Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.15, No.1, 2024

Utilizing Artificial Intelligence for the Identification of Sleeper Cells

Preethi Kolluru Ramanaiah
Cloud Architect, Lead of AI initiative Program, Ernst & Young LLP, New York, USA
E-mail: preethiram4@gmail.com / Preethi.kolluru.ramanaiah@ey.com

Abstract
Artificial Intelligence (AI), advanced alternative to human mind, created by human mind, to simulate human intelligence in machines to think, perform and mimic human cognitive functions. Like humans, it uses various techniques like visual perception, speech recognition, decision-making, and language translation. One of growing security treats in country is with sleeper cells, a groups of individuals or agents operating undercover, within a society as normal people, until activated for a specific purpose, but identifying sleeper cells among community is a complex task that involves various intelligence and security measures. Artificial Intelligence (AI) can play a role in enhancing some aspects of this process, but it is important to note that AI alone may not be a panacea for such challenges due to ethical, legal, and technical considerations. This paper describes how AI help to identify sleeper cells.
Keywords: Sleeper cells, Behavioural analysis, Artificial Intelligence, Defence, Security threats
DOI: 10.7176/CEIS/15-1-02
Publication date: January 31st 2024

1. Introduction

In era of technology advancements, national security treats face advanced challenges day by day with technology, and most important among them being the detection of sleeper cells – clandestine groups strategically embedded within societies to carry out covert activities upon activation. Traditional methods used by intelligence agencies for identifying such threats are resource-intensive and often constrained by human limitations. However, the advent of Artificial Intelligence (AI) presents a promising avenue for revolutionizing the way we approach this critical aspect of counterterrorism.

This research paper seeks to explore the integration of AI technologies in the identification of sleeper cells, acknowledging the multifaceted nature of the challenge and the potential benefits and ethical considerations associated with such advancements. It is very essential to understand the dynamics of sleeper cells, their operational strategies, and the evolving landscape of national security threats.

The deployment of AI in this context involves harnessing its capacity for data analysis, pattern recognition, and predictive modeling. AI algorithms can scrutinize vast datasets, monitoring communication patterns, financial transactions, and social interactions to discern subtle indicators of sleeper cell activity. Video analytics and facial recognition technologies further contribute by enabling the identification of suspicious behavior in public spaces.

However, the integration of AI into counter-terrorism efforts is not without its complexities. Ethical concerns loom large, especially in terms of privacy infringement and potential misuse of advanced surveillance technologies. Striking a delicate balance between the imperative to safeguard national security and respecting individual rights is a challenge that demands careful consideration.

This research aims to provide a comprehensive overview of the current landscape, examining the potential of AI in identifying sleeper cells while critically evaluating the ethical implications and addressing the need for a robust legal framework. By scrutinizing the strengths and limitations of AI applications in counterterrorism, this paper aims to contribute to the ongoing discourse surrounding the responsible and effective integration of artificial intelligence in the realm of national security.

2. Growing Sleeper Cells Population

Sleeper cells are group of terrorist agents, who remain inactive until ordered to act. Till then, no one ever recognize them as terrorist, including close friends and family. Several factors can contribute for individual involved in activities that align with concept of sleeper cells. Few contributing factors are :

- Individuals manipulated or influenced by ideologies via propaganda, social networks, leaders, religions, aversion towards government.
- Sometimes people may feel marginalized, or face personal traumas or cries, and feel disenfranchised, resentful may be victims on the recruitment by extremist groups.
- Political, social, cultural, and religious causes may draw their attention to be part of extreme groups to achieve their goals.

