International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-14 Issue-6, March 2026

Surveying Hybrid Intelligence Approaches that Combine Honeypots and AI for Ransomware Defence in Critical Infrastructure

Ibrahim Shaikh, Omkar Nachare, Srivaramangai Ramanujam

Abstract: ***Ransomware is a rapidly increasing hazard to essential networks, including the health care, finance, energy, and government sectors. Traditional security solutions have shown deficiencies in their ability to rapidly recognise zero-day ransomware attacks. This research project proposes a hybrid artificial intelligence-honeypot framework for proactive detection and mitigation of ransomware within critical infrastructure. Honeypot-based security technologies will be combined with artificial intelligence-based behavioural analysis of attackers to identify potential ransomware signatures at the earliest possible stage. Machine learning algorithms provide continuous estimates of file system interactions, network traffic patterns, and system calls captured in honeypot environments to detect and profile malicious behaviour. This research will contribute to the effectiveness of combining deception-based security measures with AI-based behavioural models, thus enhancing the resiliency of ransomware defence solutions in critical infrastructure.***

Keywords: ***Ransomware, Honeypot, Artificial Intelligence, Machine Learning, Cybersecurity, Critical Networks***

Nomenclature:
SCADA: Supervisory Control and Data Acquisition
IoT: Internet of Things
AI: Artificial Intelligence
ML: Machine Learning
ICS: Industrial Control Systems

I. INTRODUCTION

Ransomware attacks are a serious concern for critical infrastructure networks, such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and Internet of Things (IoT) networks, where cascading failures can lead to operational breakdowns and economic losses of millions per attack.

Manuscript received on 01 March 2026 | Revised Manuscript received on 09 March 2026 | Manuscript Accepted on 15 March 2026 | Manuscript published on 30 March 2026.
*Correspondence Author(s)
Ibrahim Shaikh, MS. (Cybersecurity) Student, Department of Information Technology, University of Mumbai, Vidyanagri, Kalina, Santacruz, Mumbai, (Maharashtra), India. Email ID: ibrahimsworksplace@gmail.com
Omkar Nachare, MS. (Cybersecurity) Student, Department of Information Technology, University of Mumbai, Vidyanagri, Kalina, Santacruz, Mumbai, (Maharashtra), India. Email ID: nachareomkar025@gmail.com
Srivaramangai Ramanujam*, Professor, Department of Information Technology, University of Mumbai, Vidyanagri, Kalina, Santacruz, Mumbai, (Maharashtra), India. Email ID: rsrimangai@gmail.com, ORCID ID: 0000-0003-2723-6067

This overall literature review on hybrid models that combine artificial intelligence (AI) with honeypot technology aims to detect and mitigate ransomware attacks beforehand by analysing more than 150 papers to understand the mechanisms, challenges, and research gaps in current studies. By spotlighting honeypot deception systems integrated with AI-Based analytics, this literature review explains how hybrid models overcome the limitations of traditional reactive security measures, especially for critical and crucial networks with limited resources under polymorphic and targeted attacks.

Findings from the literature review confirm the effectiveness of hybrid models in understanding attacker behaviour over time and using machine learning (ML) for anomaly prediction, with detection accuracies of up to 97% in simulated virtual system scenarios. However, limitations remain, including scalability issues and ethical concerns about deploying honeypots, and the collective evidence demands adaptive frameworks to handle zero-day variants. Critical network infrastructures such as hospitals, electric power distribution networks, banking services, government departments, etc., are major targets due to the valuable and important data they contain and their limited tolerance for downtime during service restoration [5]. Conventional signature-based security solutions have limited ability to combat advanced variants and unknown ransomware types [3] [19]. There is a requirement for self-controlled, intelligent defence systems.

II. RANSOMWARE

Ransomware is a type of malware that prevents users from accessing data or computing resources until a ransom is paid. In contrast to conventional malware designed to steal data or evade detection, ransomware attacks directly target integrity or availability. Initial research by Scaife et al. [1] and Kharraz et al. [2] shows that contemporary ransomware employs strong, advanced cryptography (e.g., RSA and AES) to render file recovery impossible without the attacker's private key. For many years, ransomware was a basic kind of virus that only locked files. Still, today it is a more financially driven aspect of criminal activity against computers and networks, with ransomware as the method of operation.

