IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, October 2025
Impact Factor: 7.67

Role of User Entity and Behavior Analytics (UEBA) in Cybersecurity: A Study

Shambhavi Sharma[1], K Sampath Kumar[2], Pramod Kumar Jha[3]
Scientist –'B', IT, CAS, DRDO, Hyderabad, India[1]
JRF, IT, CAS, DRDO, Hyderabad, India[2]
Scientist –'G', IT, CAS, DRDO, Hyderabad, India[3]

Abstract: *User Entity and Behavior Analytics (UEBA) is emerging as a disruptive technology in the areas of cybersecurity, empowering organizations to detect technologically advanced threats by analyzing behavioral signatures of both internal and external users. UEBA unlike other proactive security solutions doesn't solely rely on static rules, rather it leverages Machine Learning (ML) and sophisticated statistical tools to identify anomalies that may indicate insider threats, compromised accounts or Advanced Persistent Threats (APTs). This paper attempts to study the architecture, methodologies and practical industrial applications of UEBA, bringing out its role in enhancing threat detection and response capabilities.*

Keywords*:* Cybersecurity, UEBA, machine learning, behavioral Analytics, Insider Threats

I. INTRODUCTION

With the exponentially growing complexity and frequency of cyber-attacks, traditional security mechanisms have been rendered insufficient and incompetent. Signature based detection systems often fail to identify zero-day exploits and insider threats. UEBA addresses and bridges this gap by focusing on behavioral patterns instead of predefined static rules. By proactive continuous monitoring and analysis of user activities, UEBA can detect anomaly that may signal malicious intent or compromise.

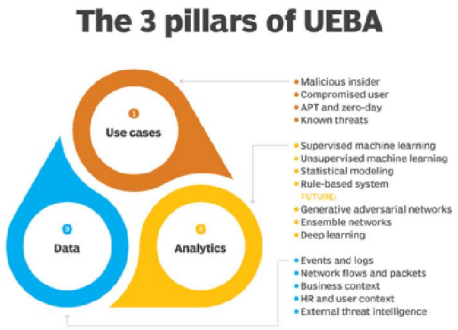

Fig 1. Three Pillars of UEBA

Architecture and Components of UEBA

UEBA system primarily consists of 4 main components, which are as described below:

- Data Collection Layer: This layer collects system logs from applications, endpoints, servers and various network devices.
- Analytics Engine: This engine applies mathematical models and machine learning algorithms to identify existing anomalies, if any.
- Threat Intelligence: As the name suggests, this layer enhances detection accuracy by correlating behavioral anomalies with known threat indicators.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, October 2025
Impact Factor: 7.67

- Alerts/Notification engine: This layer generates alerts and integrates with Security Information and Event Management (SIEM) systems for automated response.

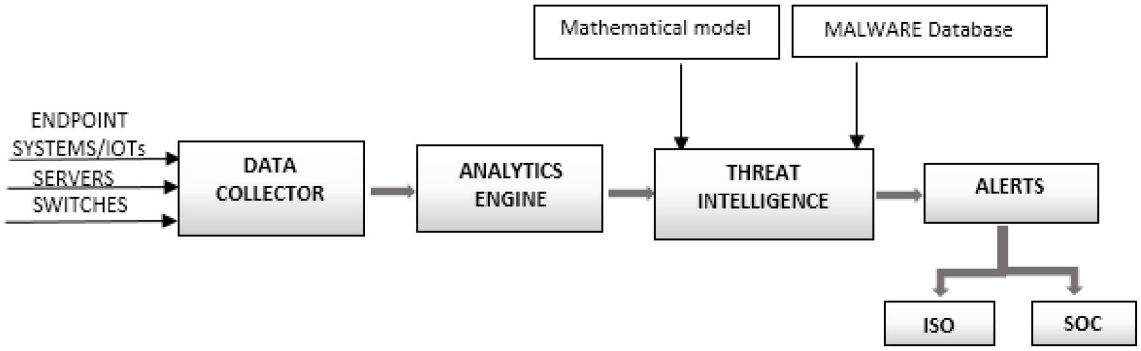

Fig 2. Schematic diagram of UEBA

II. PROBLEM STATEMENT

The main problem that UEBA solves is that traditional security tools, which we have been using for a long time to protect against external attacks, are not effective in detecting insider threats. Traditional tools, like Security Information and Event Management (SIEM) systems, struggle to find threats that don't follow predefined rules or known patterns. Many current security systems also lack the ability to understand the full context of how users and devices normally behave, making it hard to tell the difference between harmful actions and legitimate ones. Now to solve these problems UEBA establishes baselines of normal user and entity behavior using machine learning algorithms. If there is any deviation from established baselines, UEBA can identify suspicious activities that would be missed by rule-based systems.

