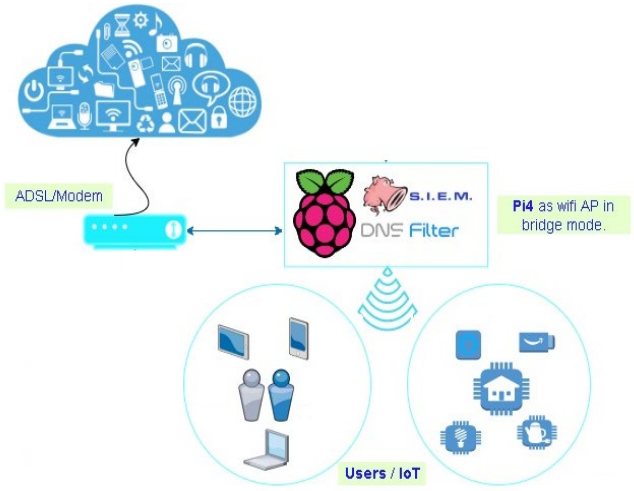

Fig. 1. mSOC Solution

This solution involves developing a system based on the following requirements in mind:

a. Portability: It is small enough to carry and secure the device wherever required.

b. Minimum configuration: The device should require limited configuration and default protection enabled.

c. Frontend Software Application Development: Develop a user interface to manage and control SOC functionalities.

d. UX and Data Analytics.

2.1. MSOC – Tools Integration

In the primary stage, open-source applications were selected and scoped for mSOC solutions. The scoped application modules are studied to be supported on the ARM CPU architecture and compatible with Raspberry PI Hardware limitations. Based on the research and tests, Open-Source modules in Fig. 2, SNORT- as NIDS, dnsmasq – as Domina Filter, Graylog – as ELK for SIEM, Linux IP Tables – as Unified FW controls, SQLite – as DB, were concluded.

Fig. 2. Modular Stages

mSOC is developed with the following features:

a. Domain Filtering: Filter domains based on a blacklist, and whitelist. Support Regex-based filtering

b. NIDS: Snort IDS for traffic visibility, app identification, and IP Reputation check.

c. SIEM: Analytics and Data Visualization of Domain/IDS logs. Geo-Location information of CPE

d. IPtables: To block traffic based on L3 and L4 filters.

