 ISSN: **3107-6513**

TRUSTTRACE A Trust-Decay Based Cyber Forensics Tool for Insider and Advanced Threat Analysis

A. Athulya[#1], Dr. M. Ramaraj[*2]

*B.Sc. Digital & Cyber Forensic Science[#1], Assistant professor[*2], Department of Computer Science, Rathinam College of arts and science, Pollachi Main Road, Eachanari, Coimbatore, Tamil Nadu, 641021.*

[1]athulyaarjunan333@gmail.com, [2]ramaraj.cs@rathinam.in

***Abstract*—**This paper presents TRUSTTRACE, a trust-decay based cyber forensic system designed to detect insider threats and advanced malicious activities. Traditional security systems often fail to identify behavioral anomalies and rely heavily on static rules, making them ineffective against evolving threats. The proposed system continuously monitors system logs, analyzes user behavior, and dynamically calculates trust scores using a decay-based model. Suspicious activities are identified through anomaly detection, and relevant forensic evidence is collected and stored for investigation. The system improves threat detection accuracy, enables real-time monitoring, and supports efficient forensic analysis. Experimental results demonstrate that TRUSTTRACE enhances security by identifying hidden threats while reducing false positives.

Keywords—Cyber Forensics; Insider Threat Detection; Trust Decay Model; Anomaly Detection; Log Analysis; Behavioral Analysis

I. INTRODUCTION

Modern organizations rely heavily on digital systems for communication, data storage, and operational management. With increasing system complexity, the risk of cyber threats has also grown significantly. Traditional security mechanisms such as firewalls and signature-based detection systems are limited in identifying sophisticated and insider-based attacks. Insider threats are particularly dangerous as they originate from authorized users, making detection more challenging.

Cyber forensics plays a vital role in identifying and analyzing such threats by collecting and preserving digital evidence. However, most existing systems focus on post-incident analysis rather than proactive detection. To overcome these limitations, intelligent systems that integrate real-time monitoring and behavioral analysis are required. This paper introduces TRUSTTRACE, a trust-decay based cyber forensic system that dynamically evaluates user behavior and detects anomalies. The system enhances threat detection accuracy while supporting efficient forensic investigation.

II. LIMITATIONS OF EXISTING SYSTEM

Existing security systems primarily depend on static rules and predefined signatures, which are ineffective against evolving threats. They lack the capability to analyse user behaviour dynamically and often fail to detect insider attacks. Most systems focus on reactive analysis after an incident has occurred, resulting in delayed response and increased damage.

Additionally, traditional forensic tools do not provide real-time monitoring or automated trust evaluation. They generate large volumes of logs but lack efficient mechanisms to extract

III. PROPOSED SYSTEM

The proposed system, TRUSTTRACE, introduces a trust-decay based approach to enhance cyber forensic analysis. It continuously monitors system activities and evaluates user behaviour using dynamic trust scores. The trust-decay mechanism reduces trust levels over time based on suspicious or inactive behaviour, ensuring that trust values reflect real-time user actions.

The system integrates multiple components including log collection, behavioural analysis, anomaly detection, and forensic evidence storage. System logs are continuously captured from various sources and processed to identify patterns of normal and abnormal behaviour. Any deviation from expected patterns triggers alerts and reduces the corresponding user's trust score.

Additionally, the system maintains a structured repository of forensic evidence, which can be used for further investigation and reporting. The modular architecture ensures scalability, flexibility, and efficient performance. By combining proactive monitoring with forensic capabilities, TRUSTTRACE provides a comprehensive solution for detecting insider threats and advanced cyber-attacks. Suspicious actions reduce trust scores, triggering alerts and evidence collection. The system integrates log analysis, anomaly detection, and reporting into a unified framework, enabling proactive threat detection.

Another key feature of the proposed system is its ability to differentiate between normal variations in user behaviour and actual malicious activities. This reduces the occurrence of false positives and ensures that only genuine threats are flagged. The integration of forensic evidence collection further strengthens the system by preserving critical data for investigation purposes.

ISSN: **3107-6513**

IV. METHODOLOGY

The methodology of TRUSTTRACE is designed to ensure a systematic flow of data from collection to analysis and reporting. The process begins with continuous log acquisition, where system logs are extracted at regular intervals using automated scripts. This ensures that no critical event is missed during monitoring.

After preprocessing, the system applies rule-based and pattern-based analysis techniques to evaluate user behaviour. These techniques help in identifying both known and unknown anomalies. The trust-decay model plays a crucial role in maintaining a dynamic representation of user reliability over time.

