# Beyond the Dashboard: Unseen Cybersecurity Vulnerabilities Caused by User Behaviour in Connected and Autonomous Vehicles Systems

**Dimah Almani**
Shaqra University, Saudi Arabia

dimah.almani2@nottingham.ac.uk
dalmanea@su.edu.sa

**Abstract:** As Connected and Autonomous Vehicles (CAVs) become increasingly integrated into Intelligent transportation systems, cybersecurity is no longer limited to protecting onboard technologies—it must also account for the everyday digital behaviours of the users who manage and interact with these vehicles. This paper introduces the concept of the "behavior-driven cyber-risk layer" in CAVs, a hidden but critical vulnerability surface created not by system flaws, but by routine user actions surrounding the vehicle ecosystem. Although CAVs rely on advanced communication, sensors, and cloud connectivity, small human habits—such as ignoring software update alerts, connecting infotainment systems to insecure personal devices, oversharing trip information, accepting unverified apps, or reusing credentials across applications—can undermine even the most sophisticated vehicle security architectures. This study examines how these seemingly minor behaviors interact with CAVs' security mechanisms, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, certificate-based authentication, and onboard digital systems. We show how attackers exploit predictable user routines—such as uploading navigation routes to cloud platforms, pairing phones via Bluetooth, or trusting unsolicited messages that appear to come from vehicle services—to introduce false data, manipulate trust decisions, or gain unauthorized access. Through real-world scenarios, we demonstrate how small mistakes can escalate into larger risks, enabling targeted tracking, spoofed messages, or remote access to vehicle functions. Instead of treating these behaviours as psychological tendencies, this paper frames them as operational cybersecurity weaknesses that directly affect the safety and reliability of CAVs. To illustrate, existing user awareness strategies are evaluated to highlight why they fail in high-convenience environments, where users expect seamless automation and often overlook security steps. Finally, a set of human-centered cybersecurity practices are proposed that are designed specifically for CAVs ecosystems, including simplified interface warnings, context-aware security prompts, secure-by-default connectivity options, and automated verification mechanisms that reduce reliance on user judgment. By revealing the hidden risks embedded in everyday interactions, this work emphasizes that the cybersecurity of CAVs depends not only on the technology itself, but also on how people engage with it.

**Keywords:** Vulnerabilities, Behaviours, CAVs, Security, Transportation, V2V, Attacks, Safety, Awareness

## 1. Introduction

In Intelligent Transportation Systems (ITS), Connected and Autonomous Vehicles (CAVs) form the core of the smart driving system, and they are rapidly becoming the primary component in ITS. In CAVs, the vehicles communicate with each other, forming Vehicle-to-Vehicle (V2V) communications, and communicate with the infrastructure around them, forming Vehicle-to-Infrastructure (V2I) communications (Falcone et al., 2007). CAVs rely on a sophisticated system of Onboard Units (OBUs), including sensors, radar, lidar, camera, and digital services to enable different levels of automation, efficient driving, and user safety. The automation levels in CAVs range from low level (0) to high level (5) (SAE International, 2021), and in each level the vehicle has different features as shown in Figure1. While significant research efforts have focused on securing vehicle hardware, communication protocols, and backend infrastructures, cybersecurity in CAVs cannot be fully addressed by technical mechanisms alone (Almani, 2024). In addition, much attention has been given to protecting (V2V) and (V2I) communications, certificate-based authentication, and onboard control systems, but a critical vulnerability surface remains largely overlooked: the everyday digital behaviors of users interacting with the vehicle ecosystem. The main contribution of this paper is a structured analysis of how predictable user behaviors interact with CAV security mechanisms and create exploitable attack paths. Through real-world-inspired scenarios, we demonstrate how attackers leverage these behaviors to introduce false data, manipulate trust decisions, or gain unauthorized access to vehicle systems. Rather than framing these behaviors as psychological shortcomings, we treat them as operational cybersecurity weaknesses that directly impact safety, reliability, and trust in CAV environments.

