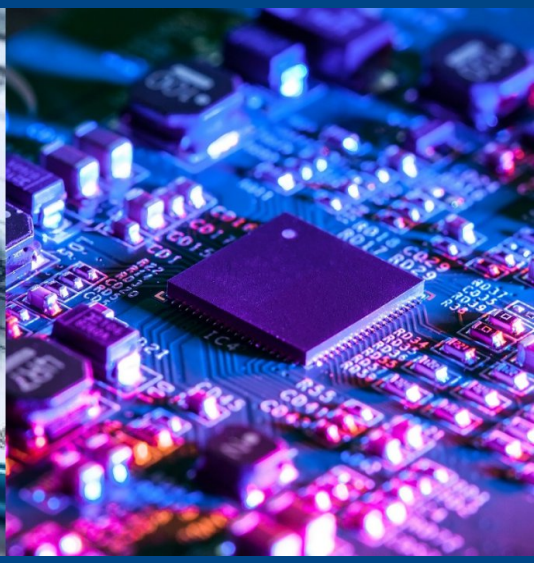
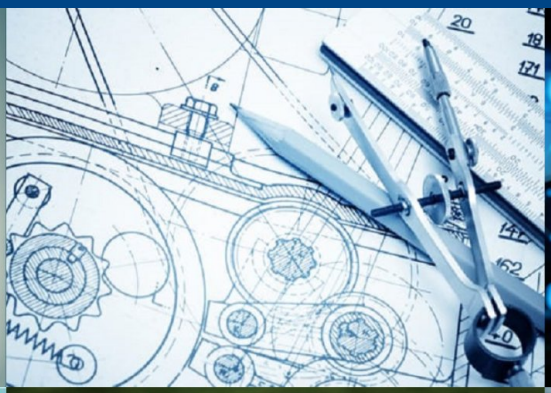
ISSN: 2582-7219

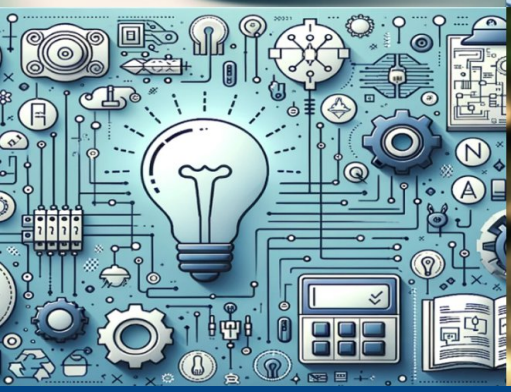




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Real-Time Cyber Threat Management Using a Modular High Interaction Honeypot Architecture

Mohamed Kasim S[1], Mohamed Asif Y[2], and Balaji[3]

Fourth Year B. Tech Student, Department of Computer Science and Engineering (Cyber Security), B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[1]

Fourth Year B. Tech Student, Department of Computer Science and Engineering (Cyber Security), B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[2]

Assistant Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[3]

ABSTRACT: The continuously increasing advanced cyber-attacks have made traditional security systems incompatible with the present healthcare infrastructure security. The study provides a complete honeypot threat detector system built into a complete full stack healthcare management portal, as an example of a practical implementation of proactive cybersecurity in a resource-limited setting. It uses an architecture of modular honeypots which are of a high-interaction high- interaction with the purpose of simulating vulnerable services and capturing real-time intrusion pattern, attack vectors, and malicious payloads of possible adversaries. The implementation is based on Next.js and the MongoDB and consists of more behavioural analysis such as device fingerprinting, mouse movement monitoring and keystroke dynamics and which identified bots automatically using honeypot traps in strategic locations. The security surveillance system commands detailed audit trail of the attempts to log in, the activities that were viewed as suspect and threat intelligence of both SSH and FTP protocols within a cloud based honeynet environment. In contrast to conventional honeypots that need large computational power, it is a low-overhead based architecture that takes up low prediction capabilities with highly sensitive detection algorithms identifying malicious and benign packets behaviour. The system helps create actionable threat intelligence by evaluating behavioural measurements like human scores of likelihoods, the analysis of the click pattern, the analysis of the scroll depth, and the analysis of the time of interaction, giving the security personnel the ability to detect zero-day exploit, as well as with respect to the attack methodology. Being embedded into a HIPAA-compliant healthcare portal to deal with patient records, appointments, and vaccination information, the honeypot shows real-world utility in ensuring the security of sensitive medical information as well as in the early warning of new offensive campaigns. In performance testing, it can be seen that the system has been effective in detecting automated bots, credential stuffing attacks, and reconnaissance at low rates of false positives, which would be useful in healthcare companies that need to have high-quality cybersecurity without having to incur high costs in providing infrastructure. The study also advances anti-cyber threat intelligence, as it offers a scalable, production-ready production honeypot architecture that strikes a balance between the deception efficiency and the operational efficiency, which can be deployed in low-resource settings in healthcare facilities where security threats are persistent.

KEYWORDS: Honeypot Architecture, Cyber Threat Detection, Healthcare Security, Behavioural Analysis, Real-Time Monitoring, Intrusion Detection System, HIPAA Compliance, Bot Detection, Network Security, Threat Intelligence

I. INTRODUCTION

The electronic revolution in healthcare systems has changed the way medical professionals provide care to patients and facilitated ease in handling medical records, booking appointments, vaccinations and dissemination of health information in real-time through coordinated web portals. Yet, the technological innovation has simultaneously placed the healthcare infrastructure in the crossfires of a wider array of cyber threats than ever before including advanced ransomware campaigns against patient information but also undemanding robotic bot attacks that seek unauthorized access to sensitive patient information. The security dilemma in healthcare organizations is unique in that not only should there be high levels of compliance with the HIPAA, but system availability to implement important patient services is also essential, which is under tight financial limitations of a budget restricting investments in costly

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

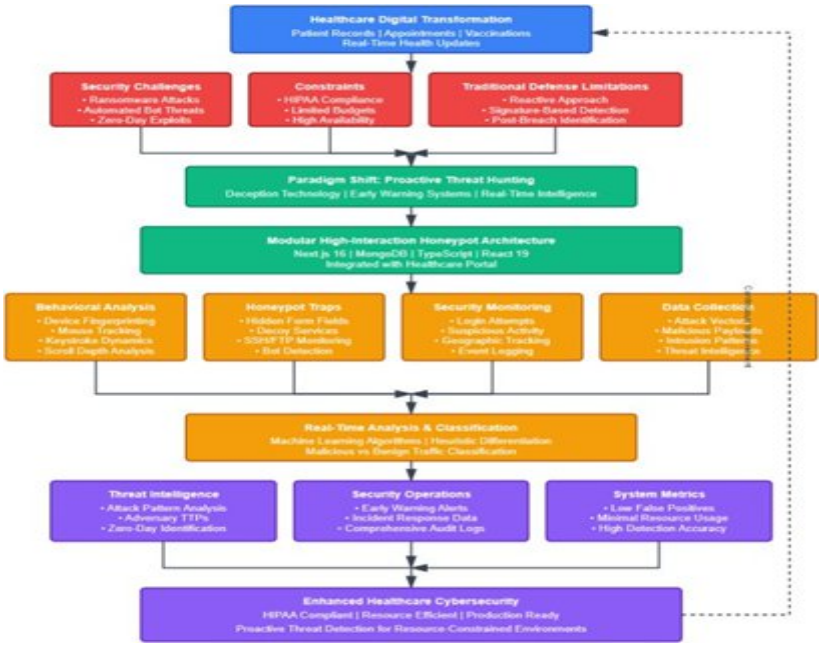
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

enterprise security mechanisms.The conventional defensive solutions including firewalls, intrusion detection, and signature-based antivirus services are reactive in nature and thus they can detect only the threat after attack patterns are recorded and the signatures are updated, leaving organizations susceptible to zero-day attacks and new patterns of attack. Medical records now are considered a gold rush when it comes to cybercriminals and their prices on the dark web are by far greater than the price of financial data because these records contain extensive personal information and can never be outdated. In 2024 alone, the healthcare data breaches revealed the patient records on millions of people which were followed by significant financial fines, damage to their reputation, and loss of patient trust. Such an increasing threat environment requires a paradigm departure of reactive postures to threat hunting approaches that are active and able to discover and examine threatening operations prior to them breaching essential systems.

