# Application of Finite State Machines in Intrusion Detection Systems

# Introduction

Today's digital landscape faces an evolution in complex cyber-attacks that access sensitive data and compromise systems. Detecting these intricate attacks is crucial for the mitigation, prevention, and protection against many cybersecurity threats. The increase of sophisticated and complex cyber threats requires robust detection systems that can identify and respond to attack patterns. This report explores how Finite State Machines (FSMs) can enhance Intrusion Detection Systems (IDS) capabilities to detect intricate attack patterns effectively.

# Theoretical Framework

FSMs are computational models that illustrate a system as several finite states, transitioning between them based on specific inputs. Their ability to represent sequential logic and recognise deviations in anticipated behaviour is why FSMs are applied in a variety of systems, including cybersecurity. Key components include:

- **States:** System conditions (e.g., "Normal Traffic", "Potential Threat", "Attack Detection", "Alert & Response" and "System Isolation)
- **Transitions:** Rules for movement between states (e.g., if a brute force attack on login attempts is detected, the IDS may transition from "Normal Traffic" to "Potential Threat")
- **Inputs:** Signals that activate transitions between states (e.g., known brute force attack patterns such as XXS)
- **Outputs:** System responses to the change of states (e.g., when transitioning to "Alert & Response" state, the system may alert the targeted victim or administrator of suspicious login attempts or block the suspicious IP address)