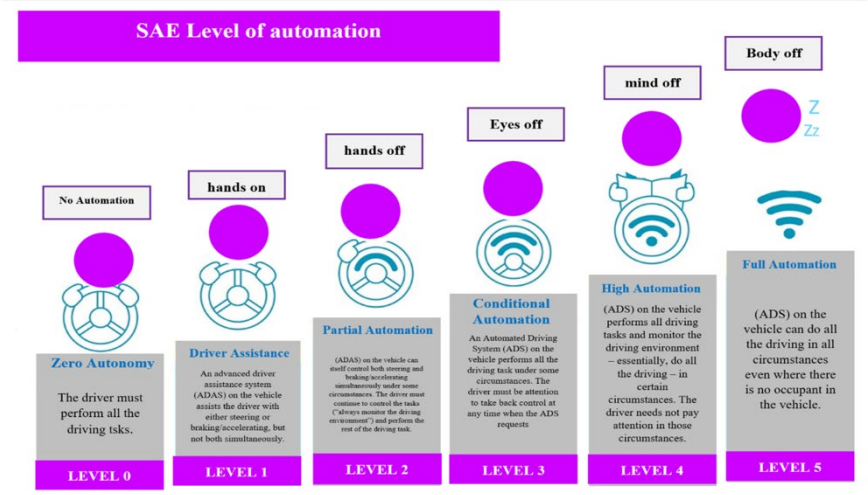


**Figure 1: SAE Levels of Automation (SAE International, 2021)**

## 2. Background: Security Architecture of CAV Ecosystems

In ITS, the more vehicles are connected, the more they will be able to obtain drastic enhancements in driving environment safety and traffic flow optimization, and consequently, offer a full set of services for passengers and drivers. CAVs operate within a highly interconnected digital ecosystem composed of multiple security-sensitive components. These include onboard electronic control units (ECUs), infotainment systems, wireless communication modules, mobile devices, and cloud-based services (Khanmohamadi & Guerrieri, 2024). This section discusses the key concepts of CAVs networks and their integration into autonomous vehicles, highlighting the importance of network infrastructure and connectivity. Recent research on CAV cybersecurity has primarily focused on securing communication protocols, intrusion detection mechanisms, and cryptographic authentication systems. However, relatively limited attention has been given to the role of user interaction and behavioral patterns in shaping the overall attack surface of CAV ecosystems. Several studies highlight the growing importance of human factors in cyber-physical systems, yet their integration into vehicle cybersecurity architectures remains largely unexplored.

### 2.1 Communication and Trust Mechanisms

CAVs are highly dependent on V2V communications as well as V2I communications to exchange safety messages, traffic messages, as well as environment messages. These communications often employ certificate-based authentication frameworks, such as public key infrastructure, to verify message integrity as well as authenticity (Almani et al., 2022). Messages are often deemed to be from trustworthy sources if they appear to be so after cryptographic analysis. Although these measures can and indeed are intended to prevent attacks by malicious third parties, they tacitly presuppose that the rest of the digital world, and specifically user-controlled interfaces, will be safe (Zhang et al., 2021).

### 2.2 User Interaction Points

Modern CAVs present various interaction opportunities for the user, such as infotainment systems, mobile applications, cloud-based dashboards, and the use of external services. The most common interactions occur through the smartphone via Bluetooth and/or USB connectors, data synchronization from navigation systems to the cloud, as well as the installation of applications. These interaction points serve as the bridges between the safe interior of the vehicle and the larger, more uncontrolled digital world. These interaction zones can often rely for their security upon the choices of users, making it an essential area in terms of the overall attack surface (Chattopadhyay et al., 2020). From the above discussion, it can be noticed that the CAV ecosystem is a complex, multi-layered environment that depends not on a single layer for security but rather a complex array that comprises various levels such as physical devices, networks, application-level systems, cloud services, backend services, in addition to those managed by the user for interaction. Each level has a unique mechanism for protection, which in turn faces a specific source for threats but, at the same time, could affect the entire environment's reliability (Bendiab et al., 2023).

For this particular environment, a conceptual model for identifying the various levels, a quick reference table (Table 1) has been prepared below that defines the levels, the components, methods, in addition to identifying the distinct source for each, while identifying, with particular emphasis, the source for behavioral cyber risks.

**Table 1: Security Layers in Connected and Autonomous Vehicle Ecosystems**

| Security Layer | Primary Components | Typical Protection Mechanisms | Common Threat Sources |
|---|---|---|---|
| **Physical Layer** | Sensors, ECUs, onboard hardware | Tamper resistance, secure boot | Physical access, hardware attacks |
| **Network Layer** | V2V, V2I, wireless channels | PKI, certificates, encryption | Message spoofing, replay attacks |
| **Application Layer** | Infotainment, vehicle apps | Access control, sandboxing | Malware, vulnerable applications |
| **Cloud & Backend Layer** | Navigation services, data storage | Authentication, secure APIs | Data breaches, credential theft |
| **Behavior-Driven Cyber-Risk Layer** | User-device interaction, cloud usage, update decisions | User prompts, policies (often weak) | Exploitable user routines, trust misuse |

## 3. The Behavior-Driven Cyber-Risk Layer

The behavior-driven cyber-risk level: This pertains to risks that are not due to weaknesses in cryptographic methods or software bugs but are a result of common user behavior that affects the security level of CAVs negatively (Negash and Yang, 2023).