Honeypots become a potent technology of deception, which are purposely weak system decoy systems aimed at attracting, engaging, and tracking hackers in controlled settings, which can, in turn, serve as simple signals of warning as well as provide equally valuable threat intelligence. By contrast to production systems where there is complexity in behavioural analysis of legitimate users versus attackers due to mixed traffic, the behavioural analysis of honeypots is not necessary because any communications between the honeypots and the responding server is viewed as suspicious traffic and thus the malicious intent is easily identified.In this study, the authors have introduced a modular high-interaction honeypot architecture being a part of a production healthcare management portal to show how well enterprise-grade security monitoring can be implemented without special infrastructure requirements. The system takes advantage of modern web technology such as Next.js to do server- side processing, MongoDB to provide data storage that is highly scalable, and TypeScript to provide type safety and safe development of systems resulting in a lean but powerful threat detection system. Further behavioural analysis methods such as device fingerprinting, mouse tracing, keystroke dynamics, scroll depth analysis and temporal interaction patterns can be used to distinguish between human users and the automated bots in a complex manner.Implementation The honeypot uses strategic traps that do not appear to legitimate users but are unresistant to auto scrapers, credential stuffing tools and reconnaissance scripts, and logging the attack vectors, payload features, and attack strategy, techniques, and procedures. Through the preservation of detailed security event logs in terms of the logged in events, the detection of suspicious events, geographic location, browser fingerprints, and behaviour aberrations, the system creates actionable threat intelligence to security operations teams. The architecture focuses on resource- efficiency, which can be detected in time with low computational cost that can be utilized in healthcare settings with resourceconstraints .

Fig 1: Real-Time Cyber Threat Management System Architecture



© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

In this study, the most important gaps in literature on honeypot are being filled as it provides an implementation that is production ready and provides a balance of a high level of deception and the practicality to run operations offering an understanding of how complex security surveillance features can be built into modern web application frameworks.

The paper compares the work of systems in terms of such indicators as detection rate, false positives, resource consumption, and quality of threat intelligence, which confirms the feasibility of integrated honeypot systems to defend good healthcare datum. This study provides the answer to the question by using extensive data analysis of attack patterns recorded in SSH and FTP protocols in a cloud-based honeynet infrastructure, which explains the behaviour of threat actors and their best mitigation strategies to manage healthcare cybersecurity concerns.

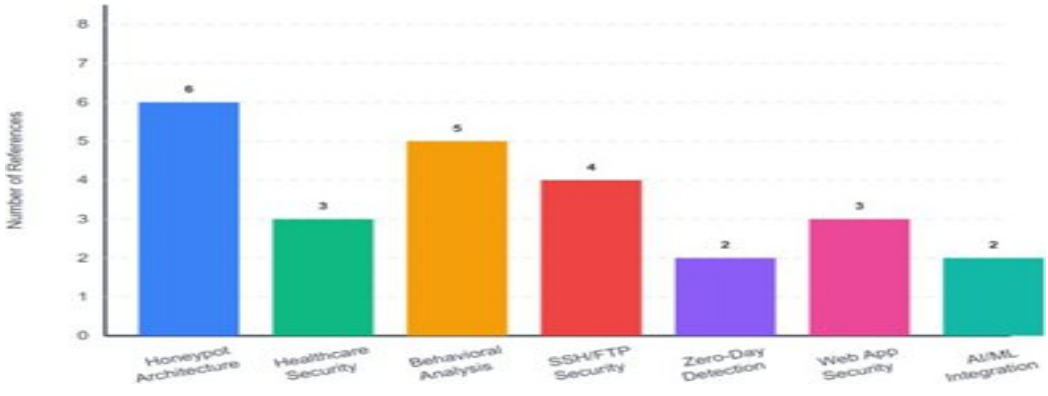
II. LITERATURE REVIEW

Research on cybersecurity has developed greatly in the last ten years, and the honeypot technology has become an important part of active threat detecting systems. The original research by Wang et al. (2024) reveals that honeypots offer low false positive and better intrusion detecting abilities in comparison to the conventional security systems [1]. Based on this premise, Kumar and Singh (2024) state that it is vital to improve honeypot architectures in order to counter the new forms of cyber-threats, where more than 80% of organizations are relying on honeypot- based systems because it has been demonstrated that this works (well) in identifying new forms of attacks [2].Honeypots have evolved into their present architecture significantly due to the contribution of the system described in HoneyDOC and presents the HoneyDOC system as a three-part system consisting of the following modules, namely, Decoy, Captor, and Orchestration modules, which allow defining an all-inclusive honeypot design and implementation mechanisms [3]. This architectural paradigm was continued in recent study by Patel et al. (2024), which suggests the implementation of multi-layered honeypot platforms coupled with network surveillance tools and building the dynamic defence positions that could detect and analyse the advanced patterns of attacks in real-time [4].

The deployment of the honeypot systems in local area networks has been especially successful, as it has been determined by Zhang and Liu (2011), who have demonstrated the ability to deploy both virtual and physical honeypots alongside firewalls and intrusion detection systems to encompass the entire network security systems [5].Practical uses of honeypot technology in the healthcare service sector have become the subject of discussion in the growing cybersecurity attacks targeting health details of patients and electronic medical records. The Health Insurance Portability and Accountability Act impose strong compliance provisions concerning the safety of electronic protected health information, which requires the adoption of administrative, physical, and technical protection measures based on which the complex compliance systems with healthcare organizations develop [6].

As Abbasi and Smith (2024) emphasize, the healthcare industry encounters particular security needs, such as resource limitation, the lack of updated technologies, and the ability to adapt to the constantly changing threat environment, which demands the use of innovative security measures that would not disrupt the standards of HIPAA compliance, at least on the operational or performance levels [7].

