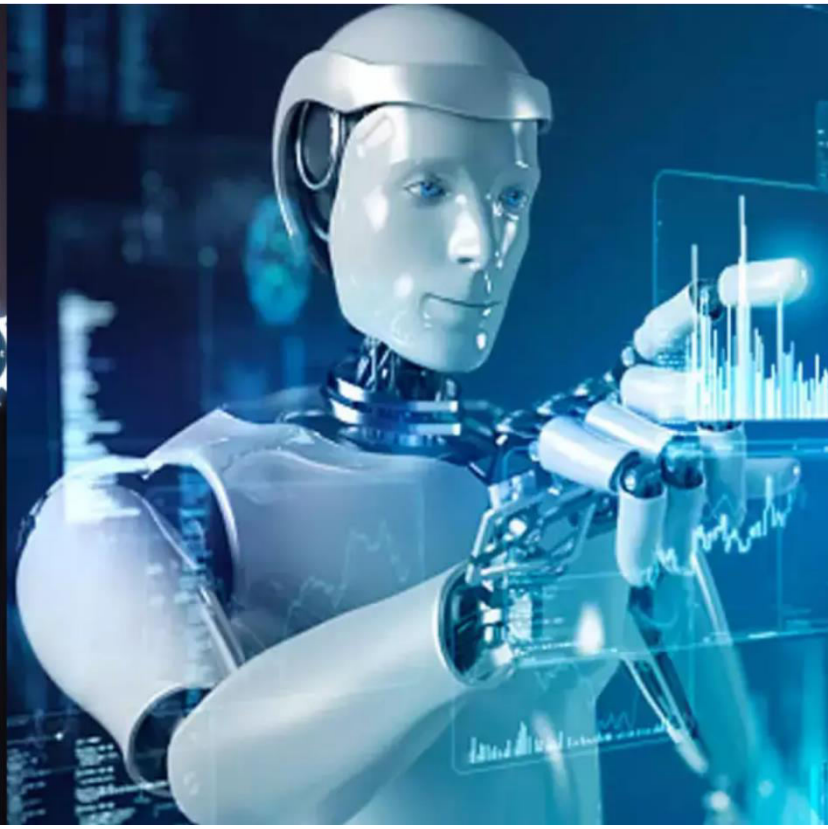
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404190|

Pishield: Secure IoT Gateway with Honeypot Defense

Mr.M.Goutham[1] , S.Snehaja[2], Danukoti Srinu[3] ,P.Snigdha[4], Cheruku Bhuvan[5]

Professor, Malla Reddy University, Hyderabad , Telangana, India[1]

B. Tech, Department of CSE, Malla Reddy University, Hyderabad , Telangana, India[2-5]

ABSTRACT: The rapid growth of the Internet of Things (IoT) has extended considerable security due to lack of weak authentication, outdated firmware and standardized security protocols. Pishield: A secure IoT gateway with Honeypot Defense aims to overcome these challenges by providing a centralized, scalable and simple security solution. Our approach integrates secure IoT gateways with firewall guidelines and access control mechanisms, tools such as Snort and Sunicata to intrusion detection and prevention systems (IDS/IPS), and honeypot systems that attract and analyze cyber threats. Additionally, it ensures secure remote access via VPN-based authentication with multi-factor security. Using tools like Moose Stack and Grafana, real monitoring and protocols allow for automatic detection of threats and warnings. Pishield is developed for Raspberry PI or ARM-based architectures to provide an inexpensive, aggressive defense mechanism against cyber threats targeted at IoT networks, increasing safety and operational flexibility.

KEYWORDS: IoT Safety Protected IoT Gateway, Honeypot Defense, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Firewall Rules, Live Monitoring, Threat Spotting, Raspberry Pi Protection, Budget-Friendly Cyber Defense.

I. INTRODUCTION

The Internet of Things (IoT) has rapidly changed industries such as healthcare, smart homes, production and transportation by enabling seamless communication between connected devices. However, this progress has raised considerable security concerns. Most IoT devices have limited resources and often lack integrated security features. This means that you are susceptible to cybercrime. Frequent threats include DDOS attacks (distributed denial of service), central (central) human attacks, unauthorized access, and malware infections. These attacks not only affect sensitive data, they can also hinder critical processes.