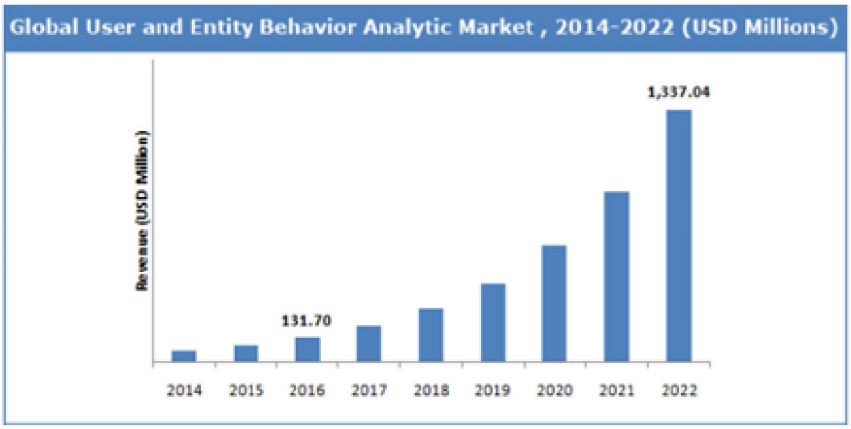

Fig 3. UEBA Growth Trend

III. WORKING PRINCIPLE

Basically UEBA transforms raw captured data into actionable security insights. UEBA system collects a wide variety of data from multiple sources to check both human and machine activities. System logs, Network logs, endpoint telemetered data, application and database logs, Identity and access management events, net flow, cloud logs etc., serves as the main data sources for this purpose. The data collected from all of the above sources contains a wealth of information about individual activities, such as login and logout times, file operations, accessed servers, application usage, USB device connections, remote access events, file uploads and downloads, attempts to modify server configuration settings, email activities, web searches, and any efforts to establish a connection between the private and the public network. The collected data is in raw form and raw data logs differ in formats and needs to be normalized

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, October 2025
Impact Factor: 7.67

before it becomes useful for analytics. After the data is passed to the analytics engine, analytic engine tries to connect the dots by linking different pieces of information to understand what the user is doing. If the analytics engine detects any suspicious activities or threats by finding significant deviations from that baseline, it generates anomaly alerts based on these findings. The output of the analytics engine is fed to the threat intelligence layer, which in turn tries to find out perceived threat. This layer improves detection by combining unusual user or system behaviour with known threat information, like malware signatures, blacklisted IP addresses, or attack patterns. Instead of looking at events separately, UEBA links unusual actions—such as accessing sensitive files at strange times or large data transfers—with known threats. This helps the system to decide if the activity is normal or suspicious, reducing false alarms and giving more useful alerts, verified positive alerts are send to ISO and SOC teams for further investigate of potential breaches, insider threats, or other cyber-attacks. As depicted in Fig [2].

IV. ADVANTAGES AND DRAWBACKS

Advantage of UEBA over conventional signature based defenses is it continuously monitors and learns a user's typical activities, like login times and accessed files and it can detects any deviation from this baseline, such as a user suddenly accessing sensitive data at an unusual hour, it flags the behavior as suspicious. Another key benefit of UEBA is the reduction of alert fatigue. By using contextual analysis to prioritize alerts and providing a risk score, it filters out false positives and presents security teams with fewer, but higher-fidelity, alerts. This allows analysts to focus on the most critical threats. It also provides richer context and risk scoring, building detailed profiles for users, servers, and devices to give security teams an immediate understanding of a potential threat's severity.

Using machine learning techniques in UEBA comes with several drawbacks. One major issue is handling users with special privileges, like developers or administrators, whose job requires unusual actions that don't fit normal behavior patterns. This makes it hard for the system to create a correct baseline for detecting threats. Another problem is insider knowledge—these users already understand the system well, making it easier for them to hide malicious actions. Additionally, UEBA struggles to detect slow and careful attacks that happen over a long time, because they don't show obvious changes daily. These small changes often seem normal, so they go unnoticed by the system. As a result, UEBA cannot catch every type of threat on its own

V. FUTURE SCOPE

In future UEBA can be integrated with platforms like Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) where it can get data from these systems with behavioural context. Beyond just simply alerting security teams, in future UEBA can automate responses for alerts like on detecting a high risk anomaly, the system could automatically lock a compromised account, disable a specific device or trigger a multi-factor authentication prompt speeding up response time and minimizing potential damage.

VI. CONCLUSION

UEBA is becoming an important part of modern offensive cybersecurity because it helps organizations to detect advanced threats that traditional systems often miss. By focusing on the behaviour of users and devices, rather than just fixed rules, UEBA provides a smarter and more flexible way to spot unusual activities that could indicate insider threats, compromised accounts, or other attacks. Its combination of data collection, machine learning-based analytics, threat intelligence, and automated alerts makes it easier to find real threats while reducing false alarms. Overall, implementing UEBA helps strengthen an organization's ability to respond quickly to security risks and keep sensitive data safe.

VII. ACKNOWLEDGMENT

We sincerely thank Dr N Sivasubramaniam, DS & Director CAS, for his valuable guidance and unwavering support in upholding cybersecurity compliance. Our heartfelt gratitude goes to Shri. Praveen Tandon, Scientist-'G' for his constant motivation. We also appreciate our teammates for their ongoing support throughout the process.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, October 2025
Impact Factor: 7.67

REFERENCES

[1]. Measuring the Effectiveness of User and Entity Behavior Analytics for the Prevention of Insider Threats.
[2]. Detecting Unknown Cyber Security Attacks through System Behavior Analysis.
[3]. Early detection of cyber security threats using structured behavior modelling.
[4]. Salman Khaliq; Zain Ul Abideen Tariq; and Ammar Masood, "Role of User and Entity Behavior Analytics in Detecting Insider Attacks".
[5]. V. Muliukha, A. Lukashin, L Utkin, M. Popov, and A. Meldo, "Anomaly Detection Approach in Cyber Security for User and Entity Behavior Analytics System", European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, October 2020.
[6]. Ahmed A. Moustafa, Abubakar Bello; and Alana Maurushat "The Role of User Behaviour in Improving Cyber Security Management"
[7]. Shari Lawrence Pfleeger ; Deanna D. Caputo "Leveraging behavioral science to mitigate cyber security risk