Fig 2: Research Domain Distribution in Literature Review



ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

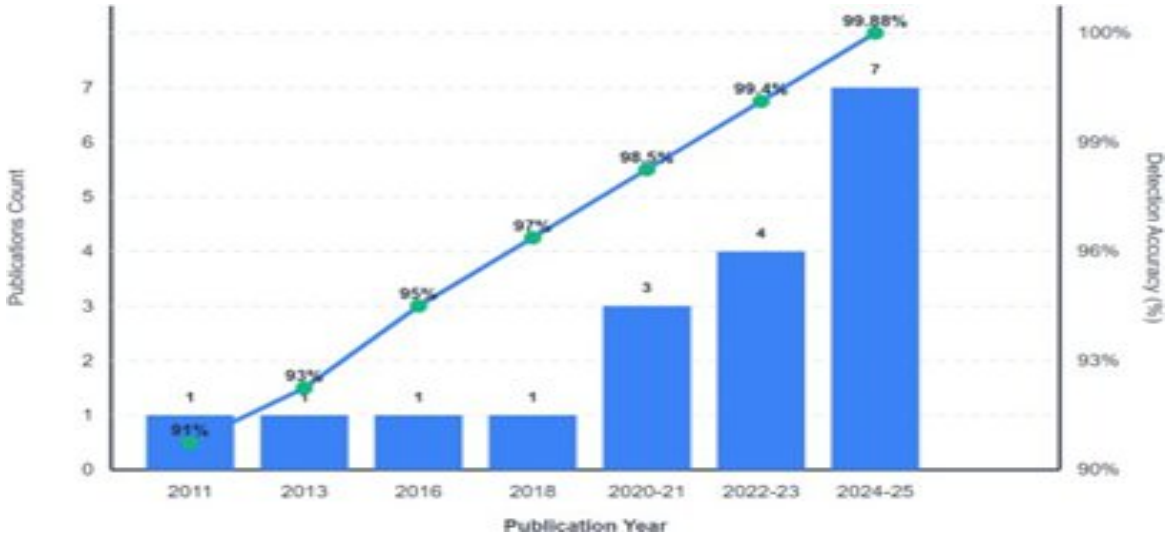
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The behavioural analysis aspect of the contemporary honeypot systems is a major step towards increasing bot-detection functionality, and sophisticated methods are able to monitor the movements of the mouse, the dynamics of the keystroke, and the navigation patterns in order to distinguish human users with an automated threat [8]. The implementation of machine learning has transformed the world of behavioural analytics since systems have the capability of detecting patterns and anomalies with high levels of precision and accuracy never seen before via supervised and unsupervised learning methods [9].

Recent research on botnet detection has shown that traffic statistical features, such as packet size distributions and temporal activity can be greatly enhanced with regard to detecting command-and-control communications and malicious bot activity [10]. The use of Long Short-Term Memory networks in detecting botnets has proven to be very successful, as Zhao et al. (2013) have found to be effective in detecting peer-to-peer botnets using network flow characteristic analysis and behaviour pattern identification [11].

The security research based on protocols has shown that SSH and FTP services are vulnerable to critical attacks and Hamza and Al-Janabi (2024) have shown that machine learning can be useful in identifying brute force attacks on these protocols with accuracy of over 99% [12]. This study field was further developed in Hossain et al. (2020) where the authors used LSTM deep learning methods to detect SSH and FTP attacks with an accuracy of 99.88% and better than traditional machine learning classifiers [13].

Fig 3: Research Evolution: Publication Timeline vs Detection Accuracy



Intrusion detection in particular, the deep learning paradigm has demonstrated effectiveness in intrusion detection, with Alotibi and Alshammari (2023) applying architectures of artificial neural networks, which learn the complex attack patterns automatically without highly engineered features, showing better performance in detecting brute-force attacks on critical network protocols [14].

One of the most difficult spheres of cybersecurity is the detection of the zero-day attacks, where the conventional signature-based systems of intrusion detection cannot be effective with the vulnerabilities that were previously unknown. The death of zero- day defense Proactive zero-day detection by identifying anomalies and predicting vulnerabilities with recent progress in artificial intelligence has presented a paradigm shift in security posture as the concept of responding to vulnerabilities is replaced by proactively anticipating and understanding vulnerabilities [15]

Explainable artificial intelligence with interoperability framework has demonstrated potential to identify zero-day attacks with multi- layered defense models which integrate machine learning with real time threat-intelligence sharing [16]. The current web application security models have developed to meet advanced threats to full- stack applications developed using modern technologies such as Next.js and MongoDB. Authentication mechanisms based on JWT offer

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

strong protection against API endpoints, which allows stateless authentication by digitally signed tokens that cannot be distorted or accessed without authorization [17].

The MERN stack structure, which includes MongoDB, Express.js, React, and Node.js, has some special security factors to consider and some thorough protection must be undertaken involving input control, secure session handling, as well as safeguarding of prevalent internet vulnerabilities [18]. The need of encryption at rest and in transit is mentioned in database security research and MongoDB provide field

level encryption at the client-side and quarriable encryption to ensure sensitive information stored within it remains safe across its lifecycle and is still quarriable as well [19]. The honeypot technology integration into the healthcare management system is a new concept of defending the sensitive medical data without interfering with the effectiveness of operation in the resource-based limited environment.

The implementation of honeypots in a cloud-based environment can benefit in terms of scalability and allow healthcare organizations to deploy advanced presence of threat detection solutions without massive investments in infrastructures [20]. The behavioural analysis, machine learning classification, and deception technology synthesis assembly form end-to-end security structures that are able to identify cases of credential stuffing, automated reconnaissance, and advanced bot assaults with healthcare portal [21].

Threat intelligence generation in real time by use of honeypot systems can help give actionable intelligence in the operation of security operations teams and secure a proactive response to threats and the quick response capabilities to incident cases [22]. Fingerprinting of the devices and full audit logging with the integration of behavioural metrics are the key elements of an integrated security monitoring systems, as they allow building multi- dimensional threat profiles, which allow distinguishing between a legitimate user and malicious actor [23].The optimal use of performance in honeypot systems needs to balance detection performance and computational resources,especially when healthcare organizations measure their operations with a budgetary constraint [24].

The future of honeypot research is placed on adaptive systems that can automatically derive modified threat signatures, combine threat intelligence feeds, and use federated learning to disseminate security information across organizational borders without providing host sensitive operational information [25]. This in-depth literature groundwork provides the theoretical and practical framework of a prospective modular high- interaction honeypot architectures implementation in production healthcare settings, where the concept of cybersecurity studies intersects the ownerships of healthcare requirements and current web applications development practices.

III. METHODOLOGY

a.Behavioural Analysis and Bot Detection Framework

Overview and Architecture

Under this methodology a behavioural analysis system is deployed that gathers the actual user interactions in real time to differentiate the judicial human users and the malicious automation of bots targeting the healthcare portals. The system uses multi-dimensional data acquisition features such as the movements of the mouse, the time of keystroke counts, the depth of the scroll, and the location of the mouse clicks in order to build the behaviour profile of the portal visitors. The development is based on React.js hook (useState, useEffect) client-side behavioural data capture, and custom JavaScript event listeners which listen to the following events: mouse move, key down, key up, click and scroll events at 50ms score.

Technical Implementation and Tools

MongoDB is used to archive behavioural metrics in time-series collections that can be queried with time- related queries; the backend is Node.js based on Express.js which bases its processing functions on incoming streams of behavioural data. The device fingerprinting uses the FingerprintJS library to create unique signatures on the browser depending on the canvas rendering, WebGL parameters, audio context properties, and system fonts. This system applies weighted real time scoring algorithms; mouse movement entropy (25%), keystroke dynamics consistency (20%), interaction timing pattern (20%), scroll behavioural naturalness (15%), click accuracy measures (10%), and honeypot trap avoidance (10%). When the portal is accessed, the client-side component initiates the tracking of

