Trusted AI Platforms for the Connected Car Ecosystem

It is common knowledge that sensitive or personal data from connected cars are at risk of being hacked or breached. More important though, is that it is critical to realize that connected cars pose serious threats to human lives, including fatalities.[1] This is because controls and features such as automated driving assistance systems (ADAS), autopilot, cruise control, speed and door locks are driven by a combination of complex technologies coupled with insecure networks. The digitalized vehicle ecosystem and related sources of cyberrisk are well documented.[2]

The first fatal accident involving a connected car occurred in May 2016 in the US State of Florida.[3] The vehicle was in autopilot mode and it is believed that it failed to recognize an incoming truck. Another connected car-related fatality took place in the US State of California in March 2018, when autopilot mode was engaged in a semi-autonomous vehicle.[4] The car was said to have presented visual and audio warnings that were not heeded by the driver, resulting in the loss of life.

Researchers have demonstrated multiple ways that a connected car can be hacked remotely, taken control of and made to halt suddenly in the middle of the road after moving at high speeds.[5] It is worth examining the case for a trusted platform in the context of connected cars that can overcome factors impacting human elements of security such as bias, unexplained decisions or predictions within the frameworks of security, and privacy by design. Also worth analysis are factors affecting personally identifiable information (PII) during data exchange and commands and instructions for voice-assisted, remote control or semi-autonomous driving,

Khyati Mehta
Is the senior manager of product and strategy at Amazon. She has more than 16 years of experience in product development, product marketing and solutions design in IT and the telecom and ecommerce industries.

Chinmoy Rajpal
Is the senior manager of security operations at Verizon India. He has more than 16 years of experience in security and privacy governance, risk and compliance (GRC) with expertise in cloud security and is passionate about trustworthy and responsible artificial intelligence (AI).

Gaurav Verma
Has more than 27 years of experience in regulatory and statutory compliance, audit, finance and operations delivery. After working with corporations for 25 years, he created a startup firm serving clients in the finance operations and regulatory compliance sectors.

> EVEN ACCURATE AND INSIGHTFUL PREDICTIONS MAY BECOME INEXPLICABLE DUE TO THEIR COMPLEXITY, REDUCING THE TRUST FACTOR OF SUCH PLATFORMS.

including telematics data exchange, commands and instructions, which leverage technologies such as cloud computing, artificial intelligence (AI), machine learning (ML), web and mobile applications (apps), and networks.

The Connected Car Market and Value Chain

Value-driven use cases and business insights[6] through predictive and prescriptive analytics are made possible by a plethora of technologies, such as big data, the Internet of Things (IoT), cloud computing, high-speed connectivity, mobile applications, AI and ML. These are some of the cornerstones of the modern business-driven, technology-led value chain leading to the rise of connected data monetization business models in the automotive industry.

As per an industry report, the connected car data-enabled services market is expected to be valued at US$450-750 billion by 2030.[7] Additional research indicates that the global connected car market was valued at $US72,499.2 million in 2019 with a compound annual growth rate (CAGR) of 24.1 percent during the period from 2020-2025, with safety and security being the key growth drivers.[8]

The Need for Security and Privacy by Design

The connected car ecosystem is fueled by the widespread availability and adoption of technologies[9] such as cloud computing, 5G and mobile devices, Wi-Fi, Bluetooth, AI, and ML, with complex algorithms, edge computing and IoT.

All or most of these technologies converge as a single platform, along with the connected car networks consisting of electronic control units (ECUs) and controller area networks (CANs),[10] to deliver value to end users and stakeholders. An important tenet for stakeholders that share data with any platform is to add valuable insights from vehicle usage data while preserving user trust and privacy. Any such platform must be trustworthy and abide by security and privacy-by-design[11] principles, rather than having them retrofitted or treated as an afterthought, in light of the factors listed in **figure 1**.

Trustworthy Platform Framework

There is growing recognition within organizations to develop trustworthy AI to gain the trust of AI consumers (e.g., explaining how the system arrived at a decision, rather than just throwing out a decision). IBM's Trust in AI team notes that:

> *Artificial intelligence will be key to helping humanity travel to new frontiers and solve problems that today seem insurmountable...enhances human expertise...automates decisions and processes...But public trust in the technology is at a low point...we've seen multiple examples of AI that makes unfair decisions, or that doesn't give any explanation for its decisions, or that can be hacked.*[12]

Figure 2 shows a typical AI life cycle,[13] incorporating security by design and adopting governance best practices from regulations and standards.