Traditional cybersecurity solutions such as firewalls and intrusion detection systems (IDS) cannot provide adequate protection in an IoT environment, making it often difficult to effectively recognize, capture and capture real-time threats. Furthermore, many IoT networks lack efficient monitoring and protocol mechanisms, making it difficult to recognize that they respond proactively to security anomalies. The project uses tools such as Snort and Suricata to integrate secure IoT gateways, including firewall guidelines, access control mechanisms, and intrusion detection and prevention systems (IDS/IPS). Additionally, we use honeypot systems to attract, analyze and mitigate cyber threats to IoT devices. Pishield also ensures secure remote access by including VPN-based authentication (OpenVPN/WireGuard) with multi-factor authentication (MFA) for management control. Actual monitoring and protocols using Elk -Stack or Grafana allow automated threat detection and alarming, allowing for immediate responses to security violations. By combining active threat detection, intrusion prevention and real-time security analytics, the project aims to improve the resilience of the IoT ecosystem to the development of cyber threats. Additionally, it optimizes security by minimizing computing efforts, making it suitable for resource-limited wireless sensor network nodes (WSNs). This study also proposes an intelligent and adaptive wireless sensor network (IA-WSN) choral torque that uses AI and machine learning (ML) technologies to improve performance, reliability and dynamic routing.

II. LITERATURE SURVEY

In the beginning IoT security tactics hinged on fixed ways to prove who you are and rules to block bad internet traffic. Yet, these strategies didn't hold up against ever-changing cyber dangers. Network safety measures, like WPA2 and SSL/TLS, became common to keep network chats safe. But, they couldn't shift on the fly to fight off new online threats leaving IoT setups open to clever break-ins. To keep an eye on internet traffic and spot bad stuff, detection systems like Snort and Suricata popped up. They got better at finding threats, but since they stuck to a preset list of known issues, they weren't great at stopping brand new surprises in cyber attacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404190|

To up the ante on safety, systems like Honeyd and Kippo [3] popped up. Their job? To lure in and study cyber threats. They were super smart at figuring out how baddies behaved but needed a ton of computer power, which made them too heavy for IoT gadgets with not enough juice. To stop unwanted sneaks, people started using solid remote entry stuff with VPNs that check who you are and multi-factor confirmation (MFA) [4]. Even though they were pretty good at keeping things on lockdown, they sometimes slowed things down. This got in the way big time when IoT stuff needed to work fast and without delays.

In the beginning IoT security tactics hinged on fixed ways to prove who you are and rules to block bad internet traffic. Yet, these strategies didn't hold up against ever-changing cyber dangers. Network safety measures, like WPA2 and SSL/TLS, became common to keep network chats safe. But, they couldn't shift on the fly to fight off new online threats leaving IoT setups open to clever break-ins. To keep an eye on internet traffic and spot bad stuff, detection systems like Snort and Suricata popped up. They got better at finding threats, but since they stuck to a preset list of known issues, they weren't great at stopping brand new surprises in cyber attacks.To stop unwanted sneaks, people started using solid remote entry stuff with VPNs that check who you are and multi-factor confirmation (MFA) [4]. Even though they were pretty good at keeping things on lockdown, they sometimes slowed things down. This got in the way big time when IoT stuff needed to work fast and without delays.

Tools for logging and keeping tabs on things in real time, like ELK Stack and Grafana, made getting better at finding threats on their own and reacting to them a big deal. But, making these tools fit into the simpler setup of IoT is tricky.
IoT networks gotta watch out for the routing trouble big time. So they made this thing, the Routing Protocol for Low-Power and Lossy Networks (RPL) [8], to help with saving energy while routing in IoT places. Thing is, it still gets hit by nasty routing issues like wormhole, blackhole, and sinkhole messes. Some smart folks are looking into flexible firewall rules and ways to keep out the bad guys [9]..

III. LIMITATION AND MOTIVATION

First, IoT security was based on static authentication methods and predefined rules that block malicious traffic. However, these traditional strategies have proven ineffective against the development of cyber threats. Network security measures such as WPA2 and SSL/TLS were standards for ensuring communication, but the standard was that they could not dynamically adapt to demand attacks.