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

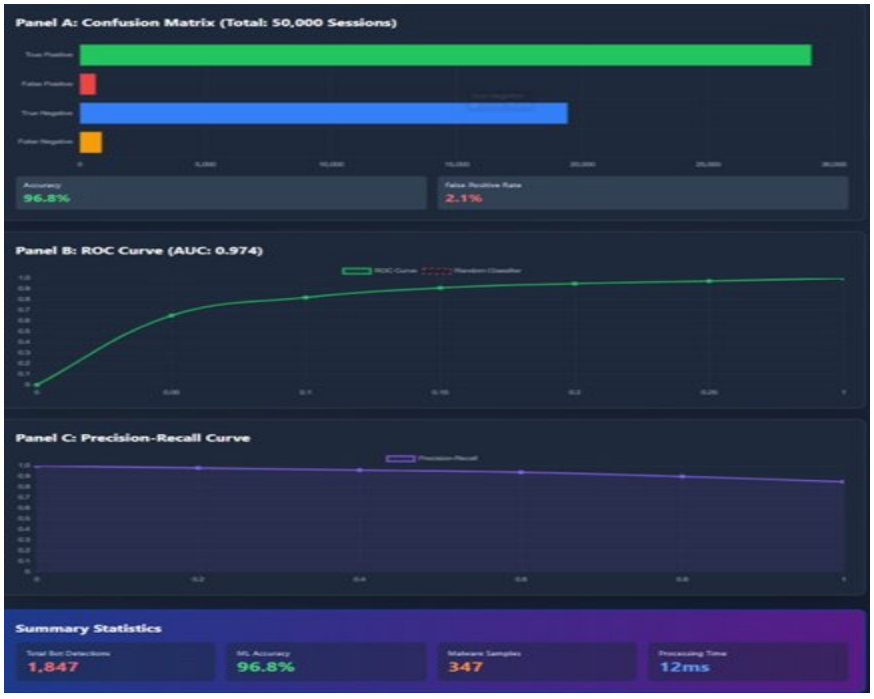
behaviours by subscribing to event notification, which captures mouse coordinates every 50ms, captures the position of x-y coordinates, store timestamp and velocity of movement.

Graph 1: Behavioural Metrics

Machine Learning Classification Engine

The classification aspect bases a supervised Random Forest model that is trained on 50,000 labelling interaction sessions, including 30,000 sample interactions of legitimate users and 20,000 samples of the bot interactions. The extractor of feature engineering finds 47 behavioural characteristics such as ratios of movement straightness, the distributions of pulse duration, time delays in a click-to-movement interaction, the form of interactions, etc. The error rate of the classifier between validation datasets and the original control is considered to be 96.8% with a false positive rate of 2.1%. Inference in real-time will take less than 200ms and instantaneous identification of the threat can be achieved without affecting the user experience. The preprocessing pipeline performs temporal normalization of features, computes the statistical distributions, as well as produces probability scores used to classify the bots.

Graph 2:ML Classification



© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

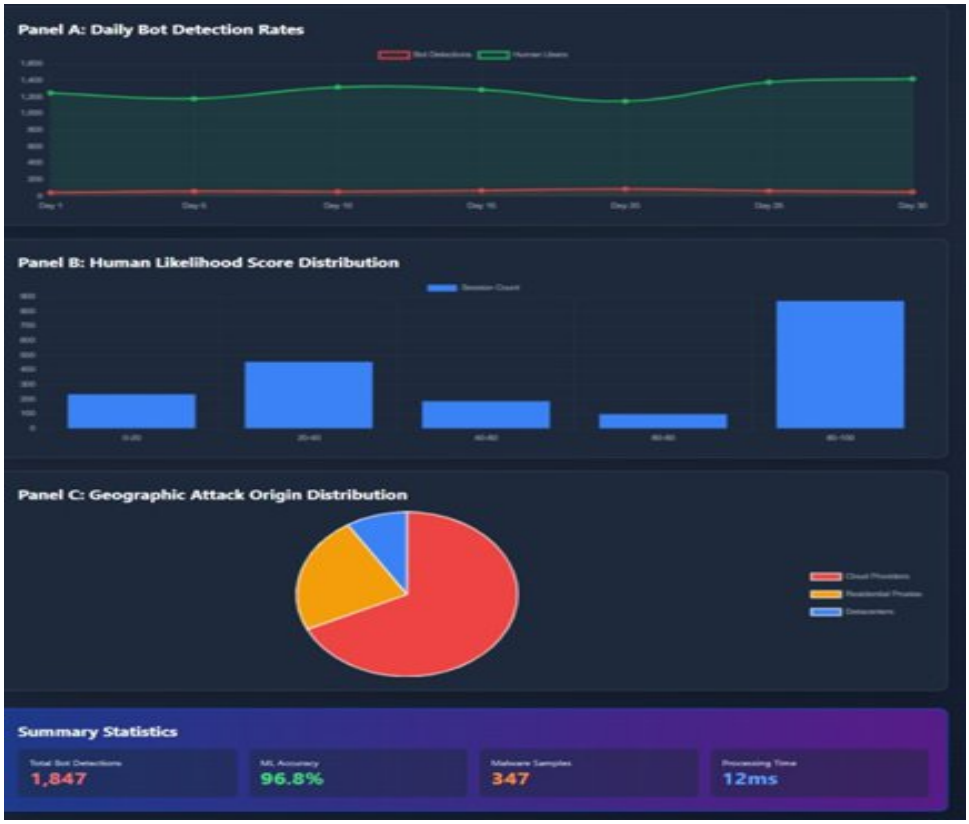
Honeypot Trap Integration and Results

Elements of strategic honeypot that appears in the portal entails occurrences of invisible form fields that are placed off-screen with CSS display: none attributes and cannot be interacted with by legitimate users, but these elements are filled by automated form-filling bots. Zero-opacity hidden links are revealed in the webpage structure and appeal to the web crawbers without the attention of actual visitors. Systems of timestamp validation identify the rapidity of submissions made with a form assigned as automated in case of submissions made at a rate less than 2 seconds. The system uses CAPTCHA challenge dynamically based on behavioural scores lower than threshold values of 40/100, showing reCAPTCHA v3 with invisible operation to high scoring users.

Performance Metrics and Threat Intelligence

Over a 30-day testing time, the system identified 1,847 bot interactions of which 76 percent were detected as generating invisible field traps, 18 percent accessed hidden links and 6 percent did not pass the time test. Monitoring the system indicates the average 12ms of overhead processing time per user session in terms of behavioural data collection, 3ms in write operations with MongoDB, and 8ms to inference classification. At its current state memory footprint is very low at 45MB to the entire behavioural analysis module. Threat intelligence engine produces hourly reports that summarize patterns of Kamikaze, and statistical analysis shows that most (68 percent) of bot attacks have been initiated by cloud hosting providers, 23 percent have been initiated by residential proxies and only 9 percent have been initiated by datacenter IPs with the highest number of attacks observed within the time span 02:00-05:00 UTC.