The objective of the trustworthy AI platform is to provide a framework for the safe and ethical use of AI in connected car ecosystems and build fairness, transparency and trust in AI-assisted decision-making systems. Furthermore, the trustworthy AI platform treats continuous feedback as an important cog in the wheel, as it helps periodically evaluate the accuracy of the AI model in its build, train, test and deploy phases and monitors any drift in performance that could introduce bias or render predictions meaningless or inaccurate.

Data Ingestion, Training and Testing

The platform should also account for secure and ethical AI. This is where data and algorithms converge to form predictive or prescriptive models, and where an error in training data, also known as noise in an AI/ML context, makes it low-quality data, or poisoned data—if intentionally induced—and could result in inaccurate and misleading predictions.

Model Deployment and Monitoring

Even accurate and insightful predictions may become inexplicable due to their complexity, reducing the trust factor of such platforms. Hence,

Figure 1—Factors Impacting Human Elements of Security and Privacy in Connected Cars

Factor	Threat	Potential Mitigation Process
Profiling and automated decision-making	Denial of legitimate services (e.g., loan application rejected)	Conduct a data privacy impact assessment.
Bias and ethical issues	Moral machine dilemma scenarios[a]	Use high-quality, clean data for training and testing.
Insecure AI and ML algorithms	Attacks such as algorithm poisoning and adversarial ML[b]	Train ML models using adversarial samples to embed robustness by design against attacks on ML models for early detection and mitigation.
Trust deficit	Black box models	Leverage explainable AI[c] tools such as SHapley Additive exPlanations (SHAP) and local interpretable model-agnostic explanations (LIME) to help consumers of the models to understand and interpret why a decision was made by the system.
Inaccurate data in the models	Data poisoning	Legal recourse to privacy rights by data subjects based on privacy regulations such as the EU General Data Privacy Regulation (GDPR) and US State of California Consumer Privacy Act (CCPA)
Lack of security awareness	Social engineering attacks	Enhance efforts to build connected car security awareness.
Confidential data leakage	Intentional or unintentional PII leakage, model stealing attacks	Deploy strong access control mechanisms, data encryption at rest and in transit, federated learning (FL), anonymization, and proactive monitoring.
Inherent software vulnerabilities	Malware, ransomware, advanced persistent threats (APTs)	Implement application security best practices such as Open Web Application Security Project (OWASP),[d] mobile, IoT Top 10 and SANS Top 25.[e]

Source: (a) Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts, USA, Moral Machine, *https://www.moralmachine.net/*, (b) GitHub, "Adversarial Machine Learning 101," *https://github.com/mitre/advmlthreatmatrix/blob/master/pages/adversarial-ml-101.md#adversarial-machine-learning-101*, (c) Phillips, P. J., *et al.*; Draft NISTIR 8312: *Four Principles of Explainable Artificial Intelligence*, National Institute of Standards and Technology (NIST), USA, 17 August 2020, *https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable %20AI%20Draft%20NISTIR8312%20%281%29.pdf*, (d) Open Web Application Security Project (OWASP), *https://owasp.org/*
(e) SANS Institute, "CWE/SANS Top 25 Most Dangerous Software Errors," 20 August 2020, *https://www.sans.org/top25-software-errors/*

