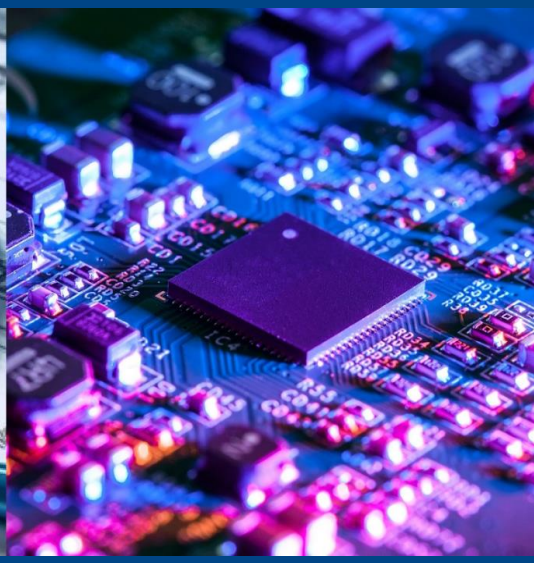
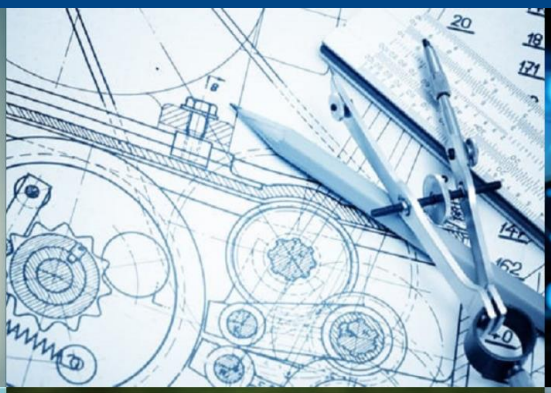
ISSN: 2582-7219

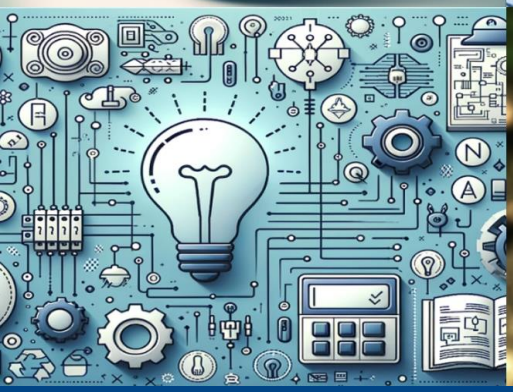




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 9, Issue 3, March 2026**

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903116

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)

Adaptive Context-Aware Multi-Layer Automata for Zero-Day Cyber Attack Detection

Mrs.D.Sterlin Rani[1], S Navya Sri[2], B Niranjana[3], S Mugaseeni[4]

Assistant Professor, Department of Computer Science and Engineering, R.M.D Engineering College, Chennai, Tamil Nadu, India[1]

Student, Department of Computer Science and Engineering, R.M.D Engineering College, Chennai, Tamil Nadu, India [2]

Student, Department of Computer Science and Engineering, R.M.D Engineering College, Chennai, Tamil Nadu, India [3]

Student, Department of Computer Science and Engineering, R.M.D Engineering College, Chennai, Tamil Nadu, India [4]

ABSTRACT: Cyber threats are becoming more dynamic and sophisticated, capable of evading traditional signature-based intrusion detection systems. The paper proposes a novel Adaptive Context Aware Multi-Layer Automata-based intrusion detection framework for zero-day and insider threats. Unlike traditional automata-based intrusion detection systems, the proposed framework utilizes a novel approach that combines finite automata with a dynamic transition refinement mechanism and context awareness. The framework creates individual automata for user, network, and system activities and correlates the state transition among them to identify anomalous patterns. The experimental simulation results show that the proposed framework improves the real-time intrusion detection efficiency and offers better explainability than traditional machine learning-based intrusion detection systems.

KEYWORDS: Cybersecurity, Finite Automata, Intrusion Detection, Zero-Day Attack, Behavioral Analysis, DFA.

I. INTRODUCTION

Cybersecurity has become a significant aspect in the field of information technology because of the rapid growth of cloud computing, IoT devices, and distributed systems. Traditional intrusion detection systems widely rely on signature-based detection mechanisms. Though signature-based detection mechanisms can detect known attacks, they fail to detect zero-day attacks.