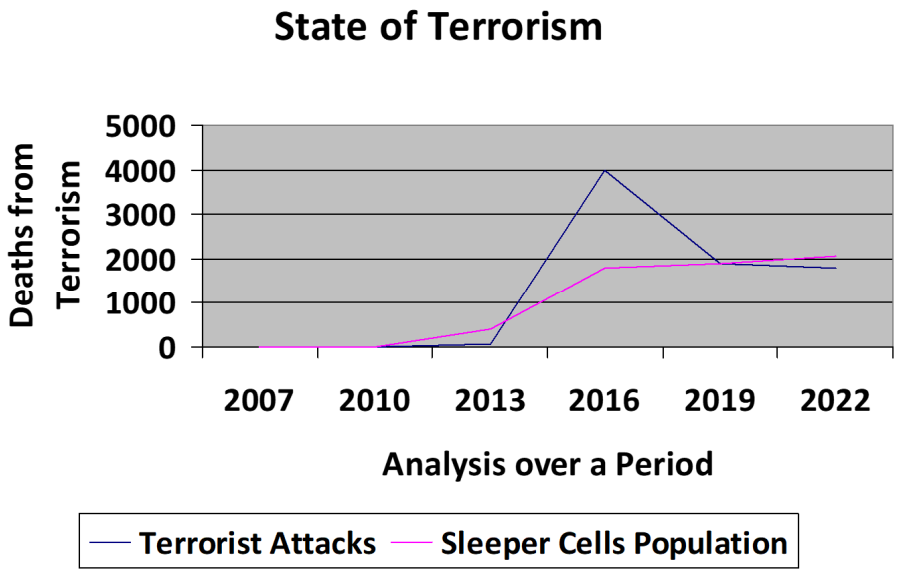


Chart 1: State of Terrorism Graph

Common factor on all above scenarios are psychological vulnerabilities that drive individual to be involved in sleeper cell activities. When considered graph, growing count of sleeper cells in drastically increasing. By an article published by centre for strategic and international studies, and data provided by Dragonfly terrorism tracker (provided on chart 1), even though terrorist attacks and number of deaths caused by terrorist attack is declining from 2016, but terrorists' population seems increasing and remains inactive.

3. BIN Technique in Sleeper cells Identification

Integration of Artificial Intelligence (AI) in identifying sleeper cells involves an approach that encompasses technological, ethical, and legal considerations. Here are key elements to consider:

3.1 Data Collection and Processing:

This step involves collecting different sets of data from diverse sources like medical records, criminal history, travel records, banking records/transaction details, social media connections, communication channels, call records so on. These data help in training AI system to identify patterns that deviate from normal behavior, signaling potential extreme activity. Also, historical data can be useful in building predictive models to identify regions or individuals at risk. Realtime data streams is very effective method to identify the treat sooner. Once data collection is complete, use processing tools to clean the collected data, and convert into standardize format for analysis.

3.2 BIN Analysis:

Next step involves data classification using BIN technique. BIN stands for Behavioral, Image and Network Analysis

- Behavioral analysis to understand gait patterns, voice patterns, any activity that are suspicious. Behavioural indicators that may precede sleeper cell activation and incorporate them into predictive algorithms. It helps in finding unusual patterns in individual or group behaviour that may indicate secrecy, isolation, or sudden changes in lifestyle.
- Image/video analysis to identify facial expressions, body language, visual communication patterns. Employ AI-powered video analytics for monitoring public spaces, identifying unusual behaviour, and tracking potential threats.
- Network analysis to understand individuals' connections and their criminal records through social networking. Monitor online activities for signs of radicalization, recruitment, or coordination. Identify connections and communication patterns among individuals to uncover hidden networks Monitor online communication, including social media, encrypted messaging platforms, and other online forums where sleeper cells might communicate. Detect irregularities or sudden changes in communication patterns that may signal preparation for activation. Apply AI for analysing complex networks to uncover hidden connections between individuals or groups.

Based on above details, will understand patterns by going through historical data analysis and ends in predictive Analytics to identify potential future threats. On all the above, finalizing, making the risk scoring helps in decision making. But it needs to be interviewed and re-verified by humans for any false positive or