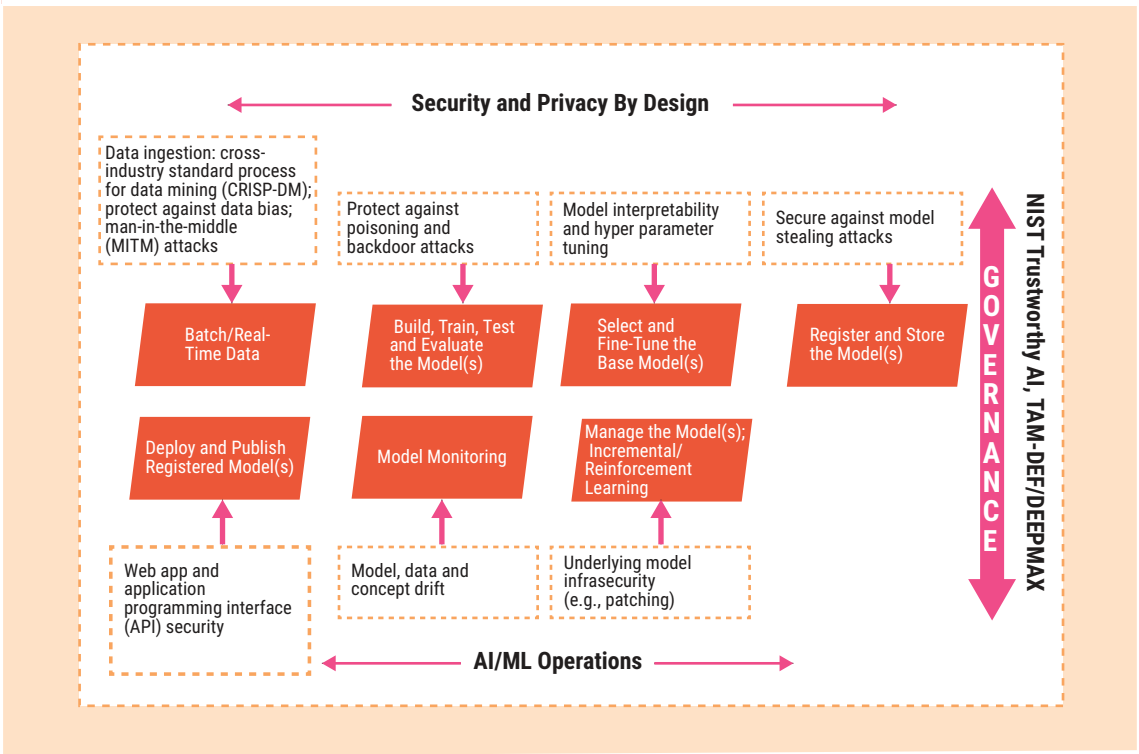
the platform must also incorporate explainable models such as SHAP and LIME so that predictions are accurate, explainable, ethical and free from bias. AI and ML operations become a critical governance component of the connected value chain for the AI committee, comprising representatives from the board, executive leadership, business, legal and security, to provide strategic directions on business requirements from AI solutions; oversee its relevance and outcome to the business; and decide whether a model requires retraining or needs to be retired. In fact, throughout the AI life cycle, key roles such as business leaders; data scientists; security architects; compliance, privacy and legal experts; solution architects; ML engineers; software engineers; data analysts; IT teams; and developers must work in conjunction and take responsibility to deliver trust and value in the platform.

AI Platform and Model Governance

A complex, technology-driven platform used to deliver or facilitate life-impacting decisions requires close oversight for any deviation from its intended purpose. For example, the AI policy of Tamil Nadu, India, outlines a six-step framework that addresses six core challenges in AI, represented by the acronym TAM-DEF, along with AI solution evaluation criteria scorecard DEEP-MAX[14] within the Tamil Nadu Government's vision of safe and ethical AI. These governance metrics provide necessary guidance for developing ethical AI.

The US National Institute of Standards and Technology (NIST) trustworthy AI initiative proactively engages in the development of AI technical standards with the goal of ensuring that

Figure 2—Trustworthy AI Platform for Connected Devices



Source: Adapted from European Union Agency for Cybersecurity (ENISA), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence*, Greece, December 2020, *https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges*

they minimize vulnerability to attacks by malicious actors and reflect US or any federal priorities for innovation, public trust and public confidence in systems that use AI technologies.[15] NIST's AI trustworthiness standards include guidance and requirements for accuracy, explainability, resilience, safety, reliability, objectivity and security.

The TAM-DEF/DEEP-MAX framework not only aligns with NIST's vision of trustworthy AI, but it also relates to the objective of the US Algorithmic Accountability Act of 2019,[16] which, as of the time of this writing, is a US bill. Other open source tools and frameworks provide metrics such as fairness and are great resources for guidance.[17]

Conclusion

Security and privacy cannot be an afterthought for any new technology and must be built into the processes, especially for connected cars, as it could be a matter of life and death in case of inaccurate prediction. Those processes must account for adversarial attacks on the algorithms that give more power to the connected car ecosystem, where the inputs are influenced to provide incorrect predictions. Researchers have demonstrated how a connected car can be hijacked or hacked to control the opening and closing of doors, suddenly apply brakes or take control of infotainment systems.[18] Combined with the risk of PII breaches, APTs, bad actors exploiting connected devices to leverage adversarial machine learning (AML), and a lack of consideration for security and privacy by design, this is a recipe for disaster.