Behavioral detection mechanisms can solve the limitations of signature-based detection mechanisms by modeling the system's behavior. Finite Automata, proposed by Stephen Kleene in the field of formal language theory, is a mathematical construct to model sequence-based events.

The limitations of existing automata-based detection mechanisms are:

- Static state definitions
- Lack of contextual awareness
- State explosion problem
- Inflexibility

To overcome the limitations of the existing detection mechanisms, the authors propose a new concept called Multi-Layer Context-Aware Adaptive Automata.

II. PROPOSED SYSTEM

A. System Overview

The ACM-AZCAD system has three layers of automaton that work independently of one another:
1. User Behavior Automaton (UBA)
2. Network Behavior Automaton (NBA)
3. System Call Automaton (SCA)

The state of the automaton is correlated by the Correlation Engine.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903116

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)

B. Mathematical Model

The mathematical model of the automaton is as follows:

$M = (Q, \Sigma, \delta, q_0, F, C)$

where:

- Q: set of states
- Σ: set of input symbols
- δ: transition function
- q_0: initial state
- F: set of accepting states
- C: contextual validation function (new addition)

The contextual validation function C checks parameters such as:

- Time of access
- Frequency of access
- Sensitivity of resources accessed
- Privileges of the user

C. Adaptive Mechanism

The system adjusts the weight value of the transition when the transition occurs frequently without malicious confirmation.

Suspicion Score Formula:

Suspicion Score = α(T_invalid) + β(Frequency Deviation) + γ(Context Risk Level)

where:

α, β, γ: weight coefficients of the formula.

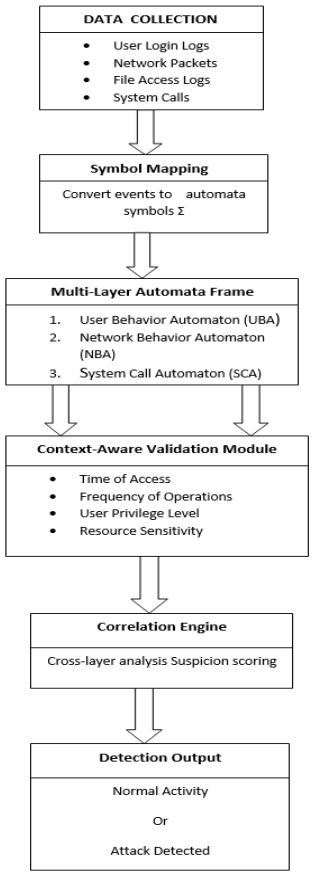


Fig: Architecture

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903116

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)

III. OPERATION AND SYSTEM FUNCTIONALITY

Step 1: Data Collection
• Login activities
• File access logs
• Network packets
• System calls

Step 2: Symbol Mapping
All activities are mapped to the symbol set Σ.

Step 3: Multi-Layer State Evaluation
Each automaton evaluates the data independently.

Step 4: Contextual Correlation
Correlation Engine performs the following operations:
• Evaluate cross-layer consistency
• Identify privilege anomalies
• Identify abnormal frequency

Step 5: Alert Generation
If abnormal state is found, then:
• Trigger the alert
• Log the state path
• Classify the attack type

IV. LITERATURE SURVEY

Current studies on cyber -attack detection via cyber- attack detection methods have concentrated on enhancing anomaly detection, reducing false positives, and addressing zero-day attacks via sophisticated computational methods. In 2023, a study by Ni [7] reviewed the applications of various machine learning algorithms on intrusion detection systems. The study demonstrated the potential of supervised learning algorithms such as Support Vector Machines and Random Forest algorithms on detecting known intrusion patterns. Nevertheless, it showed that the algorithms are associated with a number of false positives and require labelled data. In 2024, Reddy and Shankar Lingam [3] conducted a review on artificial intelligence frameworks in intrusion detection systems and showed the evolution of intrusion detection systems from signature-based systems to intelligent systems. The research showed that AI-based intrusion detection systems improve adaptability, and there is a rise in computational complexities. In 2024, Gueriani et al. The author in "[6]" carried out a review on reinforcement learning in intrusion detection systems for IoT devices.

The author was able to prove the viability of reinforcement learning in intrusion detection systems and how it can adapt to various threats in a network. However, it demonstrated scalability and performance complexities on real-time systems. Fahim et al. [1] in 2025 suggested a probabilistic automata-based detection scheme for supervisory control systems. The scheme was based on the concept of state transition probabilities for detecting sensor-based attacks. The proposed scheme was effective for structured environments, but the approach was limited to certain industrial control systems.