The breakdown of the various stages of the attack process involved in ransomware, after the initial compromise through several ways (e.g. via a phishing email, infected documents/attachments, exploit kits, exposing weakness in an existing remote desktop service (RDP) connection), etc.; is as follows: the initial compromise is succeeded by the performance of a process

whereby the malware establishes persistence, elevates its privilege level (to maximize points of entry for the malware) and then scans the local environment to locate targeted file types that have either been determined to be of value and/or are located in specific network shares. Behavioural analyses, such as those carried out by Sgandurra et al. [3] and Homayoun et al. [17], show that ransomware malware exhibits specific behavioural patterns, including mass file access, rapid increases in entropy due to encryption, deletion of backups, and registry modifications. These behavioural patterns serve as the basis for modern detection techniques. [17] provides evidence that ransomware exhibits identifiable patterns, such as mass file access, rapidly escalating entropy through encryption (file modification), deletion of backups, and registry modifications. These behaviours underpin current detection methodologies.

There's been an evolution in the types of ransomware we see today, which has spread across several operational classes. The common and best-known variant is crypto-ransomware, which decrypts files using symmetric encryption but encrypts the symmetric key with asymmetric cryptography.

Crypto Locker is one of the earliest widespread cases in which monetised cybercrime achieved significant success through hybrid encryption [1]—subsequent variations employed enhanced evasion methods and more robust key management.

One additional type of historical ransomware is Locker. It does not use encryption to lock your computer; rather, it locks it out entirely. Although Locker ransomware was far less widely used than it is today, historically, it was generally paired with a police warning, as with the Reveton family of ransomware. In addition to typically causing less damage than other types of ransomware, Locker has historically been less sophisticated than more modern forms of ransomware.

In addition to the original method of encrypting the victim's data to hold them for ransom, today's ransomware-as-a-service (RaaS) attacks now incorporate two separate extortion methods. For example, in the first method, the hacker will encrypt the stolen victim's data and, if the victim does not pay the ransom, publicly release the decryption key. The Maze ransomware group carried this out in their attack on one of the largest corporations in North America. As a result, some victims have experienced a significant increase in both financial and reputational risk. Some of these attacks have evolved to include a third level of extortion, known as "triple extortion," which combines DDoS attacks against the victim with direct contact with customers or business partners.

The commoditization of cybercrime facilitated the advent of Ransomware-as-a-Service (RaaS). In this model, ransomware is developed by affiliates and distributed on a profit-sharing basis.

LockBit is one of the most successful RaaS platforms, making it easier for attackers to get started from scratch, and this has led to a significant rise in global ransomware attacks.

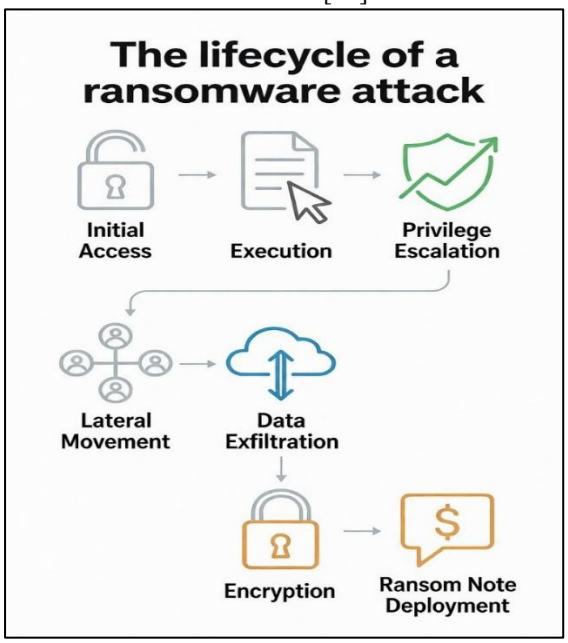
Some malicious campaigns are disguised to users as ransomware but are actually wiper malware. The most common example of wiper malware is NotPetya, which permanently wiped out all data while posing as a decryption key solution; unfortunately, this has led to billions of dollars in damage worldwide. These attacks show that the line between financially driven ransomware and cyber warfare is increasingly blurred.