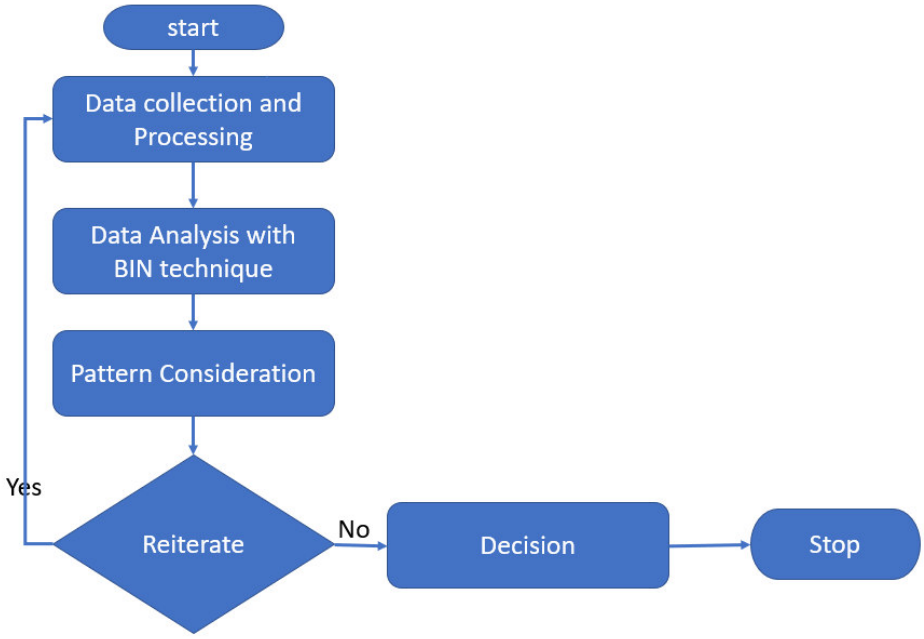
negative results. Above model requires continuous learning, allowing AI systems to adapt to new patterns and trends followed by sleeper cells.

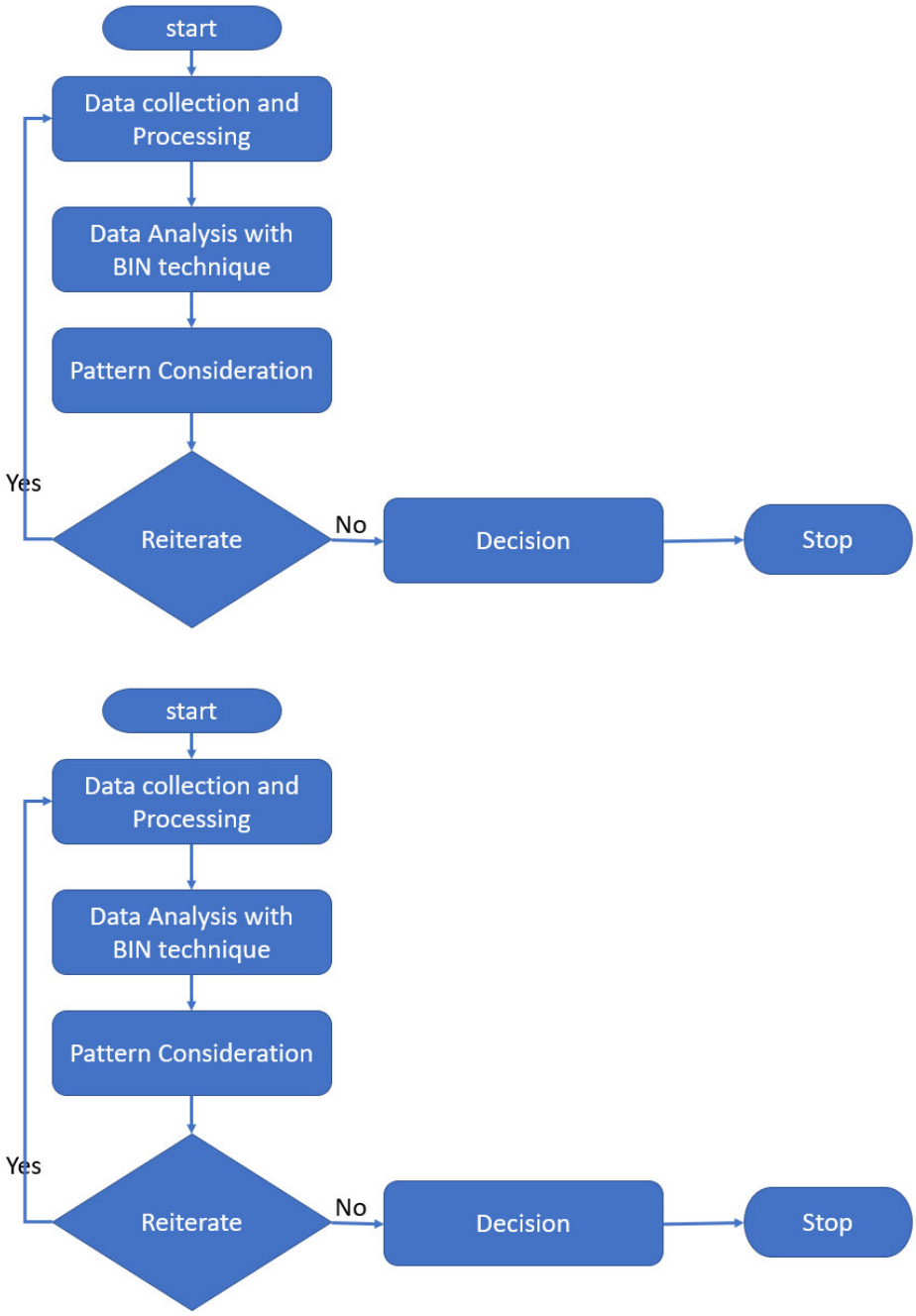
3.3 Pattern Consideration:

This method helps in identifying the patterns that deviate from normal behaviour and help in analysing individual who is potential treat. As part of Pattern consideration, system will analyse different data sets. And details of techniques will be discussed below:

- Help of travel patterns to identify individuals with frequent/unusual international travels or suspicious border crossing patterns.
- Identify unusual financial activities like large cash withdrawals, international travels, changes in spending behaviour.
- Employ surveillance systems in key locations to monitor and recognize individuals of interest. Understand cultural and societal norms to identify behaviours that deviate from the norm.
- Data Mining and Analysis: With Big Data Analytics, use advanced analytics to sift through large datasets for patterns that may indicate sleeper cell activities. And Implement machine learning algorithms to identify subtle patterns that may not be apparent through traditional analysis.
- Analyse digital footprints and conduct forensic investigations to uncover hidden online activities with digital forensic methods.

This is continuous process and need to train AI system with loads of data and develop complex algorithms to identify the patterns.





Flowchart 1: BIN technique in Sleeper cell Identification

3.4 Decision Making:

Decision point is a critical stage where AI-generated insights are assessed, verified by humans, and used to make informed decisions about potential sleeper cell activities. The design of the decision point and the criteria involved are essential components in the overall effectiveness and reliability of the system. Employ a decision support system using AI to assign risk scores to individuals or groups based on the analysis of multiple factors.

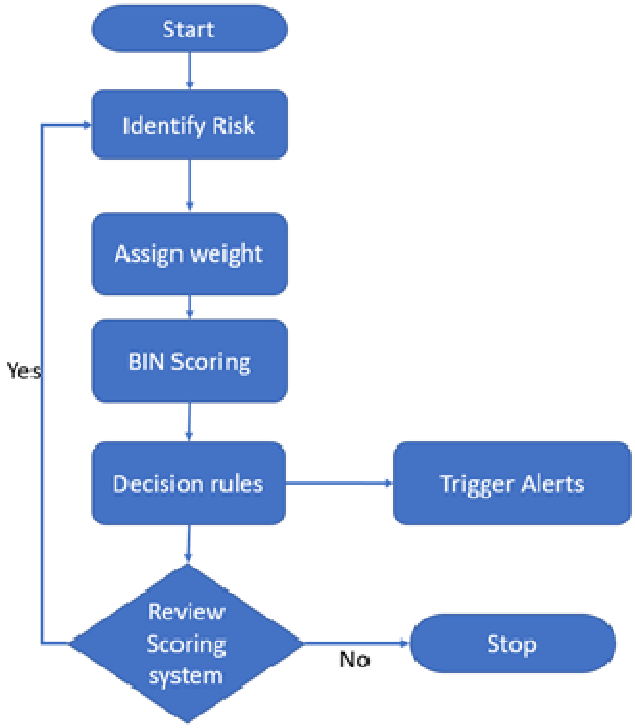
3.4.1 Risk scoring:

Calculating risk scoring involves assessing various factors and assigning numerical values to represent the level of risk associated with a particular entity or situation. The specifics of risk scoring can vary depending on the context and the nature of the data being analyzed. This paper uses BIN (Behavioural, Image and Network analysis) technique in calculating risk scoring. Identify and define the risk factors relevant to the identification of sleeper cells. These factors may include behavioral patterns, communication activities, travel history, social connections, and other indicators. Assign weights to each risk factor based on its perceived importance or

significance in identifying potential sleeper cell activities and normalize the data to ensure that values across different risk factors are on a consistent scale. Implement scoring methodology to assess the severity or likelihood of each risk factor. For each entity under consideration (individual or group), calculate the scores for each risk factor by multiplying the assigned weight by the normalized value of the factor.

$$\text{Risk score} = \sum(\text{weight} * \text{normalized value})$$

Sum up the individual scores for all risk factors to obtain a total risk score for the entity. Establish threshold values or categories to interpret the total risk score. For example, define ranges such as low risk, moderate risk, and high risk based on the total score.