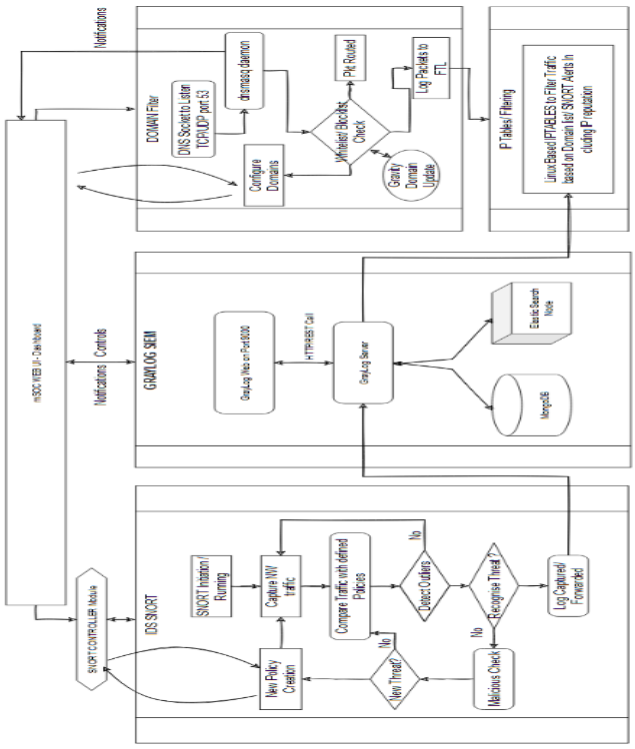

Fig. 3. Software Architecture

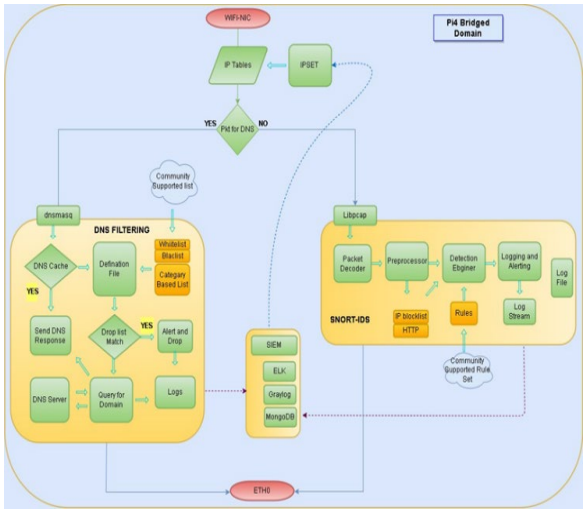

Fig. 4. Modules and Packet Flow

2.2. MSOC – Control

The second stage was a development of a Web-based Graphical User-interface that co-relates all the available data and showcases these raw data into useful information on a single dashboard – Operation view, as shown in Fig. 3. Web UI also helps integrate and manage all modules as one entity.

a. Domain Filtering Configuration and Management
b. SNORT rules management
c. Domain Filtering log correlation and Analytics
d. System Management and Monitoring

Each module in Table 1 is developed on a PHP framework to edit and manage individual applications.

Table 1. PHP Modules

Module Name	Module Function
Message.php	Manage Notifications
Adlist.php/ domains.php	Manage ad list & domains to filter.
Networks.php	Showcase real-time network mapping of clients
Debug.php	Helps to display debugs logs on web UI
snort_rule_manager.php	To manage snort rules and controls.

3. Implementation

The mSOC device is based on open-source packages and libraries compatible with ARM 64bit architecture. There are four separate modules mSOC around which the complete solution is built. Fig. 4 shows packet flow across multiple modules.

3.1. Dnsmasq and Sqlite3: Domain filtering

Dnsmasq is an open-source package that provides DNS, DHCP, and TFTP Server services. Its main function is to provide a pair of DNS and DHCP services for the LAN user. It can also be used to track all devices connected to the LAN.

Dnsmasq listens on the port 53 socket, which intercepts DNS queries and replies to queries from the local cache or local DB or recursive query to DNS servers. It also refers */etc/hosts* to resolve internal domains locally. It can act as an authoritative DNS server to publish local domains to appear in the global DNS. It supports DNSSEC validation as well.
The SQLite database stores whitelists and blacklists that are directly relevant to domain-blocking behaviour. The domain list table contains all domains on the white- and blacklists. There are fields in the database to store information related to a domain such as domain is enabled, when was domain added, last modified, and domain part of which IOC feed.

3.2. Snort NIDS: IP Reputation and App-detection

In Open-Source Intrusion Detection System (IDS), Snort is the foremost in the world. Snort IDS uses rules defined in Fig. 5 [9] that help identify malicious activity; packets are matched against the rules and generate alerts for users. Snort serves various purposes such as functioning as a network packet sniffer, a packet logger, or as a network Intrusion Prevention System (IPS) or Intrusion Detection System (IDS). Additionally, Snort rules can be employed to correlate with Indicators of Compromise (IOC) feeds that are sourced from threat intelligence.

Snort configuration files contain default values for rules paths, and local networks and allow the implementation and configuration of Snort preprocessor rules for OpenAppid and IP blacklist checks. Note that Snort preprocessors and modules allow a variety of customisations and configurations. The configurations made in this section are minimal to get started with Snort.

Snort rules, OpenAppid, and IP-reputation lists are stored in their respective directory. The `/etc/snort/rules` directory will contain all the rules:
`/etc/snort/rules/odp:` directory will contain the AppID detectors, and
`/etc/snort/rules/iplist:` directory will contain IP blacklists and whitelists

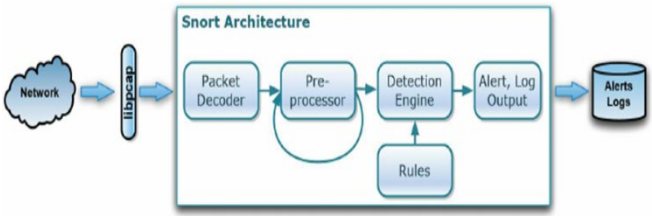

Fig. 5. IDS Flow

3.3. Iptables and Ipset: Stateful Firewall.

The Linux kernel has a packet filtering capability to control inbound/outbound and transit traffic using the iptables utility. Iptables provide L3 and L4 firewall filtering solutions that can be easily managed and configured.