The development of ransomware variants can be described in the following table:

Table I: Classification of Ransomware Types Based on Encryption and Data Exfiltration Techniques

Category	Primary Objective	Encryption Used	Data Exfiltration	Notable Example
Crypto-Ransomware	File encryption for ransom	AES + RSA	Optional	CryptoLocker
Locker Ransomware	System access restriction	No	No	Reveton
Double Extortion	Encryption + Data Leak	AES + RSA	Yes	Maze
RaaS Model	Criminal monetisation platform	Varies	Yes	LockBit
Wiper Malware (Disguised)	Data destruction	Irreversible	No	NotPetya

Technically and logically, the ransomware operates within a structured attack lifecycle. Initially, the malware performs reconnaissance and privilege escalation. It then identifies the critical file extensions (e.g., .docx, .xlsx, .db, .pdf, etc.) and performs encryption using a symmetric encryption key for speed. This encryption key is then encrypted using the attacker's public key. Studies such as Sgandurra & Lupu [16] emphasise that entropy-based detection can reveal encryption activity by measuring anomalous randomness in files. After encryption, ransomware deletes its shadow copies and backups to prevent recovery; this behaviour was also documented in ShieldFS research [18].



[Fig.1: The Lifecycle of a Ransomware Attack]

This structured process has been observed across different variants of ransomware and is supported by behavioural

mining techniques, as mentioned in [17], and by process-based detection studies in [20].

The truth is, a ransomware attack in places like hospitals or power plants isn't just an inconvenience; it's a whole different level of danger, and it can be life-threatening as well. The WannaCry attack was a perfect example of this; it exploited basic network protocols and brought hospital operations to a screeching halt worldwide. It was a wake-up call that showed just how vulnerable our physical infrastructure (Operational Technology) is to digital threats. The good news is that by watching network behaviour closely, researchers have found that these attacks aren't invisible; they generate weird network signals, unusual C2 traffic or strange SMB activity that we can actually spot if we know what to look for [5].

It's just like a classic cat-and-mouse game. As ransomware gangs have gotten smarter, the ways we catch them have had to evolve, too. The old-school method of just looking for a known bad signature simply doesn't work anymore, especially when malware can change its shape to evade detection. The behavioural detection, as described in [3] and [16], examines API call patterns, file system activity, and process execution. The cutting edge of ransomware defence now involves machines that think like detectives. By using techniques such as machine learning, deep learning, recurrent neural networks, and analysing file entropy [7], [8], [9], these models can detect an attack with over 95% accuracy in laboratory settings. False positives and scalability are still major concerns. And as the network grows, the challenge is to ensure detection scales with it without becoming a bottleneck.

What makes ransomware so terrifying today isn't just the malware itself; it's how much it has evolved. It grew up, and it keeps adapting. It started as simple, opportunistic file-locking software. It has transformed into a structured, multi-stage cybercrime ecosystem with sound economic foundations, characterised by complex technical operations, reliance on powerful cryptography, and data-extraction strategies. It is with such information and its scaling strategies that the main danger to present-day digital infrastructure lies. And because it keeps adapting, the only way to stay in the game is to double down on research in these fields: behavioural modelling, machine-learning tools for malware detection, and incidental mitigation strategies, which are deemed very important for tackling its incessant evolution.

III. HONEYPOT FRAMEWORK

A honeypot is a security resource whose value lies in being probed, attacked, or compromised. Unlike production systems that deliver business services to legitimate users, honeypots exist exclusively to be discovered and targeted by malicious actors. They have no authorised users and generate no legitimate traffic. This fundamental characteristic means that any interaction with a honeypot is, by definition, suspicious and worthy of investigation.

The logic underlying honeypot deployment is straightforward. Attackers scanning networks for vulnerable targets will eventually encounter these decoy systems. By attempting to exploit what they believe is a genuine asset, they reveal their presence, methods, and objectives. Defenders gain intelligence without exposing real production infrastructure to harm. This intelligence can inform signature updates, trigger alerts, or feed machine-learning models designed to recognise similar attack patterns in the future.

A. Classification by Interaction Level: Honeypots are most commonly classified by the level of interaction they provide to an attacker. This classification ranges from low to high levels of interaction. This classification represents a fundamental trade-off between safety and information richness.