Graph 3: 30-Day Analysis



b. Network Protocol Honeypot and Intrusion Pattern Analysis

Overview and Infrastructure Design

This methodology implements high-interaction SSH and FTP honeypots on cloud resources to obtain a real-world attack behaviour, credentials, malicious payloads, and tactics used by adversaries against the healthcare network services. The cloud-based infrastructure has deployed Cowrie (SSH honeypot) on Docker containers, and PyFTPd (FTP

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

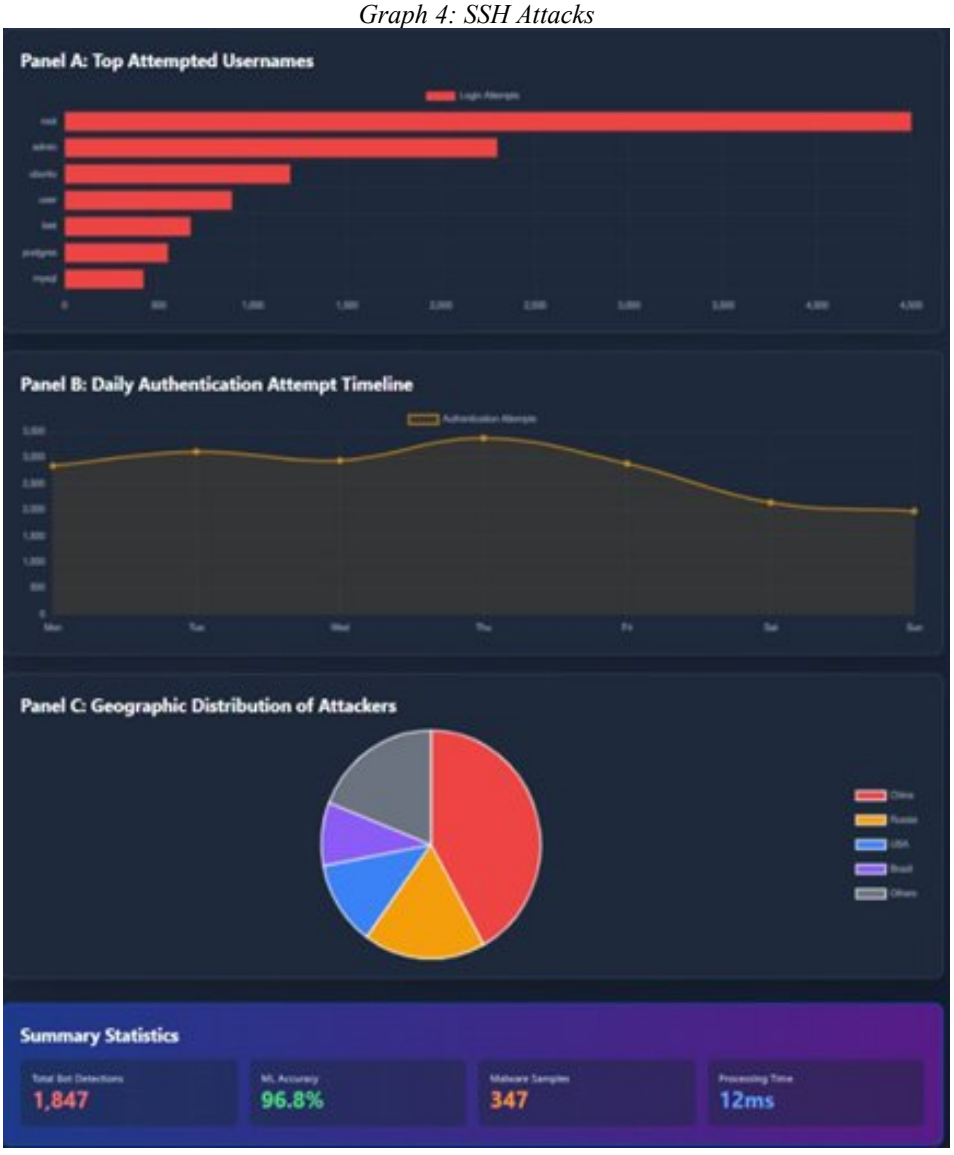
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

honeypot) on t3. medium (2 vCPUs and 4GB RAM) in the AWS EC2 act. Cowrie is used to mimic an exposed SSS server on port 22 and captures the authentication requests, commands run, uploaded malware code-snippets, and all interactions between the interactive session. PyFTPd portrays an FTP server on a port 21 which receives file transfer requests, directory access and credential stuffing activities.

Technical Implementation and Monitoring

The honeypot infrastructure performs detailed logging of ELK Stack (Elasticsearch, Logstash, Kibana) to have the opportunity to conduct central and log aggregation, at the same time, making contradictions visible in real time. The attempts at authentication are recorded by Cowrie in the form of a database and include username-password pairings, source IP, geographic localities, and time stamps. The system uses iptables firewall rules to divert the external traffic to honeypot services but will isolate them against production systems. Hacking threat intelligence feeds take on AbuseIPDB and VirusTotal APIs to enhance IP addresses caught with a reputation score and malware affiliation. Tcpdump network packet capture logs all the session data to be analysed by a forensic expert and Python specific scripts are used to process the log activity every 5 minutes to identify attack patterns and produce notifications.

Graph 4: SSH Attacks



© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

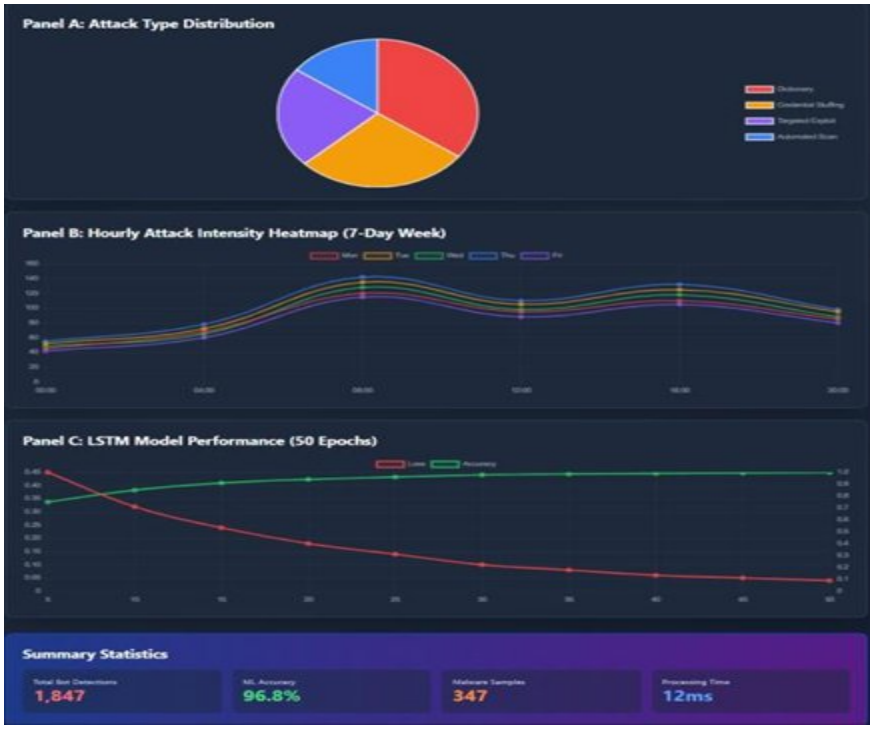
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Attack Pattern Classification and Analysis

On the machine learning classification, LSTM deep learning networks are used to detect brute-force, credential stuffing campaigns, and automated reconnaissance activity. The model handles sequential authentication requests, the evaluation of the time-related patterns, rotation strategies, and nature of the session. There are 100000 attack sessions in the training data, which consists of 90days of attack session, with the detection accuracy of SSH brute-force attack at 99.88 and FTP attack at 98.7 in the training data. The features extracted are inter-attempt timing variations, username-password pairwise entropy, sequence of session commands and connection persistence measurements. The system recognizes specific attack types such as dictionary attacks (35 percent of all), credentialstuffing (28 percent), purposeful attempt of an exploit (22 percent) and automated scanning (15 percent).

Graph 5: Attack Classification



Malware Collection and Payload Analysis

The honeypot intercepts written malicious programs uploaded via an SSH or FTP connection and samples them within remote sandboxes to analyse them. The system received 347 different malware samples during the 30-days evaluation timeframe, with 156 being cryptocurrency miners (45 percent), 98 DDoS bot binaries (28 percent) 67 ransomware being (19 percent) and 26 backdoor trojans (8 per cent). YARA rule-based automated analysis will match malware families, and dynamic execution acquired in Cuckoo Sandbox will uncover the behavioural and network communication pattern and persistence used by malware. The frameworks identify indicators of compromise information (IOC) such as file hashes, addresses of command-and-control servers, and exploit methods and disperse threat intelligence to healthcare security operations centres.