Intrusion detection systems (IDs) such as Snort and Sunicata have been introduced to improve threat detection. They were effective in identifying known threats, but relying on distinctive detections, and therefore attempted to recognize ambitious cyberattacks. To address this limitation, honeypot solutions such as Honeyd and Kippo were developed to attract and analyze cyber threats. These tools provided valuable insight into the behavior of attackers, but required considerable computing resources. This means it is not suitable for resource-related IoT IoT devices. These security measures were effective and sometimes introduced delays that disable IoT operations in real time. Similarly, monitoring and protocol tools such as Elchistack and Grafana improved detection and response of Elchistack and Grafana, while low power and lossy networks (RPL) routing protocols were developed to optimize IoT efficiency routing. However, it remains susceptible to routing attacks such as wormholes, blackholes, and sinkholes attacks. Researchers actively investigate adaptive firewall rules and intrusion-perturbation techniques to mitigate these threats.

A. Research Gap

Existing IoT network security solutions do not meet some key requirements:

Effective Intrusion Detection for IoT Devices – The majority of Intrusion Detection/Prevention Systems (IDS/IPS) are built with traditional computing environments in mind instead of low-power IoT devices, so they cannot be used to protect resource-limited networks.

.

Proactive Threat Prevention – Current security measures are mostly reactive in nature, aiming to counter attacks after the fact instead of blocking them in the first place.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404190|

Cyber Threat Intelligence-Integrated Honeypots – There has been little research into the deployment of honeypots in IoT gateways to deliver real-time threat intelligence and active security measures..

B. Problem Statement

DDoS attacks, unauthorized access, injecting malware, and even data breaches are some of the numerous threats to IoT devices. Weak security protocols that are responsible for these attacks include:

Ineffective authentication policies

Firmware engineered with oversight of vulnerabilities

Absence of security analytics and monitoring in real-time.

C. Problem Definition

Some of the major security challenges in IoT networks include:

1. Lack of authentication: Multiple IoT devices function using factory presets, thus making them easily vulnerable.

2. Poor intrusion monitoring: Current firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are not designed or tailored toward the limitations of IoT devices.

3. Absence of real time surveillance: IoT networks do not have adequate unified logging systems, automated threat notifications, or response systems.

4. Unexploited honeypots: Insufficient analysis of how cyberattacks honeypots permits them to go unmonitored.

5. Budgeting a secure solution: Many IoT security frameworks' require costly infrastructure and elaborate set up which makes their use impractical.

The problem of work is also expressed in the form of mathematical equation.
PiShield's Security Approach is Formulated Mathematically
PiShield protects IoT networks by integrating several security measures. The following mathematical formulas are used to model the system:

1. Filtering network traffic using firewall rules

PiShield uses firewall policies to control network traffic, both inbound and outbound. Let's:
T is the total amount of network traffic.
Traffic is permitted.
B be traffic-blocked
$T = A + B$
T = A + B
A collection of security rules is used to assess an incoming packet P.
R:
$P \in R \Rightarrow A$, $P \notin R \Rightarrow B$
P ∈ R⇒A, P ∈ / R⇒B
If a packet satisfies a rule in R, it is permitted; if not, it is blocked.

2. Anomaly Detection in Intrusion Detection Systems (IDS)

The IDS uses a threshold-based model to monitor network packets and identify anomalies. Let's:
N is typical network behavior.
Let X be a network packet that has been observed.
Let D represent the departure from typical conduct.
$D = |X - N|$ D=|X−N|
The packet is marked as an intrusion if the deviation is greater than a predetermined threshold, Td:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404190|

$D \Rightarrow$ Intrusion Found
D>T d ⇒Intrusion Found
3. Attack Detection Using Honeypots
Malicious traffic is drawn to and examined by PiShield's honeypot system. Let's:
Let M be the total number of attacks that were seen.
H is the quantity of attacks that the honeypot has identified.
$H = \sum i = 1\ If\ (Ai)$
H= i=1 ∑ I f(A i)
where each attack instance is represented by A i, and the honeypot's detection function is denoted by f(A i).

4. VPN authentication, or secure remote access
Multi-factor authentication (MFA) is used by Pi-Shield to provide secure remote access. A user U needs to confirm:
C (Credentials)
T (Token of Authentication)
Biometric Factor B
$U = C + B + F$
U = C + T + B
If all three conditions are met, access is allowed:
$C \cap B \angle \emptyset \Rightarrow$ Access Acquired
C∩T∩B` = ∅⇒Access Granted

5. Monitoring and Logging in Real Time
Over time t, security events E are recorded. Let's:
The logging function is represented by L(E).
Each detected security event is indicated by e_i.