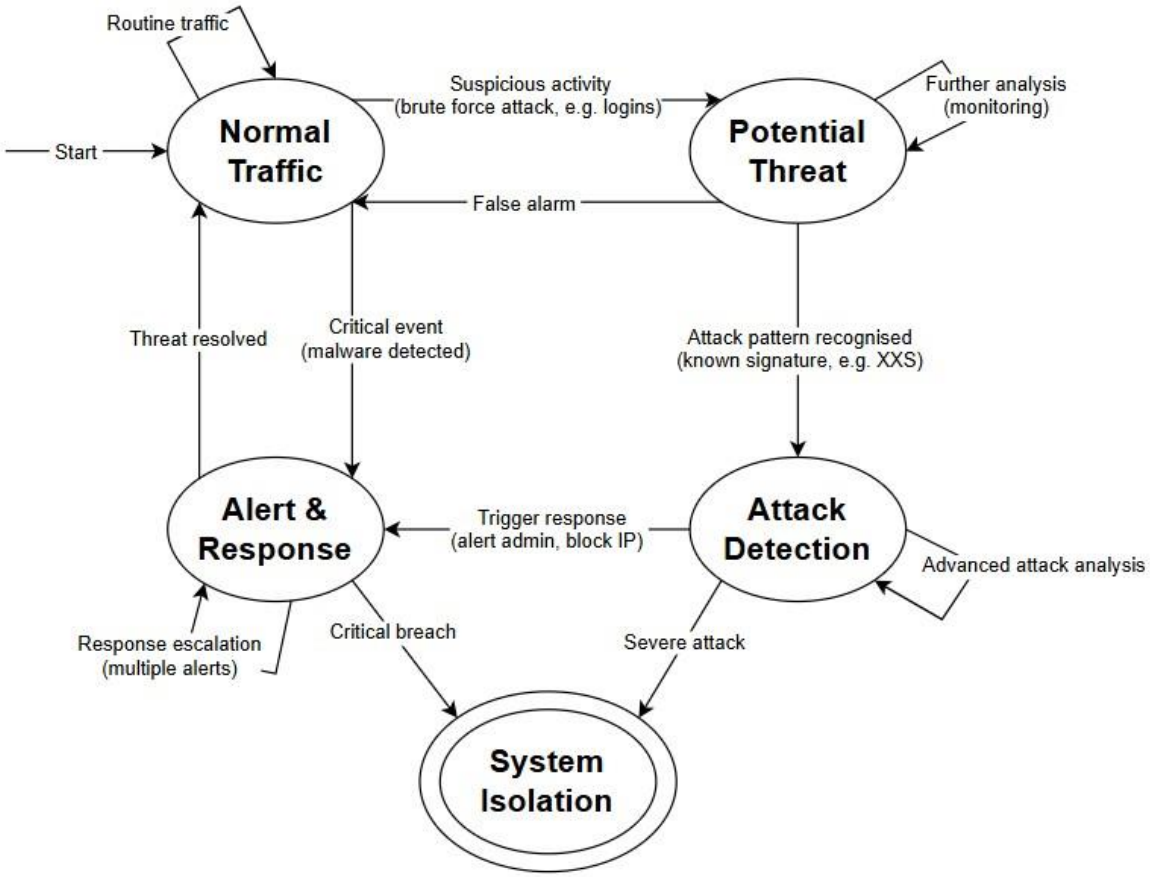


Figure 1: An FSM model for an IDS, detecting a critical brute force attack such as breaches to systems containing sensitive information.

An Intrusion Detection System (IDS) is a security mechanism designed for detecting unauthorised activities within a network system to prevent exploitation against a target. Figure 1 above illustrates how the collaboration of FSM components within an IDS environment, where states represent various security conditions and transitions triggered by specific network events. Two common variants of IDS include:

- **Signature-Based IDS:** Compares patterns of activities against known attack signatures to monitor inbound network activities. Although it can be effective for these objectives, it lacks the ability to detect unknown attacks with previously unseen patterns.
- **Anomaly-Based IDS**: Uses machine learning to analyse network behaviour and identify deviations using defined models of normal activity. Any deviations from this model are identified as anomalies, making it prone to false alarms.

## Application of FSM in Intrusion Detection

FSMs play a vital role in IDS by representing normal and potentially malicious behaviours through defined states and transitions, enabling systems to highlight anomalies in network activity and address the security threats with greater accuracy. Ayoughi et al. (2024) present findings on how automata learning, a FSMs extension, enhances security infrastructure through dynamic threat detection. Their evaluation suggests IDS efficiency improves when incorporating FSMs by discussing key challenges such as high false positives, evasion techniques, and performance overhead. In contrast, T.N. & Pramod (2022) propose a methodology centred on the modelling of user behaviour and network events to identify anomalies indicative of potential threats, using an event-based network model utilising FSMs. Their research implies that the application of FSMs in IDS frameworks makes the detection process more reliable, facilitating improved identification and mitigation of security threats.

## Advantages and Limitations

FSMs address IDS challenges through their systematic approach to modelling network behaviours. While there are several advantages, some limitations present themselves that are important to consider when applying them to complex systems.

**Benefits:**

- **Methodical Detection:** Captures familiar attack sequences and incorporates them into the structured approach FSMs offer, providing fast and reliable detection of suspicious activity
- **Processing Efficiency:** Depend on predefined instructions and transitions to process inbound traffic efficiently

**Challenges:**

- **Limited Adaptability:** Struggles in detecting novel and previously unseen attack patterns
- **Maintenance Requirements:** Requires frequent updates to include new attack patterns, possibly become resource-intensive

# Conclusion

Finite State Machines significantly improve Intrusion Detection Systems (IDS) through their ability to represent and detect complex cyber-attacks. Their structured approach to representing network behaviours contributes substantially to cybersecurity detection mechanisms. While acknowledging current challenges of FSM-based IDS, future research should focus on the integration of machine learning techniques with FSMs to develop more intelligent and adaptive systems. By developing dynamic models that can identify and respond to evolving cyber-attack patterns, this approach could potentially overcome current constraints and improve the overall accuracy of network security systems.

# References

Ayoughi, N., Nejati, S., Sabetzadeh, M. & Saavedra, P., 2024. *Enhancing Automata Learning with Statistical Machine Learning: A Network Security Case Study.* [Online] Available at: https://arxiv.org/abs/2405.11141

T.N., N. & Pramod, D., 2022. *Network event-based model using finite state machine to detect and predict insider intrusion on enterprise networks.* [Online]
Available at:
https://www.researchgate.net/publication/365721400_Network_eventbased_model_using_finite_state_machine_to_detect_and_predict_insider_intrusion_on_enterprise_networks