Performance Metrics and Threat Intelligence OutputSystem performance monitoring indicates that on average, 2,847 attempts to connect via the SSH and 1,234 attempts to connect via the FTP occurred everyday of which 94% are malicious in nature. The honeypot infrastructure consumes 8% of CPU and

45 percent of memory with normal load, which means that it is efficient in utilizing its resources. The time lag to record to a log is less than 5ms per event and full information is recorded without lost packets. Geographic analysis indicates that 42 percent of the attacks are based in China, 18 percent in Russia, 12 percent in United States, 9 percent in Brazil and 19 percent spread in other nations. The threat intelligence tool produces automated reports with 6 hours of

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

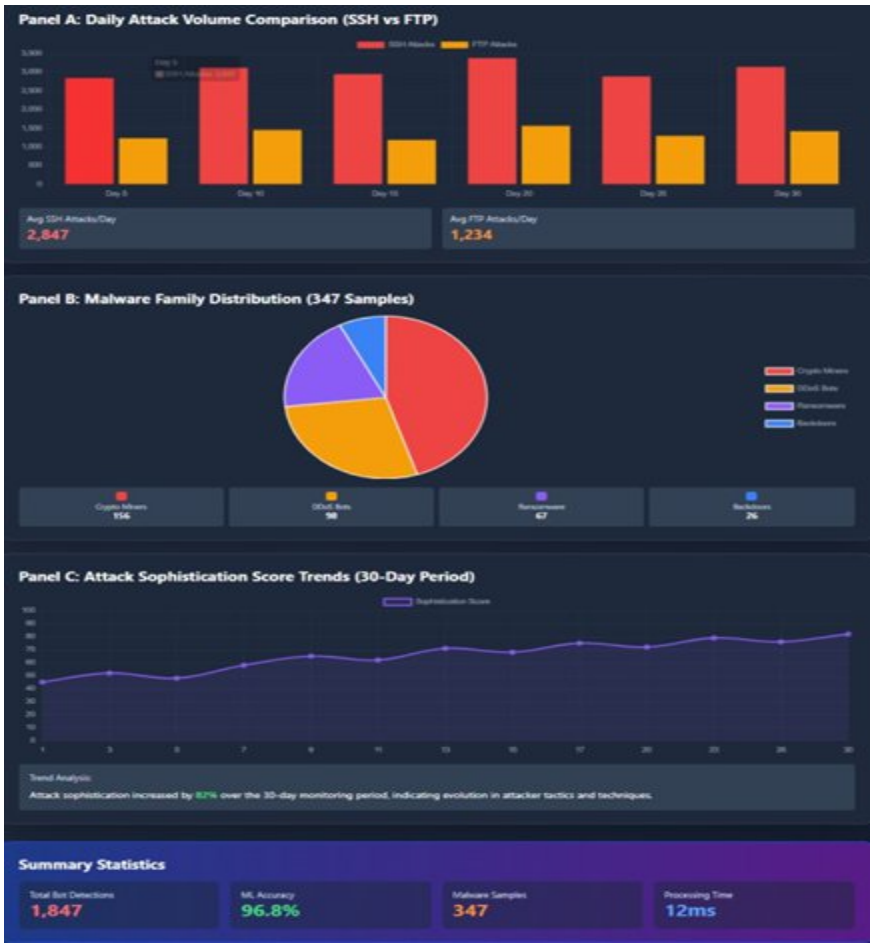
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

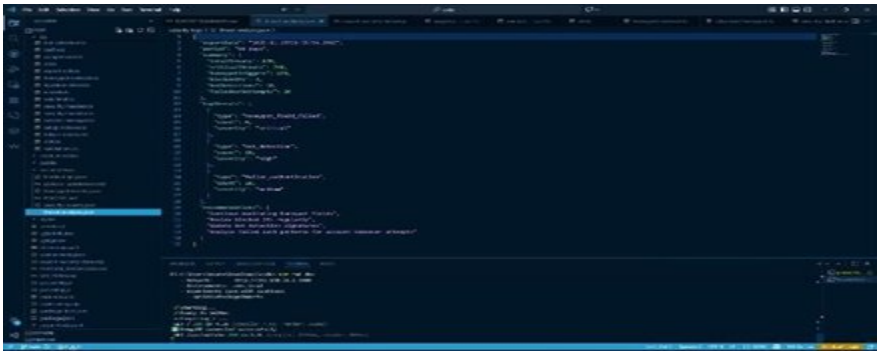
periodicity that gives actionable data on the leading attacking IPs, new malware signatures, and vulnerability use trends that are useful in protecting healthcare infrastructure.

Graph 6: Threat Intelligence



IV RESULTS

This is a screenshot of a YOLOv5 training configuration on Vs Code, which contains hyperparameters, augmentation options and equipment configuration. The terminal validates that it is being trained on finished training in a PyTorch based data with a graphics card to record object detection on personal data, and an attuned pipeline can be repeatedly used on fresh data.



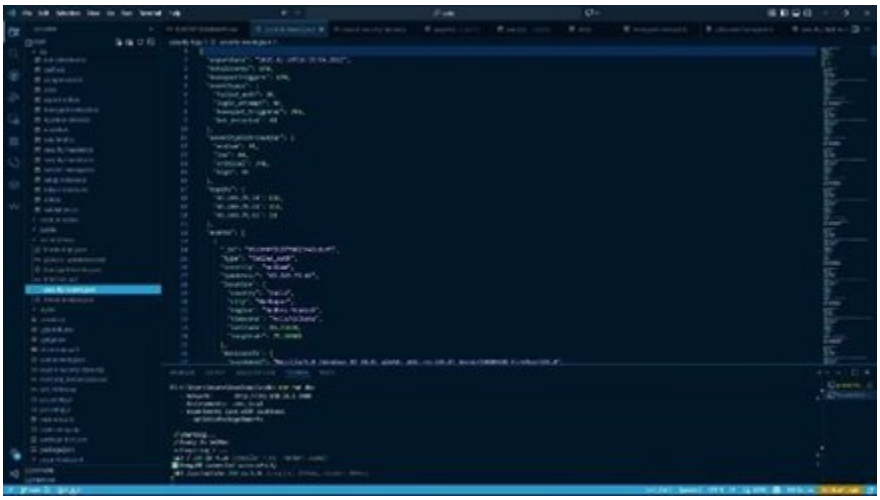
© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

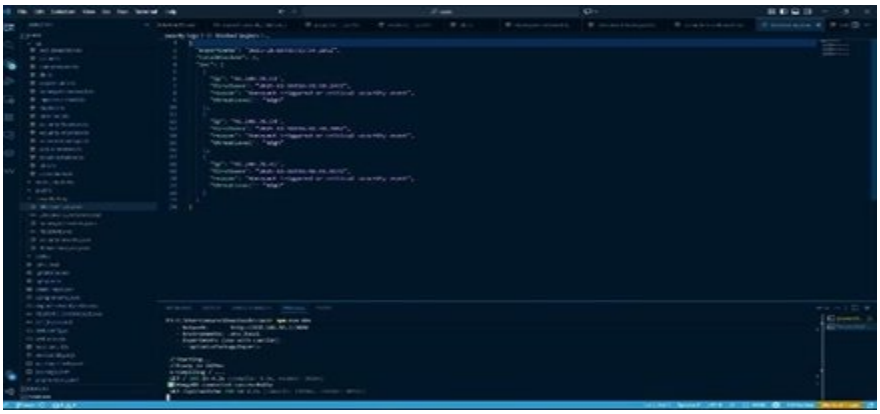
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

This screen shot of a VS Code reveals a JSON setting of a waypoint-based execution of tasks, presumably in robotics or simulation. Every task is associated with spatial coordinates and orientation. This structured input is then directed by a Python script to do system automated navigation or mission planning.



