NUSTL®
NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY

SAVER TechNote

September 2022

ARTIFICIAL INTELLIGENCE/MACHINE LEARNING TECHNOLOGY USES FOR FIRST RESPONDERS

Artificial Intelligence/Machine Learning (AI/ML) can be applied to address various operational challenges in the first responder community. This technote defines AI/ML; discusses its possible uses, advantages, challenges, and limitations; and offers some basic guidance. AI/ML applications are too ranging to fit within a single AEL category, though some capability is covered by AEL 13IT-00-DACQ, titled "Data Acquisition."

Overview

AI refers to automated, machine-based technologies with at least some capacity for self-governance that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. ML is a subset of AI. ML systems receive inputs in the form of training data, and then generate rules that produce outputs. ML systems "learn" from examples, rather than human-created rules.

With the recent, exponential increase in cheap and massively parallel computation power, like with Graphical Processing Units (GPUs), ML can finally process enormous amounts of information, that would be impossible for humans to go through, and make decisions, predictions, provide guidance, or identify trends rapidly enough to be advantageous.

While humans are great at critical thinking and decision-making, it is impossible for most humans to process and retain massive amounts of data at the speed of current computing platforms. If you gave a human a mugshot and a few million images to search and match, it would be an impossible job to do in a timely manner. The functionality for a computer to do that has existed for a long time, however most of the rules for matching images were programmed by humans ahead of time. Building upon this capability and the recent growth in the ability to process and further analyze immense amounts of information, computers can now compare and match faces without using a static set of human-programmed rules.

With ML systems, we can do much more than previously possible with statically programmed rules alone. In most instances though, ML is dependent on a significant amount of data to learn and provide responses that are accurate and are of significant use. For example, ML systems can learn how people age by analyzing images of individuals over time and then apply an aging (or de-aging) process to images of different individuals to match pictures of them that may be years or decades apart, or even determine age by analyzing an image.

Advantages, Applications, and Methodologies

Many first responder tools are progressively relying more on AI/ML. These tools can vary in their utility and have their advantages and challenges in helping first responders accomplish their mission. AI/ML technologies are used for video surveillance, emergency medical services (EMS)/healthcare decision-making and guidance, 911 call center auto prioritization and recommendation, facial recognition, drug/chemical and contraband detection, fraud prevention, anomaly detection, unmanned aircraft systems navigation, wildfire prediction, collision prevention and much more.

Potential advantages include less risk to human life, less bias, no emotional decisions, fewer operator errors, constant availability, and increases in speed, accuracy and privacy.

AI/ML can be applied to solve problems through three key methodologies or types of ML: Supervised Learning (SL), Unsupervised Learning (UL) and Reinforcement Learning (RL).

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) program to inform emergency responder equipment selection and procurement decisions.

Located within the Science and Technology Directorate, the National Urban Security Technology Laboratory (NUSTL) manages the SAVER program and works with emergency responders to conduct objective operational assessments of commercially available equipment.

SAVER knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the responder community: "What equipment is available?" and "How does it perform?"

To explore the full library, visit SAVER online at www.dhs.gov/science-and-technology/saver-documents-library.

For additional information on the SAVER program, email NUSTL at NUSTL@hq.dhs.gov.

Science and Technology

Supervised Learning, much like a supervisor might instruct a new employee on their job functions, is a type of ML in which the system is given a set of information and matching answers to learn, and based on that information, makes decisions or predictions. SL can be used for drug/chemical and contraband detection, facial recognition, video surveillance, EMS/healthcare decision-making/guidance, and 911 call center auto-prioritization and recommendation, and more.

Unsupervised Learning systems receive information without any pre-programmed answers or guidance and are expected to generate useful information for users. An UL system discovers patterns across multiple dimensions of data and provides information that can be used to make decisions. UL has various applications such as video surveillance, cybersecurity, and pattern detection. For example, COVID decision dashboards correlated multiple dimensions like age, location, ethnicity, and income to COVID levels with the use of UL [1]. This allowed officials to make decisions to ensure the most effective use of limited resources by highlighting hotspots, most vulnerable age groups, and relationships between socioeconomic factors.

Anomaly detection, another example, can be used to detect breaches as part of zero trust cybersecurity efforts or be used for detecting and flagging certain potential hazards while scanning luggage at an airport or people at an event or checkpoint. Anomaly detection can also be used for video monitoring to reduce operator workload and ensure critical event detection. Other uses include crowd behavior analysis for threat detection.

Reinforcement Learning allows a system to learn and change its behavior based on the end results of its action. For example, a traffic light can use RL to learn and take actions to ensure the most efficient flow of traffic. RL is the key to creating the feedback loop required to minimize failures of ML in critical systems.

Operational Challenges and Limitations

AI/ML has limitations such as a lack of critical thinking; possible inability to handle ethical issues; lack of emotions; lack of regard for privacy; and possible incorporation of bias if the data used to learn is skewed.

AI/ML currently can only be applied to a very specific set of problems, since the ability to replicate human thinking in an expansive way does not exist yet.

Implementation and use of ML requires powerful computation platforms that are easily attainable nowadays, but require special care to ensure sufficient quantity, quality and breadth of data is used to ensure the system can handle a broad set of scenarios and avoid bias [2]. The privacy concerns of massive data available to a system that include personally identifiable information present another challenge. This increases the risk of leaks or misuse, and thus requires special care and constraints be applied to the data. Accuracy is also a concern; while it is acceptable to have a false alarm on piece of luggage once in a while, it is another scale of issue to have someone put on a "no-fly" list or get arrested due to an incorrect classification by an AI system.

These kinds of critical scenarios require additional checks and balances and feedback loops to ensure failures are corrected. Recent developments in threats to ML systems like "poison attacks" that confuse a system to defeat license plate readers and other camera technologies may not yet have solutions other than a human in the loop [3].

Another challenge from a legal perspective is that AI/ML decisions cannot always be explained and may not be defendable in court. The liability of errors and mishaps caused by an AI system is still in debate.

To utilize AI/ML effectively, it is imperative to have domain experts who understand the users' mission space and staff with understanding of legal constraints as well as technical experts who can support its implementation. To create a usable system, all disciplines must work in sync: the domain experts gathering operational requirements, advisors noting legal constraints with an understanding of the data available and the technical experts determining possible solutions based on collaboration with the domain and legal experts.

References

[1] MITRE, "SMARTER CRISIS RESPONSE THROUGH THE COVID-19 DECISION SUPPORT DASHBOARD," August 2020. [Online]. Available: https://www.mitre.org/news-insights/impact-story/smarter-crisis-response-through-covid-19-decision-support-dashboard.

[2] NIST, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," [Online]. Available: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[3] Belfer Center for Science and International Affairs, Harvard Kennedy School, "Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It," August 2019. [Online]. Available: https://www.belfercenter.org/publication/AttackingAI.