B. The Low-Interaction: Honeypots emulate only the minimum set of network services and protocols. This might include an open TCP port, a simple file transfer service, or a login prompt with any credentials. The main benefit of this classification method is its safety and ease of implementation. Since no actual operating system or application code exists in the honeypot's backend, an attacker cannot exploit what does not exist. This classification method can easily deploy honeypots at a wide range of address spaces with minimal computational cost. However, the limitation of this classification method is equally clear. This classification method only detects the initial stages of an attack, usually limited to automated scanning and initial probing.

C. The Medium-Interaction: Honeypots represent the middle ground. They provide a more realistic emulation of service than low-interaction honeypots, without requiring a complete system implementation. For example, a medium-interaction honeypot may be a working web server that responds to HTTP requests or a database service that responds to Structured Query Language commands. The attacker is allowed to interact more fully with the service, gaining greater knowledge of the tactics and tools employed. However, the simulated operating system still limits the system's complete compromise. The additional complexity also provides the attacker with more opportunities for implementation mistakes that a sophisticated attacker may use to detect the deception.

D. The Highly Interactive: Honeypots are the ultimate in honeypot design. These systems are real, with real operating systems, applications, and services. There is nothing artificial about a high-interaction honeypot. This is the ultimate in intelligence gathering capability, as the researchers can see everything, from every command to every tool used to every attempt to elevate privileges and move about the network, just as if it were a real production network. The drawback to high-interaction honeypots is that they are highly dangerous, as they must be implemented under strict control to prevent attackers from using them to attack real production networks. This likelihood cannot be avoided.

Automated honeynet management frameworks, such as Puppet, have shown detection accuracy of 92% on IoT devices. Still, it is hard to maintain the deceptive lure against sophisticated human adversaries. For critical infrastructures, a hybrid approach combining honeypots and NIDS provides real-time packet capture and prevention, achieving 35% better performance than traditional IDS systems in simulated attacks.

Table II: Summary of Representative Frameworks. This Section Summarises the Various Frameworks, Demonstrating the Effectiveness of Hybrid Frameworks in Proactive Settings, Though Validation in Real-World Settings Remains Limited

Framework Type	Key Components	Detection Accuracy	Application in Critical Networks
Low-Interaction Honeypot	Simulated services (UPnP, SOAP ports); Log-based alerting	85-90% for family identification	IoT/SCADA decoys for early warning
High-Interaction Honeynet	Virtual PLC/RTU emulation; Docker deployment	97% for APTs and replays	ICS denial-of-service mitigation
AI-Hybrid Model	ML classifiers (LSTM/ensembles) on honeypot data; Bayesian decision-making	92-99% for zero-days	IIoT predictive analysis and isolation
Context-Aware Framework	Ontology for feature extraction; Federated learning	93% precision with reduced latency	Ransomware evasion in dynamic networks

IV. LITERATURE SURVEY

Scaife et al. [1] they introduced **CryptoDrop**, a system for early detecting warning signs of suspicious file activity, such as entropy, type, and deletion, to inform or alert users and interrupt ransomware attacks while still in progress, achieving a huge reduction in the number of lost files (median of 10 out of thousands) and destroying the economic model for ransomware payments.

Kodela [2] used AI predictive analytics to forecast upcoming ransomware attacks by analysing previous cybersecurity incidents and tracking attacker behaviour patterns.

Sgandurra et al. [3] have introduced EldeRan. This machine-learning-based dynamic analysis detects systems beforehand to identify potential issues during the installation phase (such as API calls and file system activity), thereby precisely differentiating between ransomware and legitimate software.

Mathane and Lakshmi [4] proposed a **context-aware AI framework** for predicting ransomware attacks in IoT systems that integrates device behaviour and network conditions to improve detection accuracy.

Cabaj et al. [5] analysed the network traffic of CryptoLocker (and other variants, such as CryptoWall, in extensions) in depth, using honeypots to record C2 communication, Bitcoin transactions, and network traffic, thereby detecting and blocking at the network level.

Nawrocki et al. [6] conducted a thorough survey on honeypot software, deployment, data collection, and analysis, providing essential background for honeypot-based malware analysis, including ransomware analysis.

Albshaier et al. [7] performed a systematic literature review on early ransomware detection techniques from 2020 to 2024, grouping pre-encryption behavioural indicators, machine learning frameworks, and other indicators to enable faster detection before the full impact is realised. In the review, he also pointed out the limitations of existing techniques.

Lee et al. [8] proposed an ML-based detection model targeting evasion techniques such as format-preserving encryption or encoding based on file-entropy manipulation, using such manipulated files to achieve high precision (about 94-95%) in identifying ransomware-modified content.