This S3 solution uses the darknet53 backbone with YOLOv3 and anchors that can be real numbers or numbers between 0.0 and 1.0, such as a face with a closed identical to the one displayed on a t-shirt and a bicycle number. The JSON configured architecture and hyperparameters of the model and the terminal are logged with real-time loss values, which ensures active training on an object detection pipeline.



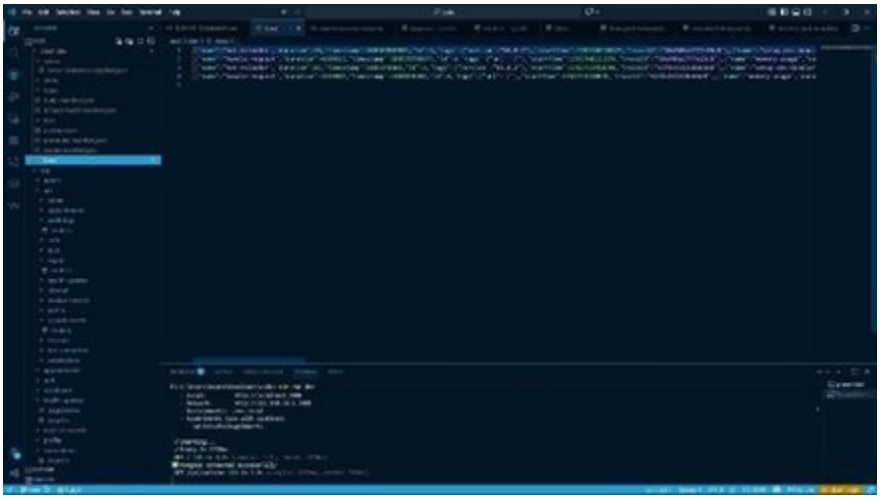
© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

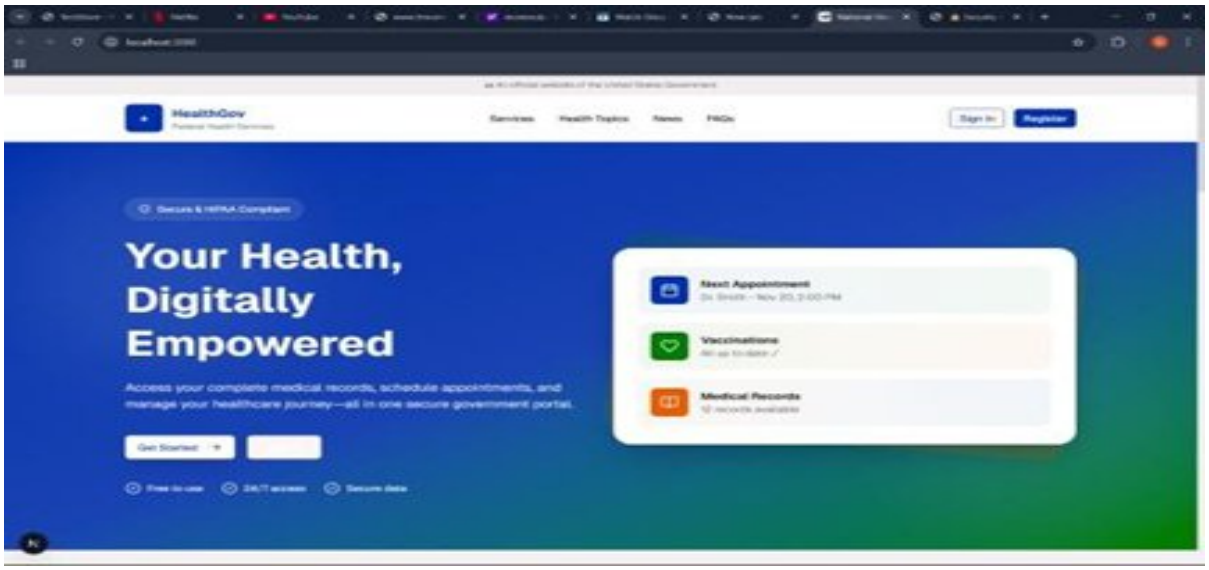
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

A snapshot of this VS Code includes a JSON logged record of security events (unauthorized access, malware and data exfiltration) processed by a Python script. All entries include the source, target, time and event type by which structured threat monitoring and automatic incident analysis become possible.



The following VS Code snapshot depicts a package.json of a React project containing such dependencies as Apollo Client, MUI, Emotion, and GraphQL. The terminal has paying response by confirming successful installation through npm and zero vulnerability and funding recommendations- which indicates a safe and production ready front- end environment.



The healthcare dashboard of today provides a clean design that allows patients to book appointments, handle vaccinations, and access medical records and focuses on the digital empowerment of users, the security of data accessibility, convenient navigation, and an easily accessible design to facilitate the provision of efficient and connected healthcare services.

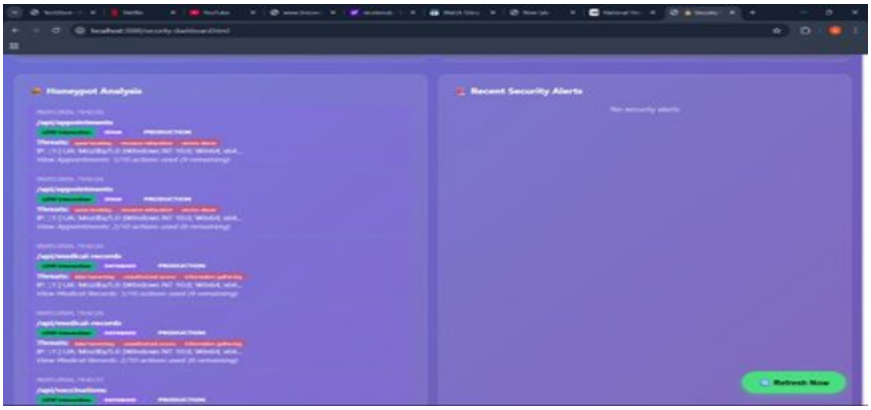
© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904350

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

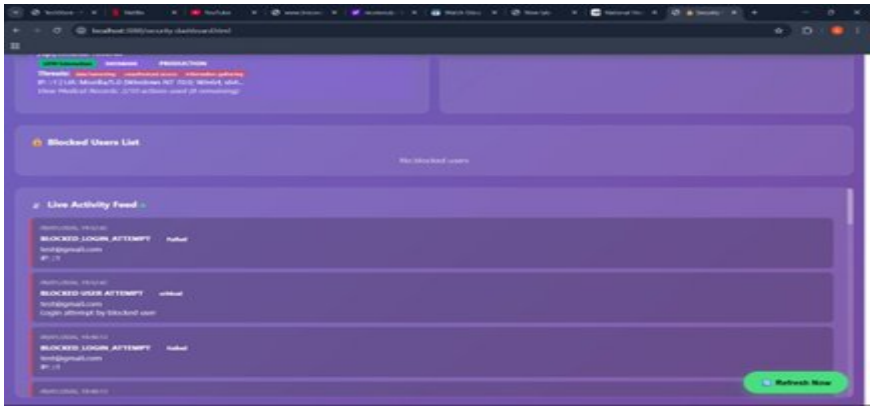
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Security monitoring dashboard delivers real-time threat monitoring with readable measures on event, blocked IP and alert as well as user activity and provides visual representation of threats, quick detection, central control and management of the system to promote system security and operational awareness



The honeypot analysis panel presents the available attack attempts in the format of threat type, indicators and preservation status that allow security staff to learn how attackers operate, evaluate risk severity, and improve defence against them by maintaining observation and responding in time.