Iptables is particularly well-suited for Linux-based firewalls. It can filter traffic based on L3 and L4 information, it can also check if there is an existing connection bypass for further filtering to reduce the processing overhead. We can use IOC feeds to apply to iptables, but the feed can have thousands of IPs, which can affect system performance. In combination with iptables, we can use an ipset list that can have thousands of IP or port combinations, and this single ipset list is called in iptables. Lockup with ipset is very fast as IP address and port pairs as saved in the hash. This provides the ability to block thousands of IPs with one iptables rules without much impact on performance. Iptables rules are saved in /etc/iptables/rules.v4. There are four ipset lists are created, which are further mapped to the main ipset list called in the iptables drop rule.

3.4. Web UI /Dashboard

Front-End web page design and structure were developed to enhance the users' experience. Achieving a harmony between practical and visually appealing design, while flawlessly integrating with smartphone functionality.

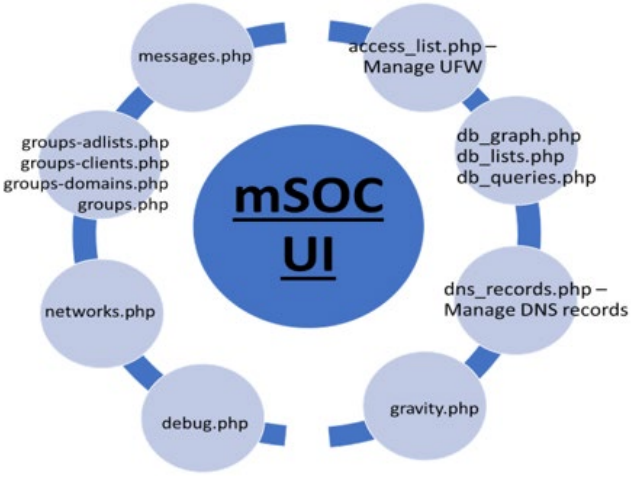

Fig. 6. UI Interactions

Open-Source Code Adminlte [10] was re-used to achieve a better user experience in the dashboard showcasing Timeline, Pie charts and Bar charts etc., Web pages are optimised for best speed and scalability by employing a diverse selection of markup languages to design web pages including, JavaScript and CSS.

PHP is used to develop backend; all the web pages are directly called on click this helps us to reduce overhead by eliminating pre-defined frameworks. For Web Hosting lighttpd daemon is used to handle HTTP requests. All the associated PHP files are shown in Fig. 6.
access_list.php, auditlog.php, cname_records.php, db_graph.php, db_lists.php, db_queries.php, debug.php, dns_records.php, groups.php, network.php, queries.php, queryads.php, settings.php, taillog-FTL.php, taillog.php

Lighttpd (pronounced /lighty/) is a robust, speedy, compliant, and incredibly adaptable web server that's been fine-tuned for high-performance settings. It employs memory and CPU in an efficient manner, ensuring less resource consumption compared to other well-known web servers. Its broad range of advanced capabilities, including CGI, URL-Rewriting, Auth and much more,

position lighttpd as an ideal application for all sizes of application, from small to large. Lighttpd is distributed under the open-source revised BSD license.

AdminLTE is based on Bootstrap 4.6 framework a totally responsive management template. It's a customizab le and clean-to-use template
and fits many display resolutions from
small cell devices to massive computer systems. desk II captures all the possible plugins which might be being used to develop the frontend internet application.

Table 2. Open-Source Plugin

Used For	Plugins
Charts	ChartJS, Flot, Sparkline, uPlot
Editors	Summernote, CodeMirror
Form Elements	Bootstrap Colorpicker, Bootstrap Slider, Bootstrap Switch, Date Range Picker, Dropzone JS, iCheck Bootstrap
Icon Packs	FontAwesome 5, flag-icon-css
Table Grids	DataTables, jsGrid

4. Conclusion and Recommendations for Future Work

Our solution fundamentally revolves around a Raspberry Pi that is equipped with DNS filtering, Snort IDS, IP-Filtering, Data Analytics, and a Single pane of glass to manage the solution. This research posits that our solution is built on a commonly used device like the Raspberry Pi, is capable of functioning as a security operations center, dashboard, single window control management, and integration of multiple open-source applications.
To substantiate our assertions, we conducted tests where the Raspberry Pi served as an Access Point, analysing, and filtering different types of network traffic from connected devices and users. Additionally, this study experimented with a different configuration, namely an App Detection engine, DNS filtering-based opensource database, and the number of rules loaded.
Our findings indicate that the Raspberry Pi can successfully host all mSOC modules, thus, demonstrating the feasibility of using Raspberry Pi in this context. Surprisingly, the Raspberry Pi 4 model was able to accommodate the intensive resource demands of the mSOC module without taxing the CPU and RAM excessively. In further test scenarios, even with multiple IoT devices connected to mSOC and high data transfer rates within a four-member family setup, memory usage never hit 100% capacity. However, additional tests involving larger networks are needed to ascertain the true capabilities of the Pi4+mSOC for possible application in Small and Medium-sized Enterprises (SMEs).
Furthermore, this study plans to evolve User Interface, Data Correlation, and Data Analytics and move them to the cloud. RPi4 will run as an edge device managed centrally from the cloud or mobile app.
Additionally, this study intends to add features like Zero Touch Provisioning, IoT devices detection & Segmentation, and URL filtering..