Alzakari et al. [9] proposed a multi-head attention-based recurrent neural network improved by optimisation methods for sequence-based ransomware detection, especially beneficial for behavioural patterns in resource-limited settings such as IoT.

Kritika et al. [10] provided a comprehensive literature review on deep learning approaches (CNNs, RNNs, and autoencoders) for ransomware detection, summarising feature extraction methods, datasets, performance characteristics, and future research in DL-based ransomware defences.

Iqbal and Serra Ruiz [11] provided a wide-ranging survey of AI-assisted ransomware detection, including machine learning and deep learning approaches, hybrid models, behavioural analysis, advantages, disadvantages, and current AI trends.

Higuchi et al. [12] proposed **ROFBSα**, a real-time system that integrates continuous monitoring, ransomware detection, and backup systems to enable swift identification and data restoration during ransomware attacks.

AlQahtan [13] proposed HoneyLite, a lightweight honeypot system efficient for implementation in today's networks, with a focus on resource-constrained threat hunting, including ransomware patterns.

Dodson et al. [14] utilised global honeypot networks to detect targeted ICS attacks, demonstrating how distributed sensors capture sophisticated attack patterns for critical infrastructure protection.

NIST [15] proposed the Computer Security Incident Handling Guide (SP 800-61 Rev. 2), which offers basic guidance on the stages of incident preparation, detection, analysis, containment, eradication, and recovery, widely cited for ransomware incident response.

Lachtar et al. [16] introduced RansomShield, a visualisation approach for mobile systems that translates file-system activity into visual cues, enabling users to identify and halt ransomware attacks.

Homayoun et al. [17] applied frequent pattern mining to system logs and behaviour analysis to detect suspicious patterns of ransomware attacks more effectively. It's useful for threat hunting and intelligence activities.

Continella et al. [18] proposed ShieldFS, a self-healing, ransomware-affected file system that monitors I/O requests in real time and rolls back malicious changes to the original files.

Kolodenker et al. [19] proposed PayBreak, a mitigation solution that enables secure access and storage of encryption keys during ransomware operations. This system enables victims to decrypt their files without paying the attacker a ransom.

Ahmed and Al-Dabbagh [20] developed an ML-based detection system that uses process-level behavioural features, along with API calls and file operations, to achieve accurate, real-time ransomware classification.

Purnama and Prasetyo [21] conducted a systematic review

of AI-based adaptive honeypots, which showed that these systems improve threat detection by modifying behaviour in response to attacker interactions.

V. FINDINGS

The step-by-step analysis of the research from [1] to [21] clearly demonstrates the evolution of the field of ransomware defence. In the early stages of research, the main focus was empirical threat analysis, where file-level behavioural detection was considered the primary defence mechanism, and research conducted using the CryptoDrop system [1] clearly indicated the variation of the entropy value, handling of files, and the use of encryption techniques as primary early warning signs of a ransomware attack. Dynamic analysis tools such as EldeRan [3] further improved detection by considering patterns in the application's overall setup, thereby shifting from signature-based to behavioural detection. Later research progressed to network-level monitoring and deception-based intelligence gathering. Honeypot-based research works [5], [6], [13], [14] facilitated the analysis of command-and-control communication patterns and malware behaviour, especially in IoT networks. In the meantime, new defensive technologies such as ShieldFS [18] and PayBreak [19] introduced mitigation-focused design to restrain encryption attacks, while NIST [15] standardized incident response procedures. More recent developments have applied evolutionary learning, frequent pattern discovery, and deep learning techniques [7]–[12], [16], [17], [20], claiming enhanced detection rates in laboratory environments.

However, despite these improvements, some key research gaps remain.

First, many runtime behavioural and dynamic detection tools remain susceptible to evasion attacks, including delayed payload execution, code obfuscation, sandbox evasion, and polymorphic attacks [3], [7], [8]. This makes them less effective in countering sophisticated real-world ransomware attacks.

Second, network-based and honeypot-based solutions, although helpful in intelligence gathering, are less effective in countering encrypted C2 communications, domain name generation algorithms, and stealth reconnaissance attacks [5], [6], [14]. Most of these solutions are passive monitoring systems rather than adaptive intelligence-driven defence systems.