### 3.1 Most Common Risk

Various common practices make up such a hidden risk stratification level:

- Ignoring or putting off vehicle software and firmware updates
- Integration of infotainment systems with personal devices that are either unsecured or already compromised
- Shared credentials for all vehicle-related services, mobile applications, and cloud platforms
- Oversharing trip information, location data, and vehicle status via third-party applications
- Accepting unverified applications/permissions

These are usually practiced due to convenience, lack of time, or overreliance on technology. To demonstrate how such behaviors can be interpreted in tangible security threats, Table 2 outlines the principal actions taken by the user, points of interaction, and possible security consequences in the CAV environment.

**Table 2: User Behaviors and Their Security Implications in CAV Ecosystems**

| User Behavior | Interaction Point | Exploited Weakness | Potential Impact |
|---|---|---|---|
| **Ignoring software update alerts** | Onboard system / mobile app | Unpatched vulnerabilities | Remote exploitation, system compromise |
| **Pairing insecure personal devices** | Bluetooth / infotainment | Trusted device abuse | Unauthorized access, data leakage |
| **Reusing credentials** | Vehicle apps, cloud platforms | Weak identity separation | Account takeover, tracking |
| **Oversharing trip data** | Cloud navigation services | Data exposure | Targeted surveillance, profiling |
| **Accepting unverified applications** | Vehicle app ecosystem | Lack of app validation | Malware installation, system manipulation |

### 3.2 Why These Behaviors Matter

CAV security architectures are envisioned to be designed in the belief that the cryptographic trust is sufficient to engender trust (Tu et al., 2025). Nevertheless, when the attack is based on the user behavior, there is an opportunity to circumvent the trust in an indirect manner. For example, if the mobile device is compromised and used in a vehicle, it becomes possible to enter the system as a trusted relay without violating the

cryptographic trust. This layer is particularly dangerous as it stays hidden in the threat space and security analysis.

## 4. Attack Scenarios Exploiting User Behavior

In spite of the seemingly low-level nature of the risks facing individual users, the group of attackers may utilize these risks systematically to circumvent the conventional CAV security. Through the exploitation of the patterns of behavior of the users or the safe communication pathways between the users and the vehicle, the attackers may obtain false input and gain indirect vehicle access or influence the trust models of the systems. Some of the scenarios accounting for the attack vectors resulting from the patterns of the behavior of the users are presented below.

### 4.1 Cloud-Based Route and Data Sharing

Many CAV users tend to share their navigation routes and trip history data in cloud services. Attackers who obtain access to such cloud services using either credential reuse attacks or phishing attacks may be able to ascertain the predictable patterns of their driving behavior (Wu et al., 2025). In other advanced attacks, the affected car ecosystem may receive their altered route data. Route data manipulation may occur through several technical attack vectors. For example, attackers may exploit compromised cloud navigation accounts, GPS spoofing techniques, or malicious third-party navigation applications to inject falsified route information. In such cases, altered navigation instructions may redirect vehicles toward unintended routes or manipulate traffic flow. Because many CAV services synchronize route data through cloud platforms and mobile applications, compromised credentials or insecure APIs can allow attackers to modify stored route information that is later downloaded by the vehicle.

### 4.2 Bluetooth and Infotainment Exploitation

Connecting smartphones to the in-car entertainment systems in a vehicle is also a common phenomenon. Several known Bluetooth attack vectors can exploit these connections. Examples include Bluesnarfing, where attackers gain unauthorized access to data stored on paired devices; BlueBorne, which enables remote code execution through vulnerable Bluetooth implementations; and Man-in-the-Middle attacks, where malicious devices intercept communications between the vehicle and a connected smartphone. These attacks can allow adversaries to access sensitive information, inject malicious commands, or manipulate data exchanged between the vehicle and external services. An attacker, in case the system is compromised, can take advantage of the trust involved in the connection and send malicious information, read credentials, and even tap into information exchanged between the car and the server.