Likewise, Xu et al. [5] in 2025 has provided a study on different models of IDS that rely on deep learning techniques, focusing on the significance of neural networks in the detection of complex patterns. However, the authors also mentioned some of the major problems faced by the models, such as the limitations of interpretability and the requirement of large datasets.

Hozouri et al. [2] in 2025 has provided a detailed study on different modern IDS systems that rely on machine learning as well as deep learning techniques. The authors have mentioned the significance of hybrid detection systems in improving the efficiency of the models, as well as the requirement of better computational resources.

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 the year 2025, Diana et al. [4] have provided a review on the different technologies of intrusion detection systems in the field of networking environments, where the authors have mentioned that the intrusion detection systems can be categorized into signature-based systems, anomaly-based systems, and hybrid systems. The study revealed that behavior-based intrusion detection systems, where state transition mechanisms are used, are more suitable for real-time analysis in comparison to traditional systems that are based on rules.

Research Gap Identified

From the above research studies, it is observed that:

- Machine learning-based systems improve the accuracy of the intrusion detection systems, but the results are not transparent.
- Signature-based systems are not effective in detecting zero-day attacks.
- Existing automata-based systems are limited to a single layer.
- Few systems are incorporating contextual awareness in state transition mechanisms.

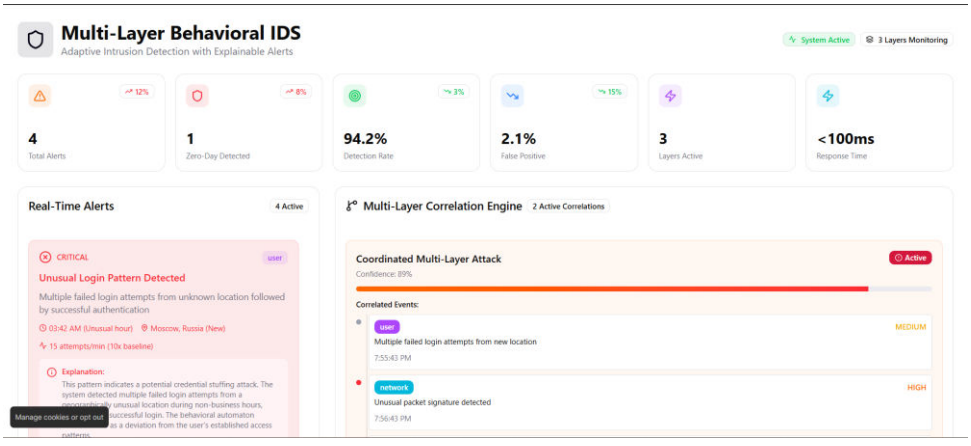
So, there is a need for a multi-layer, context-aware automata model that is capable of providing transparent and adaptive cyber- attack detection with minimal computational overhead.

V. OUTPUT

Case 1: Normal Activity
Sequence:
Login → File Access → Execute → Logout
Output:
No Alert
State Validated

Case 2: Zero-Day Behavior
Sequence:
Login → High Privilege Escalation → Bulk Data Transfer → Unknown System Call
Output:
⚠ Suspicious State
⚠ Context Risk High
⚠ Attack Detected

The system will output the following:
- Suspicion Score
- Layer involved
- Transition path



© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903116

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)