Third, file- and process-based solutions [18]-[20] can be easily exploited by kernel-level attacks, such as privilege escalation, and by ransomware variants that prioritise data exfiltration over encryption, especially in double- and triple-extortion attacks.

Fourth, AI/ML-based solutions face key deployment challenges, including imbalanced and outdated datasets, risks of adversarial manipulation, computational complexity in resource-constrained IoT/OT networks, limited model interpretability, and limited validation in real-world, operationally critical infrastructure networks [7]–[11].

Most significantly, however, the literature shows a gap in tightly integrated architectures that can combine behavioural AI detection with deception-driven threat intelligence in a proactive, automated manner. The current state of analysis is that the solutions are, for the most part, independent, either as endpoint-detection tools, network-monitoring solutions, or standalone honeypots.

The gaps above, therefore, point to the need for a Hybrid AI-Honeypot solution that combines high-fidelity deception data with adaptive behavioural analytics.

VI. CONCLUSION

Based on an analysis of existing research and the limitations of the standalone detection method, an AI-Honeypot system for proactive ransomware detection in networks can be developed as a pragmatic, forward-looking solution. The AI-Honeypot system can be developed as an integrated system that uses honeypots to lure and trap actual ransomware behaviours in controlled decoy environments, while leveraging AI-driven behavioural analysis to monitor system calls, file operations, entropy changes, and network communications. The AI-Honeypot system would detect ransomware attacks before they occur by leveraging high-fidelity threat intelligence from honeypot interactions and adaptive machine-learning models. The AI-Honeypot system would provide enhanced resilience against zero-day and polymorphic ransomware attacks and automated containment capabilities, making it highly suitable for protecting critical infrastructure networks, where early detection and rapid response are critical.

DECLARATION STATEMENT

As the article's author, I must verify the accuracy of the following information after aggregating input from all authors.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. N. Scaife, H. Carter, P. Traynor and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Nara, Japan, 2016, pp. 303-312, https://ieeexplore.ieee.org/document/7536529
2. Venkatesh Kodela, "Predictive Analytics for Ransomware Attacks: Leveraging AI to Forecast Threats", *Int J Intell Syst Appl Eng*, vol. 12, no. 22s, pp. 66, Sep. (2024). DOI: https://ijisae.org/index.php/IJISAE/article/view/6394
3. Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C, "Automated dynamic analysis of ransomware: Behavioural patterns and detection", IEEE International Conference on Trust, Security and Privacy in