### 4.3 Spoofed Service Messages and Trust Manipulation

The messages that most users tend to believe come from car services like maintenance notifications and update notifications. The attacker takes advantage of this by sending users spoofed notifications to update malware, provide excessive permissions, or provide sensitive information (Tekkesinoglu et al., 2025). After the creation of this trust through user engagement, the attacker injects false information into the V2V or V2I system chain to indirectly affect decision-making processes.

## 5. Limitations of Existing User Awareness Approaches

Conventional methods for enhancing awareness and security practices among computer users call for educating and warning users, and then following security guidelines and best practices, and it is expected that a security-aware user will make security-informed choices most of the time. The aforementioned conventional approach is not very effective for a CAV environment, wherein users demand a good deal of automation and functionality with seamless connectivity and very less cognitive efforts while using a system and services (Sevinch, 2024). Frequent reminders for security in high-convenience systems are disregarded because complex warnings are viewed more as impediments than as security solutions. It can cause users to resist and disregard notifications related to security because they do not fully understand their meaning. This is because people believe that secure-by-design safety-critical systems in vehicles are self-protecting and do not necessarily require active user participation for their security.

In addition, knowledge-based approaches are based on the idea that consumers are well-informed about technology risks involved in device pairing, permission handling in applications, data sharing in cloud environments, as well as login methodologies. However, consumers are often left in ignorance about processes that occur in the background, making it impossible to analyze risks. In this manner, consumers might

unknowingly grant permissions that lead to risks in the motor environment. A major drawback of awareness approaches is that they are of a reactive, rather than preventive, nature. These approaches seek to mitigate problems after potentially risky behaviors have taken place, rather than proactively employing system design principles that can pre-emptively prevent the risks from being realized (Butler et al., 2021). This is especially concerning in safety-critical application areas like transportation, which can be directly influenced by human error, not just concerning individual privacy but system-wide issues.

Hence, the applicability of defense mechanisms based on awareness does not scale well in practical CAV deployment, especially with the growing automation of vehicles and integration of CAV systems into everyday life. This emphasizes the importance of having effective remedies related to CAV security, promoting the responsibility of the CAV system itself, apart from humans, regarding reminders, restrictions, or the process of verification. To further clarify these limitations, Table 3 summarizes common awareness-based security strategies, their intended objectives, and the reasons why they are ineffective or impractical within CAV environments. This comparison highlights the gap between traditional user-focused defenses and the operational realities of highly automated vehicle systems.

**Table 3: Evaluation of Existing User Awareness Approaches in CAV Environments**

| Awareness Strategy | Intended Goal | Limitation in CAV Context |
|---|---|---|
| **Security warnings** | Inform users of risk | Often ignored due to automation |
| **User training** | Improve decision-making | Not scalable or timely |
| **Policy compliance** | Enforce safe behavior | Difficult to monitor |
| **Manual confirmations** | Prevent accidental actions | Causes fatigue and frustration |
| **Informational dashboards** | Increase transparency | Overwhelming for non-expert users |

## 6. Behavior-Aware Security Framework for CAV Ecosystems

This section presents the **Behavior-Driven Cyber Risk Layer Framework (BDCRL)**, a behavior-aware security architecture that integrates user interaction monitoring with existing CAV security mechanisms.It does not seek to replace cryptographic protections or network-level defenses; rather, the aim is to complement them by considering risk introduced through routine user behaviors and external device interactions. This framework operates within the scope of three interconnected domains: user interaction interfaces, vehicle onboard systems, and cloud services. In this regard, correlating activity across these domains, a system should be able to identify behavior patterns that elevate cyber risk and apply targeted mitigation strategies. Figure 2 provides an overview of this process by illustrating how data flows from user interaction interfaces, onboard vehicle systems, and cloud services into a central behavioral risk analysis component, where risk levels are assessed and translated into adaptive trust adjustments and automated mitigation actions. This visual representation clarifies the cross-layer operation of the framework and highlights how behavior-driven risks are addressed before they impact safety-critical CAV functions.