Factors such as bias, ethics, security and privacy must be looked at holistically and embedded wherever possible into the platform or solution upon which the connected car value chain is so heavily-dependent. Frameworks and standards such as TAM-DEF and NIST's concept of trustworthy AI demonstrate the efforts of audit and governance oversight, enhancing human trust in connected platforms.

Endnotes

1 Howarth, D.; "Uber Taxi Kills Woman in First Fatal Accident Between a Pedestrian and a Self-Driving Car," Dezeen, 19 March 2018, *https://www.dezeen.com/2018/03/19/self-driving-uber-kills-pedestrian-arizona/*

2 Deichmann, J.; B. Klein; G. Scherf; R. Stuetzle; "The Race for Cybersecurity: Protecting the Connected Car in the Era of New Regulation," McKinsey and Company, 10 October 2019, *https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-race-for-cybersecurity-protecting-the-connected-car-in-the-era-of-new-regulation#*

3 Yadron, D; D. Tynan; "Tesla Driver Dies in First Fatal Crash While Using Autopilot Mode," *The Guardian*, 1 July 2016, *https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk*

4 Tesla, "An Update on Last Week's Accident," 30 March 2018, *https://www.tesla.com/blog/update-last-week%E2%80%99s-accident*

5 Greenberg, A.; "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse," *Wired*, 1 August 2016, *https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/*

6 Goyal, A.; "How Will Industry Move to Data Monetization With EVs and Connected," ET Auto, 22 July 2019, *https://auto.economictimes.indiatimes.com/news/auto-technology/how-will-industry-move-to-data-monetization-with-evs-and-connected/70329403*

7 McKinsey and Company, *Monetizing Car Data: New Service Business Opportunities to Create New Customer Benefits*, USA, September 2016, *https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/monetizing%20car%20data/monetizing-car-data.ashx*

8 Prescient and Strategic Intelligence, *Connected Car Market Research Report*, India, July 2020, *https://www.psmarketresearch.com/market-analysis/connected-car-market*

9 Dhami, I.; "Top Five Threat Vectors in Connected Cars and How to Combat Them," *SecurityIntelligence*, 2 October 2020, *https://securityintelligence.com/posts/automotive-cybersecurity-attack-vectors-in-connected-cars/*

10 Huq, N.; C. Gibson; R. Vosseler; *Driving Security Into Connected Cars: Threat Model and Recommendations*, *Trend Micro*, Japan, 18 August 2020, *https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf*

11 Agarwal, P. K.; C.T. Howell; "Addressing Privacy and Security Issues in the Connected Car," *Industry Week*, 2 February 2017, *https://www.industryweek.com/technology-and-iiot/emerging-technologies/article/21998478/addressing-privacy-and-security-issues-in-the-connected-car*

12 Boinodiris, P.; "Getting to Trustworthy AI," Venture Beat: The Machine, 14 March 2021, *https://venturebeat.com/2021/03/14/getting-to-trustworthy-ai/#:~:text=Join%20Transform%202021%20for%20the,problems%20that%20today%20seem%20insurmountable*

13 European Union Agency for Cybersecurity (ENISA), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence*, Greece, December 2020, *https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges*

14 Tamil Nadu e-Governance Agency, *Tamil Nadu Safe and Ethical Artificial Intelligence Policy 2020*, India, 10 September 2020, *https://elcot.in/sites/default/files/AIPolicy2020.pdf*

15 National Institute of Standards and Technology, Exploring AI Trustworthiness: Workshop Series Kickoff Webinar, USA, 6 August 2020, *https://www.nist.gov/news-events/events/2020/08/exploring-ai-trustworthiness-workshop-series-kickoff-webinar*

16 Jones Day, "Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence," June 2019, *https://www.jonesday.com/en/insights/2019/06/proposed-algorithmic-accountability-act*

17 Janeway Bills, N.; "3 Open Source Tools for Ethical AI," Atlas Research, *Medium*, 23 October 2020, *https://medium.com/atlas-research/ethical-ai-tools-b9d276a49fea*

18 Barzilai, D.; "Protecting the Modern Infotainment System," IoT Agenda, *Tech Target*, 13 May 2019, *https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Protecting-the-modern-infotainment-system*

Enjoying this article?

- Read *Emerging Technologies: Artificial Intelligence Fundamentals Study Guide. www.isaca.org/emerging-tech-ai*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums.*