Fig:Multi-layer Behavioral IDS

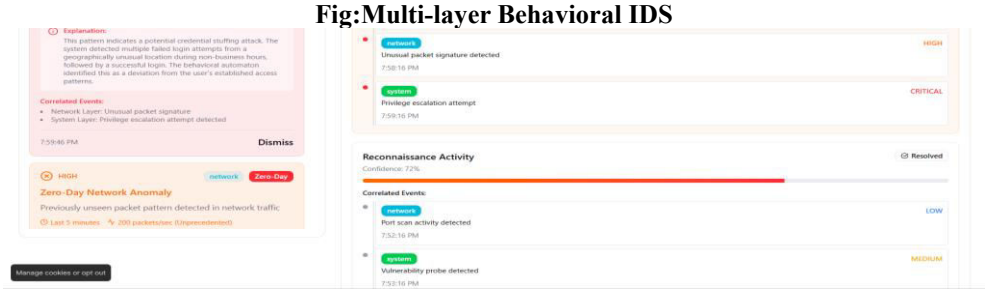


Fig: Reconnaissance Activity

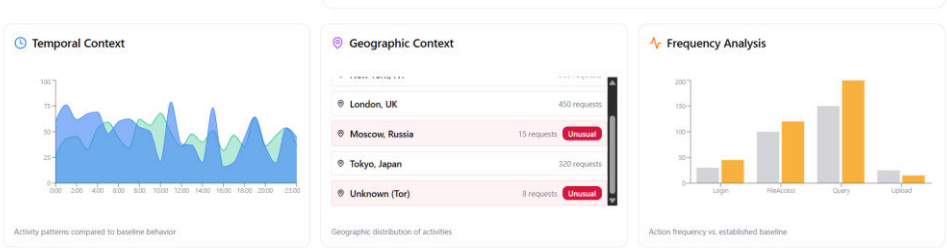


Fig: Analysis

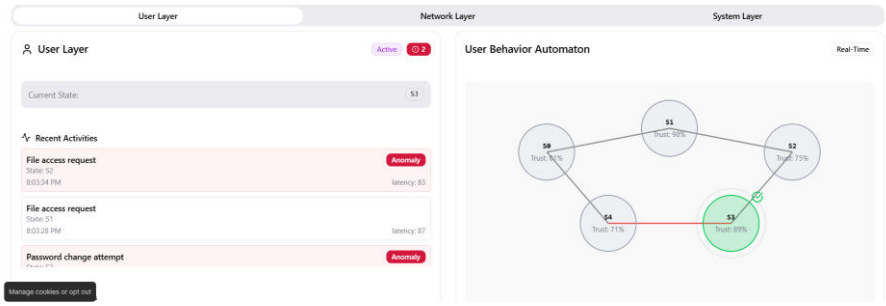


Fig: User Behaviour Automaton

VI. DRAWBACKS OF THE PROPOSED SYSTEM

1. Increased complexity in the system because of the modeling of multiple layers
2. Increased memory usage
3. Initial modeling of the behavior of the system required
4. Tuning of the threshold required
5. Scalability problems in large-scale enterprise systems

VII. APPLICATIONS

- Cloud Data Centers
- Banking Security Systems
- Industrial IoT
- Smart Grid Protection
- Government Networks
- Enterprise Security Monitoring

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)

VIII. CONCLUSION

In this paper, the author proposed an Adaptive Context Aware Multi-Layer Automata framework for detecting cyber-attacks. The proposed system differs significantly from traditional automata-based intrusion detection systems, as it includes multiple layers of modeling and contextual validation for improving zero-day attack detection. The proposed system also includes an adaptive transition refinement mechanism for improving detection accuracy while minimizing false positives.

REFERENCES

[1] P. Fahim, S. Oliveira, and R. Meira-Góes, "Enhancing sensor attack detection in supervisory control systems modeled by probabilistic automata," arXiv preprint, Feb. 2025. Available: https://arxiv.org/abs/2502.16753
[2] A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," Discover Artificial Intelligence, vol. 5, art. 314, Nov. 2025. Available: https://doi.org/10.1007/s44163-025-00578-1
[3] Y. Reddy and G. ShankarLingam, "Artificial intelligence in intrusion detection systems: trends, frameworks, and future directions for cybersecurity," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 17s, Feb. 2024. Available: https://www.ijisae.org/index.php/IJISAE/article/view/7689
[4] L. Diana, P. Dini, and D. Paolini, "Overview on intrusion detection systems for computers networking security," Computers, vol. 14, no. 3, Mar. 2025. Available: https://doi.org/10.3390/computers14030087
[5] Z. Xu, Y. Wu, S. Wang, J. Gao, T. Qiu, Z. Wang, H. Wan, and X. Zhao, "Deep learning-based intrusion detection systems: a survey," arXiv preprint, Apr. 2025. Available: https://arxiv.org/abs/2504.07839
[6] A. Gueriani, H. Kheddar, and A. C. Mazari, "Deep reinforcement learning for intrusion detection in IoT: a survey," arXiv preprint, May 2024. Available: https://arxiv.org/abs/2405.20038
[7] M. Ni, "A review on machine learning methods for intrusion detection system," Applied and Computational Engineering, Dec. 2023. Available: https://doi.org/10.54254/2755-2721/27/20230148

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