Computing and Communications, 10 Sep (2016), v1, pp. 1-12 DOI: https://doi.org/10.48550/arXiv.1609.03020
4. V. Mathane and P. Lakshmi, "Predictive Analysis of Ransomware Attacks using Context-aware AI in IoT Systems," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, (2021). DOI: https://doi.org/10.14569/IJACSA.2021.0120432
5. Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2018). Network activity analysis of CryptoLocker ransomware. IEEE Security & Privacy, 16(6), 70–77. DOI: https://doi.org/10.1016/j.compeleceng.2017.10.012
6. Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J. (2016). A survey on honeypot software and data analysis. IEEE Communications Surveys & Tutorials, 18(3), 1797-1824. DOI: https://doi.org/10.48550/arXiv.1608.06249
7. Albshaier, L., Alhussein, M., & Alqahtani, S. (2024). Early decision on ransomware identification using machine learning techniques: information (MDPI), 15(8). DOI: https://doi.org/10.3390/info15080484
8. Lee, J. (2025). A machine learning-based ransomware detection using manipulated entropy features. Sensors (MDPI), 25(8). DOI: https://doi.org/10.3390/s25082406
9. Alzakari, S. A., Aljuhani, A., & Rizwan, M. (2025). Multi-head attention-based recurrent neural network with enhanced optimization for ransomware detection. Scientific Reports (Nature). DOI: https://doi.org/10.1038/s41598-025-92711-4
10. Er. Kritika, "A comprehensive literature review on ransomware detection using deep learning, Cyber Security and Applications", Volume 3, 2025, 100078, ISSN 2772-9184. DOI: https://doi.org/10.1016/j.csa.2024.100078
11. Iqbal, Muhammad Junaid and Ruiz, Jordi Serra, "AI-Powered Ransomware Detection: A Comprehensive Survey on Machine Learning and Deep Learning Techniques", 2025. SSRN: https://ssrn.com/abstract=5355456 or DOI: http://dx.doi.org/10.2139/ssrn.5355456
12. Higuchi, K., Yamaguchi, Y., & Sakurai, K. "ROFBSα: Real-time backup and ransomware detection architecture". April 22, 2025. arXiv:2504.14162v1 [cs.CR] DOI: https://doi.org/10.48550/arXiv.2504.14162
13. AlQahtan, N. "HoneyLite: A Lightweight Honeypot Security Solution for SMEs. Sensors 2025, 25(16), 5207. EISSN 1424-8220, Published by MDPI DOI: https://doi.org/10.3390/s25165207
14. M. Dodson, A. Beresford, and M. Vingaard, "Using Global Honeypot Networks to Detect Targeted ICS Attacks," in *2020 12th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, (2020), pp. 275-291. DOI: https://doi.org/10.23919/CyCon49761.2020.9131734
15. NIST. "Incident Response Recommendations and Considerations for Cybersecurity Risk Management". NIST Special Publication 800 NIST SP 800-61r3. April 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3
16. Nada Lachtar, Duha Ibdah, Hamza Khan, and Anys Bacha. 2021. RansomShield: A Visualisation Approach to Defending Mobile Systems Against Ransomware. In ACM Transactions on Privacy and Security. ACM, New York, NY, USA, 29 pages. DOI: https://doi.org/10.1145/3579822
17. Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., & Khayami, R. (2017). Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence. IEEE Transactions on Emerging Topics in Computing, 8(2), 341–351. DOI: https://doi.org/10.1109/TETC.2017.2756908
18. Continella, A., Guagnelli, A., Zingaro, G., et al. (2016). ShieldFS: A self-healing, ransomware-aware file system. ACM Asia Conference on Computer and Communications Security. DOI: https://doi.org/10.1145/2991079.2991110
19. Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017). PayBreak: Defence against cryptographic ransomware. ACM Asia Conference on Computer and Communications Security. DOI: https://doi.org/10.1145/3052973.3053035
20. Omar Shamil Ahmed, Omar Abdulmunem Ibrahim Al-Dabbagh, Journal of Education and Science 30(5): 86-102 (2021). Ransomware Detection System Based on Machine Learning DOI: https://doi.org/10.33899/edusj.2021.130760.1173
21. L. H. Purnama and D. H. Prasetyo, "Effectiveness of Artificial Intelligence-Based Adaptive Honeypots in Cyber Threat Detection: A Systematic Literature Review and Meta-Analysis," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 14, no. 4, pp. 123-145, 2025. DOI: https://doi.org/10.32736/sisfokom.v14i4.2403

AUTHOR'S PROFILE

Ibrahim Parvez Shaikh is a Master's student in Cyber Security at the Department of Information Technology, University of Mumbai and pursued a Bachelor's degree in Computer Science in India. His research interests include secure messaging applications, web security, identity and access management (IAM), and data privacy. He has designed secure applications with end-to-end encryption and privacy-centric functionality and has hands-on experience in threat analysis and cybersecurity simulation. His research aims to develop scalable, compliance-driven, secure communication applications.

Omkar Ganesh Nachare is a Master's student in Cyber Security at the Department of Information Technology, University of Mumbai, and pursued a Bachelor's degree in Computer Science in India. His areas of interest include network security, cryptography, incident response, and secure Android application development. He has worked on projects including real-time patient data sharing, secure mobile applications built with Firebase, and web platforms with database integration. He is passionate about developing secure, scalable systems and applying cybersecurity principles to real-world problems.

Srivaramangai Ramanujam, Head, Department of IT, University of Mumbai, India. Having 24 years of experience in teaching and 6 years in industry. The specialization areas are artificial intelligence, security, and image processing. Has industry experience in web development and report code generators. Has published more than 35 International journal papers, 25 conference papers, and served as a resource person for various workshops and chaired sessions. She is actively involved in project management for multiple university projects to automate administrative functions. The papers relevant to Cyber Security include "Assessment of Deep Packet Inspection System of Network Traffic and Anomaly Detection", Enhancing Security using ECC in Cloud Storage", "Recapitulation of the Use of Machine Learning for Prevention of DDoS Attack on SDN Controller" and "Unmasking Deceptive Websites: Harnessing Machine Learning for Phishing Detection".