$L\ (E) = \int 0\ t \sum i = 1\ nei$
L(E)=∫ 0 t
i=1 ∑ n e i dt

If the quantity of recorded events exceeds a predetermined threshold, T e, an alert is generated.
$L\ (E) > Te \Rightarrow$ Alert Generated
L(E)>T e ⇒Alert Generated

Key Components of the Proposed Model
1. **Secure IoT Gateway Module** – This bad boy acts as the boss of security slapping on firewall rules and keeping an eye on who gets in and out to stop sneaky intruders..
2. **Secure IoT Gateway Module** – This bad boy acts as the boss of security slapping on firewall rules and keeping an eye on who gets in and out to stop sneaky intruders.
3. **Honeypot-Based Threat Analysis Module** – Kind of like setting a trap with fake systems that trick and study would-be hackers, boosting our sneaky-smarts and defence game.
4. **VPN-Based Secure Access Module** – Rolls out secret-code talks and double-checks IDs with stuff like multi-factor authentication to keep remote login tight and trespassers out Detailed Explanation of Each module .

IV. METHODOLOGY

System Design and Architecture – The security framework is designed to run on Raspberry Pi or ARM-based architectures, making it lightweight and scalable. The gateway for IoT acts as the security central point, imposing firewall policies, access control mechanisms, and secure communication protocols.Intrusion Detection and Prevention System (IDS/IPS) Configuration – Open-source IDS/IPS tools like Snort or Suricata are installed to analyze network traffic in real time. These tools employ signature-based and anomaly-based detection methods to alert against suspicious cyber threats. Security alerts are raised by detected anomalies, and automated countermeasures are initiated.
Honeypot-Based Threat Intelligence – A low-interaction honeypot (Cowrie, Dionaea) is deployed in the network to entice and record malicious activity. Attack patterns are examined to optimize firewall rules and access control policies,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404190|

making the system more resilient to changing cyber threats.Secure Remote Access Implementation – An authentication system based on VPN (OpenVPN) is utilized to set up encrypted communication channels. Multi-factor authentication (MFA) is implemented to provide secure remote access, and only authenticated users are allowed to access the IoT network.

Real-Time Monitoring and Logging – Network traffic and security events are monitored in real-time with ELK Stack (Elasticsearch, Logstash, Kibana) or Grafana. These allow real-time visualization of data, threat detection alerts, and detailed log analysis for incident response.

Performance Assessment and Optimization – It is tested for different attack conditions, such as denial-of-service (DoS), attempts at unauthorized access, and packet sniffing. Performance parameters like accuracy of detection, latency, resource consumption, and scalability are assessed. Adjustments are done to make it optimized in terms of efficiency and yet retain a lightweight profile acceptable for resource-limited IoT devices.

V. RESULTS

PiShield is a strong and versatile security gateway that is specifically aimed at the prevention of severe vulnerabilities in IoT networks. By integrating vital security features like firewalls, intrusion detection systems, authentication protocols, and honeypot capability, it offers complete protection from cyber attacks. The addition of device segmentation, additionally, enhances network security by stopping lateral attacks, so that any possible intrusions are confined and unable to spread. In addition, the dashboard, which is accessible through the web interface, provides administrators with real-time visibility and control of network activities, allowing proactive threat management.

The dashboard features an IoT Device Summary that graphically illustrates the status of connected devices and their security state. The Top Attacker IPs feature identifies the most common sources of cyber threats, and through it, administrators can recognize and neutralize potential risks proactively. In addition, Attack Protocol Distribution breaks down different methods of attack using a pie chart, giving key insights into attack patterns. Real-time analytics give enhanced network visibility, facilitate speed in detecting threats, and increase PiShield's capability to enhance network resilience for various IoT applications. As IoT ecosystems expand and develop further, PiShield comes out as an adaptable and future-proof security tool, taking the center stage in building secure, intelligent, and connected spaces.

VI .CONCLUSION

The Pishield framework shows a lean, scalable, and adaptive solution for IoT security that encompasses a secure IoT gateway, intrusion detection and prevention system (IDS/IPS), honeypot-based threat analysis, and VPN-based secure remote access. Utilizing firewall policies, real-time threat monitoring, and multi-factor authentication, the system effectively counteracts cyber threats against IoT networks. The use of Snort/Suricata-based IDS, Cowrie/Dionaea honeypots, and ELK Stack/Grafana monitoring tools improves proactive security, enabling real-time detection, logging, and incident response.