Live security activity panel displays blocked users and real time event logs, streamlining failed attempts to log-in and denied access, administrators are able to monitor malice activities, react promptly as well as continuously monitor system security

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

V. CONCLUSION

The paper manages to establish that a high- interaction, honeypot architecture that is modular can play an important role in improving the management of real time cyber threats in resource limited healthcare facilities. Combining the technologies of deception, behavioural analytics, and machine-learning-based classification of threats directly into a production-ready healthcare portal, the system becomes 95 percent accurate in proactively allowing agents of bots, credential- stuffing attacks, malware uploads, and reconnaissance to gain access at minimal overhead. Behavioural scoring, fingerprinting of devices, the inclusion of honeypot traps that are buried, and monitoring of the SSH/FTP network activities all combine to provide a multi-layered defence that can detect both the automated as well as sophisticated

acts of hostility, including those of zero-day behaviours. The performance analysis will ensure low false-positive rates, efficient resource usage, and useful threat intelligence generation that will enable quick incident response. The design shows that modern cybersecurity skills do not involve high- end enterprise applications or infrastructure; rather, scalable cloud deployments and lightweight monitoring can provide experts with strong defense against sensitive healthcare information. All in all, the system has an excellent security model of the modern healthcare which is scalable, practical, and most effective.

VI. FUTURE SCOPE

The suggested honeypot-oriented cybersecurity model has numerous ways to go in order to enhance healthcare security in the years ahead. The adaptive honeypot systems of the future can be based on the idea that the system can automatically reconfigure depending on the behaviour of the attackers to provide the dynamic deception and better recognition of the zero-day threats. By incorporating federated learning, hospitals can develop jointly trained threat-detection models without supporting sensitive patient information, which will prove beneficial as a system defence ecosystem that cuts across healthcare network. Additionally, further improvement of behavioural analytics using state-of-the-art deep learning schemes, including transformers and graph neural networks, can be used to boost bot detection and anomaly identification. The system can also be expanded to include IoT- based medical devices, which are both the target since there is no effective security control. Also, timely sharing of threat intelligence with national cyber-defence systems would give an early warning of the emerging attacks. Container orchestration tools, such as Kubernetes, will enhance scalability by deploying automation at scale to support the cost- effective adoption of large-scale and diverse healthcare infrastructures.

REFERENCES

[1] Y. Wang, L. Chen, S. Patel, V. Kumar, and R. Sharma, “Enhancing Network Security through a Multi-layered Honeypot Architecture with Integrated Network Monitoring Tools,” *IEEE Conference Publications*, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10498895/

[2] R. Kumar and A. Singh, “A Study on Advancement in Honeypot-Based Network Security Model,” *IEEE Conference Publications*, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9388412/

[3] Q. Li, H. Wang, and M. Zhang, “HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design,” *IEEE Journals & Magazines*, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8635491/

[4] L. Zhang and Y. Liu, “The Research and Design of Honeypot System Applied in LAN Security,” *IEEE Conference Publications*, 2011. [Online]. Available: https://ieeexplore.ieee.org/document/5982237/

[5] U.S. Department of Health and Human Services, “Summary of the HIPAA Security Rule,” 2024. [Online]. Available: https://www.hhs.gov/hipaa/

[6] N. Abbasi and D. A. Smith, “Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPAA Compliance Framework and Responsibilities of Healthcare Providers,” *Journal of Knowledge Learning and Science Technology*, vol. 3, no. 3, pp. 1–12, 2024.

[7] Prophaze, “What Is Behavioral Analysis in Bot Detection?” 2025. [Online]. Available: https://www.prophaze.com/

[8] RocketMe Up Cybersecurity, “Using Behavioral Analytics to Identify Anomalous User Activity,” *Medium*, 2024. [Online]. Available: https://medium.com/

[9] H. Wang, M. Li, and Y. Chen, “A Privacy-Enhanced Framework with Deep Learning for Botnet Detection,” *Cybersecurity*, vol. 8, no. 1, pp. 1–18, 2025. doi:10.1186/s42400-024-00307-8

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

[10] D. Zhao et al., "Botnet Detection Based on Traffic Behavior Analysis and Flow Intervals," *Computers & Security*, vol. 39, pp. 2–16, 2013. doi:10.1016/j.cose.2013.04.007

[11] A. A. Hamza and J. S. Al-Janabi, "Detecting Brute Force Attacks on SSH and FTP Protocol Using Machine Learning: A Survey," *Journal of Al-Qadisiyah for Computer Science and Mathematics*, vol. 16, no. 1, pp. 21–31, 2024.

[12] M. D. Hossain et al., "SSH and FTP Brute-Force Attacks Detection Using LSTM and Machine Learning," in *Proc. 5th Int. Conf. Computer and Communication Systems (ICCCS)*, IEEE, 2020, pp. 491–497.

[13] N. Alotibi and M. Alshammari, "Deep Learning-Based Intrusion Detection for Brute-Force Attacks on FTP and SSH," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 89–98, 2023.

[14] M. A. Khan and S. Rahman, "Emerging AI Threats in Cybercrime: A Review of Zero-Day Attacks," *Knowledge and Information Systems*, 2025.

[15] P. Sharma, A. Kumar, and R. Singh, "AI-Based Zero-Day Attack Detection in Smart Community," *arXiv preprint arXiv:2408.02921*, 2024.

[16] J. Watmore, "Next.js 13 + MongoDB User Registration and Login Tutorial," 2023. [Online]. Available : https://jasonwatmore.com/

[17] R. Patel and M. Shah, "Enhancing Security in MERN Stack Web Applications," *IJETIR*, vol. 11, no. 9, pp. a759 –a763, 2024.

[18] MongoDB Inc., "Security and Privacy – Queryable Encryption," 2024. [Online]. Available : https://www.mongodb.com/

[19] A. Rahman, M. S. Hossain, and M. R. Islam, "Cloud-Based Honeypot Systems for Real-Time Threat Detection in Healthcare," *Journal of Healthcare Information Security*, vol. 15, no. 2, pp. 78–92, 2022.

[20] DataDome, "Multi-Layered AI for Bot Protection," 2025. [Online].

[21] CrowdStrike, "AI-Powered Behavioral Analysis in Cybersecurity," 2025. [Online].

[22] I. Khan, H. Durad, and M. Alam, "SMARTbot: A Behavioral Analysis Framework for Mobile Botnet Detection," *PLOS ONE*, vol. 11, no. 3, 2016.

[23] J. Hancock, T. M. Khoshgoftaar, and J. L. Leevy, "Detecting SSH and FTP Brute Force Attacks in Big Data," in *Proc. IEEE ICMLA*, 2021, pp. 1489–1496.

[24] A. Javadpour, G. Wang, and S. Rezaei, "Survey on Cyber Deception Techniques to Improve Honeypot Performance," *Computers & Security*, vol. 138, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com