4. Acknowledgment

This research was realized with the vital contributions of Mr. Sandeep Vijaya Raghavan and Dr. Rashmi Agarwal. Right from the research's onset, their guidance was instrumental in fostering a comprehensive understanding of the subject matter. I sincerely appreciate the unique experiences they orchestrated for me and the opportunities they offered for my professional growth.

References

[1] S. Kemp, "datareportal," 21 04 2022. [Online]. Available: https://datareportal.com/reports/digital-2022-april-global-statshot.
[2] S. O'Brien, "The anatomy of a phishing email," 24 05 2018. [Online].
Available: https://securityitsummit.co.uk/briefing/guest-blog-the-anatomy-of-a-phishing-email/.
[3] Febrian Rachmad Hariawan, Septia Ulfa Sunaringtyas, "Design an Intrusion Detection System, Multiple Honeypot and Packet Analyzer Using Raspberry Pi 4 for Home Network", 2021 17th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering, pp.43-48, 2021.
[4] SARATH S, ASIF A, ARAVIND P, "Low-cost Security Solution for Micro, Small and Medium Enterprises", 2020 IEEE International Conference for Innovation in Technology (INOCON), pp.1-9, 2020.
[5] M. Coşar and S. Karasartova, "A firewall application on SOHO networks with Raspberry Pi and snort," 2017 International Conference on Computer Science and Engineering (UBMK), 2017, pp. 1000-1003, doi: 10.1109/UBMK.2017.8093414.
[6] Jose Emmanuel Cruz de la Cruz, Christian Augusto Romero Goyzueta, Cristian Delgado Cahuana, "Intrusion Detection and Prevention System for Production Supervision in Small Businesses Based on Raspberry Pi and Snort", 2020 IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing (INTERCON), pp.1-4, 2020.
[7] Shyava Tripathi, Rishi Kumar, "Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer", 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), pp.80-85, 2018.
[8] G. Vira Yudha and R. Wisnu Wardhani, "Design of a Snort-based IDS on the Raspberry Pi 3 Model B+ Applying TaZmen Sniffer Protocol and Log Alert Integrity Assurance with SHA-3," 2021 9th International Conference on Information and Communication Technology (ICoICT),

2021, pp. 556-561, doi: 10.1109/ICoICT52021.2021.9527511.
[9] Thomas Scheffler "Schematic-data-flow-in-the-Snort-IDS" 01 07 2012. [Online] Available: https://www.researchgate.net/figure/Schematic-data-flow-in-the-Snort-IDS_fig1_264149701
[10] REJack, "AdminLTE v3.2.0" 08 02 2022. [Online]. Available: https://github.com/ColorlibHQ/AdminLTE/releases
[11] L. Nagy and A. Coleşa, "Router-based IoT Security using Raspberry Pi," 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2019, pp. 1-6, doi: 10.1109/ROEDUNET.2019.8909551.
[12] Ghosh H, Rahat IS, Shaik K, Khasim S, Yesubabu M. Potato Leaf Disease Recognition and Prediction using Convolutional Neural Networks. EAI Endorsed Scal Inf Syst [Internet]. 2023 Sep. 21 [cited 2023 Sep. 22];.https://doi.org/10.4108/eetsis.3937
[13] Alenezi, F.; Armghan, A.; Mohanty, S.N.; Jhaveri, R.H.; Tiwari, P. Block-Greedy and CNN Based Underwater Image Dehazing for Novel Depth Estimation and Optimal Ambient Light. Water 2021, 13, 3470. https://doi.org/10.3390/w13233470
[14] G. P. Rout and S. N. Mohanty, "A Hybrid Approach for Network Intrusion Detection," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 614-617, doi: 10.1109/CSNT.2015.76.