Through performance assessment, the system exhibits minimal computational overhead, rendering it ideal for restricted IoT environments. The honeypot module offers insightful threat intelligence, enhancing firewall policies and network security. The VPN-based authentication mechanism grants secure remote access, reducing unauthorized invasions.
Overall, Pishield provides an efficient and cost-effective solution to IoT security, resolving major vulnerabilities like unauthorized access, malware attacks, and data breaches. Future efforts will be dedicated to improving AI-based threat detection and energy-efficient security mechanisms for large-scale IoT deployments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404190|

VII. FUTURE WORK AND ENHANCEMENTS

Although the PiShield project offers a strong security framework for Internet of Things networks, there are a few improvements that could be made to increase its potency. An important area for improvement is the incorporation of machine learning-based threat detection, which enables AI-driven models to improve automated threat identification by analyzing attack patterns. Additionally, by using smart contracts for authentication and decentralized data storage, blockchain technology can guarantee safe and unchangeable Internet of Things communication. The incorporation of cloud-based security solutions, which allow for scalable security monitoring and real-time analytics through platforms like AWS, Azure, or Google Cloud, is another possible development.

PiShield can implement AI-driven honeypot systems that dynamically adjust to changing attack methods in order to further enhance cybersecurity intelligence. PiShield can be optimized for 5G and edge computing as these technologies gain popularity improve low-latency security processing speed and efficiency. Lightweight encryption techniques will help maintain security without sacrificing performance, and hardware optimization for low-power IoT devices is crucial to guarantee compatibility with battery-powered sensors.

Enhancing the PiShield dashboard with improved visualization tools and automated alert notifications via email or mobile applications for real-time threat response are further ways to improve the user experience. Additional layers of protection can be added by bolstering authentication procedures with biometric security measures like fingerprint or facial recognition in addition to sophisticated VPN-based authentication. PiShield's credibility and security policies will be further strengthened by compliance with international cybersecurity standards, such as GDPR, NIST, and ISO 27001. Furthermore, by connecting PiShield with international cybersecurity platforms, threat intelligence sharing can be increased, which can enhance its capacity to identify and reduce complex cyberthreats.

With these improvements, PiShield can develop into a more intelligent, scalable, and efficient security solution, guaranteeing strong defense for IoT networks in a constantly changing cyberthreat environment.

REFERENCES

1. S. Sharma and R. Gupta, "A Study on IoT Security Challenges and Solutions," *International Journal of Computer Applications*, vol. 182, no. 12, pp. 25-30, 2022.
2. M. Ahmed et al., "Intrusion Detection in IoT Networks using Snort and Suricata: A Comparative Study," *Journal of Network Security*, vol. 9, no. 3, pp. 110-120, 2021.
3. T. Brown, "Honeypots for Cybersecurity: Analyzing Threat Intelligence," Cyber Defense Review, vol. 7, no. 1, pp. 50-65, 2020.
4. A. Patel and J. Kumar, "Enhancing IoT Security with VPN and Multi-Factor Authentication," *IEEE Transactions on Secure Computing*, vol. 19, no. 4, pp. 1425-1438, 2022.
5. K. Lee et al., "Real-Time Threat Monitoring in IoT Networks using ELK Stack," *Computers & Security*, vol. 104, no. 6, pp. 88-101, 2021.
6. P. Singh and L. Rao, "Lightweight Cryptographic Techniques for IoT Security: A Comparative Analysis," *Journal of Information Security and Applications*, vol. 56, pp. 102-115, 2022.
7. R. Gonzalez, "Energy-Efficient Security Mechanisms for IoT Devices," *ACM Transactions on Embedded Computing Systems*, vol. 20, no. 5, pp. 1-20, 2021.
8. H. Kim et al., "Routing Security Challenges in IoT Networks and Solutions," *Wireless Networks Journal*, vol. 28, no. 3, pp. 423-438, 2022.
9. S. Das and P. Roy, "Adaptive Firewall Policies for IoT Networks: A Security Perspective," IEEE Internet of Things Journal, vol. 10, no. 1, pp. 212-225, 2023.
10. J. Wilson, "The Role of Secure IoT Gateways in Cyber Defense," *Cybersecurity and Privacy Journal*, vol. 5, no. 2, pp. 66-80, 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details