Flowchart 2: BIN technique in Calculating Risk Score

Develop decision rules to determine the course of action based on the total risk score. For example, a high-risk score might trigger an alert for further investigation. Periodically review and adjust the risk scoring system based on feedback, new data, and evolving threat landscapes. Consider incorporating machine learning techniques to improve the accuracy of risk predictions over time. Integrate human intelligence for thorough review and verification of AI-generated results, addressing any false positives or negatives. It's important to note that risk scoring is a dynamic process, and the criteria and weights assigned to risk factors may need to be adjusted based on the specific context and the organization's evolving understanding of sleeper cell activities. Additionally, ethical considerations and compliance with legal frameworks should be paramount in designing and implementing any risk scoring system.

4. Data Privacy

When employing artificial intelligence (AI) in identifying sleeper cells or any other security-related applications, data privacy is at most important and it should adhere to ethical and legal considerations. Ensure that data collection and processing methods respect individual privacy rights. Strive to minimize the collection of unnecessary personal information and handle sensitive data securely. Users and stakeholders should have a clear understanding of how decisions are made to identify sleeper cells. Transparency builds trust and helps address concerns about biases or inaccuracies. Be vigilant about potential biases in data and algorithms that may disproportionately impact certain groups or communities. Implement measures to mitigate biases and ensure fair representation. Individuals affected using AI for sleeper cell identification should be informed about the data collection, analysis, and potential consequences. Whenever possible, seek informed consent. Ensure that the use of AI in sleeper cell identification complies with local and international laws, regulations, and human rights standards. Stay updated on legal frameworks and adapt processes Be aware of anti-discrimination laws and regulations. Implement measures to prevent biases in AI algorithms that could disproportionately affect specific groups, leading to discriminatory outcomes. Understand and adhere to local and national laws governing surveillance activities. Ensure that the deployment of AI for sleeper cell identification aligns with legal

requirements for surveillance practices. Ensure that the use of AI in security respects fundamental human rights. Consider principles outlined in international human rights agreements and conventions. Understand the legal implications related to national security, border security force, surveillance laws, data retention rules, need to comply with laws to ensure individual privacy is not compromised.

5. Conclusion

In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Also, security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention if smart approaches are used. Publications reviews indicate that studies into artificial neural networks offer the findings of AI most widely relevant to cybersecurity. Neural network implementations continue cybersecurity. For many fields where neural networks weren't the most appropriate technologies, sophisticated cybersecurity approaches are still desperately needed. Such fields include decision support, understanding of the situation, and control of information. The most interesting in this scenario is expert machine development. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that the perpetrators will exploit a new form of artificial intelligence if it is accessible. This is not obvious. In addition, the latest technology in the understanding, interpretation, and management of information, particularly around computer learning, would significantly improve systems' cybersecurity capabilities.

References

Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. SIN’09 - Proceedings of the 2nd *International Conference on Security of Information and Networks*, 229–234. https://doi.org/10.1145/1626195.1626252.

Chang, R. I., Lai, L. Bin, & Kouh, J. S. (2009). Detecting network intrusions using signal processing with query-based sampling Filter. *Eurasip Journal on Advances in Signal Processing*, 2009. https://doi.org/10.1155/2009/735283.

Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} *Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS’07)*. 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

Kotenko, I. V, Konovalov, A., & Shorov, A. (2010). Agend-based Modeling and Simulation of Botnets and Botnet Defense. *In Conference on Cyber Conflict* (pp. 21–44). http://ccdcoe.org/229.html.

Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. *MODELSWARD 2013 - Proceedings of the 1st International Conference on ModelDriven Engineering and Software Development*, 312–315. https://doi.org/10.5220/0004348203120315.

Pachghare, V. K., Kulkarni, P., & Nikam, D. M. (2009). Intrusion detection system using self organizing maps. *2009 International Conference on Intelligent Agent and Multi-Agent Systems*, IAMA 2009, 4(12), 11–16. https://doi.org/10.1109/IAMA.2009.5228074.

Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. *International Journal of Computer Sciences and Engineering*, 5(12), 317–322.