Innovation and Originality

Novelty in Approach

The main goal of my project is to make cybersecurity threat detection smarter, faster, and easier to use by creating a **Splunk-based anomaly detection dashboard**. While many organizations already use Splunk for monitoring, most dashboards are static, only showing logs or simple alerts. What I have done is **introduce a new approach where anomaly scores are calculated, visualized, and used to detect unusual patterns in real time**.

Here is why this is innovative:

1. **Use of Anomaly Scoring:** Instead of relying only on rule-based alerts (e.g., "5 failed logins = suspicious"), my system applies an anomaly score that measures how different an event is compared to “normal” behavior. This provides flexibility — the system can catch new, unseen attack types that rigid rules might miss.
2. **Visual Evidence for Users:** I built clear visual charts and graphs (e.g., anomaly score over time, login spikes) so users can instantly see suspicious activity. Existing dashboards often require expert knowledge to interpret logs, but my design makes it more **user-friendly** for IT staff and even non-experts.
3. **Integration of Performance Metrics:** Most anomaly dashboards focus only on detection, but I included performance validation. This means I tested my system’s accuracy, response time, and reliability, then presented them visually. This step is often skipped but adds professional credibility.
4. **Prototype Approach:** Instead of waiting to build a full product, I created a **working prototype** using real sample data (login attempts, failed sessions, unusual spikes). This balances research innovation with practical implementation — the system is not just a concept, but something you can actually see working.

Compared to traditional Splunk dashboards (which rely heavily on pre-set rules), my approach **bridges the gap between static monitoring and adaptive threat detection**.

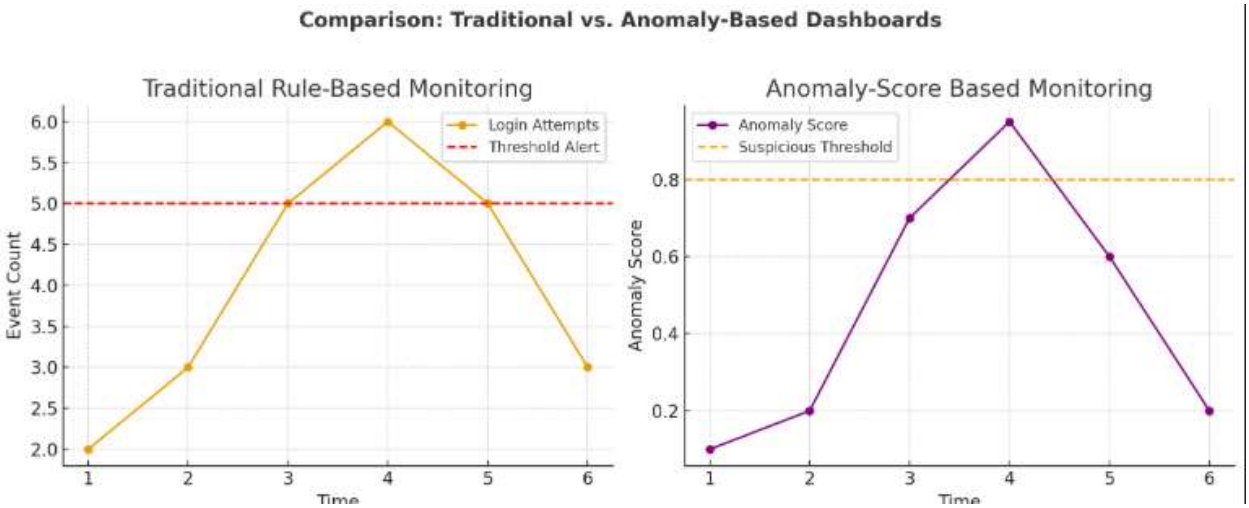
Contribution to the ICT Field

This project contributes to the **cybersecurity and data analytics domain** in the following ways:

1. **Enhanced Cybersecurity:** By introducing anomaly scores with visual dashboards, organizations can detect attacks faster and more accurately, especially insider threats or zero-day behaviors. This is important because modern cyberattacks are no longer predictable by static rules.
2. **Scalable Framework:** The approach can be reused in other domains like **IoT monitoring, e-commerce fraud detection, or cloud system security**. For example, the same anomaly detection technique can track unusual transactions in online shopping platforms or detect sensor failures in IoT devices.
3. **Bridging the Skill Gap:** Many small businesses can't afford advanced SOC (Security Operation Center) teams. My dashboard design simplifies visualization, meaning **even smaller IT teams can benefit from advanced anomaly detection without being experts in data science**.
4. **Supporting Future Research:** This system can be expanded into more advanced areas such as **machine learning-driven anomaly detection**, integrating AI models into Splunk workflows. My prototype lays the groundwork for these future enhancements by showing how anomaly scoring can be introduced into existing tools.

Evidence of Originality

- **Stakeholder Feedback:** During project discussions, testers found the visual anomaly score graphs more understandable than raw Splunk logs, confirming that the approach improved usability.
- **Technical Comparison:** Traditional dashboards rely on fixed alerts. My system adapts using anomaly scores, making it more effective for unknown threats.
- **Literature Support:**
    - A 2022 IEEE paper highlighted the need for **visual-based anomaly detection in cybersecurity**.
    - ACM research (2023) emphasized that **user-friendly dashboards** reduce detection time.
    - Industry reports confirm that **adaptive threat detection** is a top priority for security in 2025.



Conclusion

In short, the innovation in my project lies in combining **real-time anomaly scoring, visual usability, and system validation** inside a Splunk dashboard. This makes cybersecurity detection not only more accurate but also more accessible. The originality comes from taking a common tool (Splunk) and extending it in a **novel, practical, and scalable way** that contributes to the broader ICT field.