The system also incorporates threshold-based alert mechanisms. When the trust score falls below a predefined limit, the system immediately generates alerts for administrators. This enables quick response and minimizes potential damage. Additionally, all suspicious activities are recorded and stored securely, ensuring that evidence is available for future forensic analysis.

The final stage involves report generation, where the system compiles all relevant data into a structured format. This includes user details, detected anomalies, trust score variations, and collected evidence. The report is designed to be clear and easy to interpret, enabling efficient decision-making.

V. RESULTS AND ANALYSIS

The evaluation of the TRUSTTRACE system demonstrates its effectiveness in detecting insider threats and abnormal user behaviour. The system was tested under various scenarios, including normal usage, suspicious activities, and simulated malicious attacks.

In normal scenarios, the system maintained stable trust scores and did not generate unnecessary alerts. This indicates that the system accurately identifies legitimate user behaviour. In contrast, when suspicious activities such as repeated failed login attempts or unauthorized access were introduced, the system successfully detected these anomalies and reduced the corresponding trust scores.

The trust-decay mechanism proved to be effective in identifying gradual changes in user behaviour. Instead of relying on a single event, the system evaluates patterns over time, which improves detection accuracy. This approach significantly reduces false positives compared to traditional systems.

Performance analysis shows that the system operates efficiently with minimal delay in processing logs. The modular design ensures scalability, allowing the system to handle increasing volumes of data without performance degradation. Overall, the results validate that TRUSTTRACE provides a reliable and efficient solution for proactive cyber forensic analysis.

VI. CONCLUSION

The TRUSTTRACE system demonstrates a practical and efficient approach to addressing modern cybersecurity challenges. By integrating real-time monitoring, behaviour analysis, and trust-based evaluation, the system enhances the detection of insider threats and reduces response time.

The proposed approach not only improves detection accuracy but also ensures proper documentation of forensic evidence, which is essential for investigation and legal purposes. This makes TRUSTTRACE a valuable tool for both security monitoring and forensic analysis.

VII. FUTURE WORK

Future enhancements of the TRUSTTRACE system can focus on improving intelligence and adaptability. The integration of machine learning algorithms can enable the system to automatically learn from user behaviour and detect complex attack patterns that are difficult to identify using rule-based methods.

Another potential improvement is the development of a graphical user interface that provides real-time visualization of system activities, trust scores, and alerts. This would enhance usability and allow administrators to monitor the system more effectively.

The system can also be extended to support cloud environments and distributed networks, enabling it to handle large-scale infrastructures. Additionally, integrating automated response mechanisms can further improve system efficiency by taking immediate action when threats are detected.

ACKNOWLEDGMENT

The author expresses sincere gratitude to the faculty members of the Department of Information Technology for their guidance and support throughout the development of this project. Special thanks are extended to the project guide for valuable suggestions and continuous encouragement.

The author also acknowledges the support provided by the institution in facilitating the resources required for the successful completion of this work. Finally, heartfelt thanks to friends and family for their motivation and support.

REFERENCES

[1] E. Casey, Digital Evidence and Computer Crime, Academic Press, 2011.
[2] K. Scarfone and P. Mell, “Guide to Intrusion Detection Systems,” NIST, 2007.
[3] S. Axelsson, “Intrusion Detection Systems: A Survey,” 2000.
[4] A. Patcha and J. Park, “Anomaly Detection Techniques,” 2007.
[5] B. Schneier, *Applied Cryptography*, Wiley, 1996.
[6] R. Behl and A. Behl, “Cybersecurity and Cyberwar: What Everyone Needs to Know,” Oxford University Press, 2016.
[7] S. Garfinkel, “Digital Forensics Research: The Next 10 Years,” Digital Investigation, Vol. 7, 2010, pp. S64–S73.
[8] M. Bishop, “Computer Security: Art and Science,” Addison-Wesley, 2003.

ISSN: **3107-6513**

[9] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST SP 800-86, 2006.

[10] A. Patcha and J. M. Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends," Computer Networks, Vol. 51, No. 12, 2007, pp. 3448–3470.

[11] D. Denning, "An Intrusion Detection Model," IEEE Transactions on Software Engineering, Vol. 13, No. 2, 1987, pp. 222–232.

[12] W. Stallings, "Network Security Essentials: Applications and Standards," Pearson, 2017.