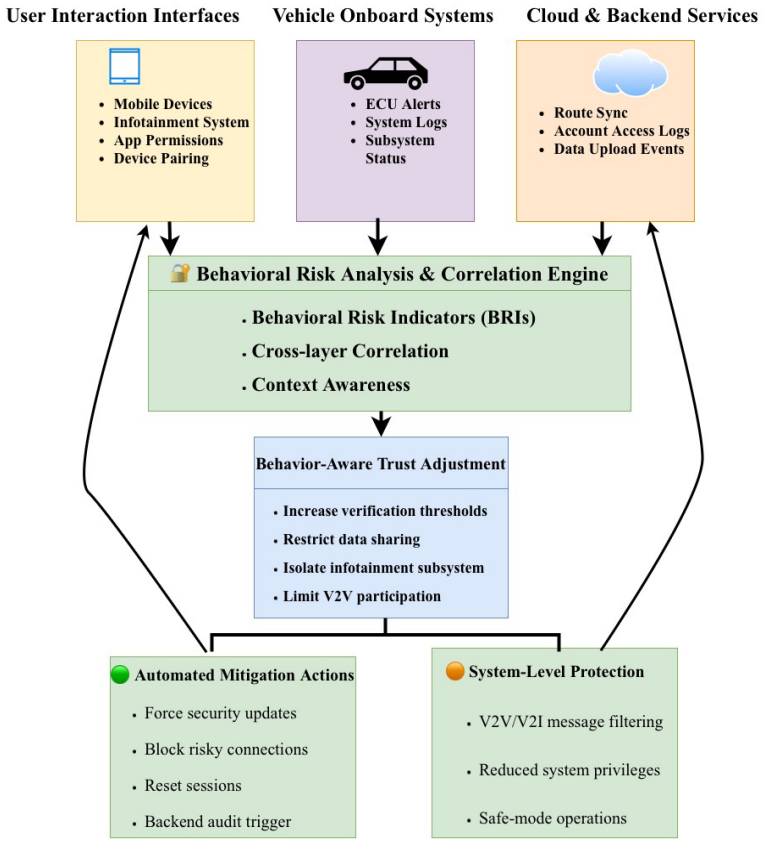


**Figure 2: Behavior-Driven Cyber Risk Layer (BDCRL)**

### 6.1 Behavioral Risk Indicators

The first component of the framework defines a set of BRIs that represent actions known to increase the probability of security compromise. These are derived from the common user behaviors that one can find in modern CAV ecosystems, such as:

- Repeated postponement of critical software updates
- Frequent pairing with new or unknown devices
- Installation of third-party applications outside verified ecosystems
- Reuse of authentication credentials across services
- Excessive sharing of location and trip data with external platforms

Each indicator is assigned to a risk weight based on the risk of degrading the overall security of the system. These weights may vary depending on the context in which the vehicle is moving, whether in autonomous mode, interacting with the roadside infrastructure, or in cooperative driving patterns.

### 6.2 Cross-Layer Risk Correlation

Unlike traditional intrusion detection systems that focus on network traffic or system logs, BDCRL performs cross-layer risk correlation by combining:

- Interface-level interaction logs (e.g., pairing events, permissions granted)
- Vehicle subsystem alerts (e.g., infotainment anomalies, ECU access attempts)
- Cloud-side access and synchronization activity

In correlating these data types, it becomes possible for the system to recognize risk patterns in compounds that individually may be harmless but in combinations suggest something different. In other words, a new device, unusual access to the cloud, and failed log-ins suggest more than simple device failure. By considering the totality of behavioral and system-level indicators, the framework can prioritize patterns that are more likely to represent coordinated or escalating security threats. The reasons behind this are that a strong correlation can facilitate

early identification of attack vectors driven by behavior before they are involved in safety-critical decision-making processes (Almani and Furnell, 2025), such as V2V trust assessment or control of navigation.

### 6.3 Behavior-Aware Trust Adjustment

The framework introduces a behavior-aware trust adjustment mechanism that influences how vehicle systems evaluate incoming data and external interactions. When elevated behavioral risk is detected, the system can:

- Increase verification thresholds for external messages
- Restrict non-essential data sharing
- Temporarily isolate infotainment and user-connected subsystems
- Limit participation in cooperative V2V decision-making

This dynamic trust adjustment prevents compromised user interfaces from indirectly influencing safety-critical functions. Importantly, trust modification occurs at the system level rather than requiring manual user intervention.

### 6.4 Automated Mitigation and User Guidance

To minimize reliance on user decision-making, mitigation actions are primarily automated. However, when user input is required, the framework provides *context-aware guidance* rather than generic warnings. For instance, instead of displaying a vague security alert, the system may indicate that recent device connections increase risk during cooperative driving and recommend postponing non-essential connectivity.

Automated responses may include:

- Enforcing immediate critical updates when risk is elevated
- Blocking high-risk device connections
- Resetting compromised authentication sessions
- Triggering backend security audits

This approach balances usability with protection, ensuring that safety is not compromised by delayed or ignored user actions.

### 6.5 Scenario-Based Validation

For the purpose of testing the feasibility of BDCRL, typical usage scenarios that involve CAVs were examined. These usage scenarios involved cloud-based navigation synchronization, device pairing, as well as service messages. Within these scenarios, the framework was successful in detecting the conditions that pose a higher level of risk prior to making any impact on the trust between V2V or V2I communication. For instance, for route synchronization scenarios, irregular login instances and late updates contributed to trust reduction for external data entry, thereby ensuring that misleading route information does not affect navigation systems. For infotainment pairing scenarios, continuous connectivity attempts from former unknown entities resulted in automatic subsystem isolation, thereby avoiding horizontal access for vehicle services (Ignatious et al., 2023).

### 6.6 Integration with Existing CAV Security Architectures

BDCRL is designed to be compatible with existing CAV security infrastructures, including certificate-based authentication, secure communication protocols, and backend anomaly detection systems. Behavioral risk scores do not replace cryptographic validation but complement it by adding contextual awareness to trust decisions. The framework uses lightweight behavioral indicators based on existing vehicle logs such as device pairing, update delays, and authentication attempts. Risk analysis can be performed locally within the vehicle, while more complex processing may be offloaded to edge or cloud systems, minimizing computational overhead on safety-critical components. This layered integration supports a more realistic threat model in which trusted vehicles may still act as compromised intermediaries due to unsafe interaction patterns. By recognizing this possibility, CAV systems can make more conservative and informed security decisions ins high-risk operational contexts.

## 7. Discussion

The behavior-driven cyber-risk layer challenges the assumption that cybersecurity in CAVs can be achieved solely through technical robustness. Even highly secure systems can be undermined by predictable user behaviors that attackers exploit strategically. Recognizing user interaction as a core part of the threat model enables a more realistic assessment of CAV security and highlights the importance of integrating human-centered design

principles into cybersecurity strategies (Xu et al., 2024). While behavioral monitoring can improve cybersecurity in CAV ecosystems, it also raises privacy concerns. To address this, behavioral indicators should minimize or anonymize personally identifiable information whenever possible. Many indicators can be processed locally within the vehicle, reducing the need to transmit user data externally. In addition, compliance with data protection regulations such as GDPR requires transparent data handling and minimal data retention. Therefore, privacy-preserving monitoring is essential for the secure deployment of BDCRL.

The results in this work indicate that cybersecurity concerns for Connected and Autonomous Vehicles cannot be holistically addressed by targeting only technical safeguards such as cryptographic authentication, secure communication protocols, and intrusion detection mechanisms. Inasmuch as such protections are necessary, the findings reveal that mundane user behaviors introduce a parallel vulnerability surface that operates outside the realm of traditional security models.This behavior-driven cyber-risk layer effectively bridges highly secured vehicle subsystems with less regulated personal digital environments, thereby weakening end-to-end system trust.

One of the most significant implications of this work is that many attack paths do not require attackers to compromise core vehicular systems directly (Yousseef et al., 2024). Instead, attackers exploit predictable user routines such as cloud synchronization, smartphone pairing, and reliance on automated services. As shown in Tables 2 and 3, these behaviors can undermine certificate-based trust mechanisms and allow false or manipulated data to propagate into V2V and V2I decision processes. This finding challenges the assumption that cryptographic validity alone is sufficient to ensure operational trust in CAV networks. Another important observation is that behavior-driven risks scale with system convenience. CAV ecosystems are explicitly designed to minimize user effort and maximize automation. The net result of this approach is that meaningful opportunities for effective human oversight are unintentionally reduced. In such environments, traditional cybersecurity awareness strategies become ineffective; users learn to trust system automation and to respond quickly to system prompts without questioning potential security implications. This study shows that real-world CAV usage patterns are poorly aligned with awareness-based defenses; thus, user vigilance is an unreliable mitigation strategy in safety-critical transportation systems (Decian & Jaafar, 2024).

This cybersecurity study further highlights a fundamental disconnect between how responsibilities are assigned for CAV cybersecurity and how these systems are actually used. Current security architectures implicitly place responsibility on users to manage updates, device pairing, and application permissions, despite the fact that users often lack visibility into system dependencies or potential consequences. Treating these behaviors as isolated user errors overlooks the structural role that system design plays in shaping user actions. Therefore, behavior-driven vulnerabilities should be regarded as design-level security issues rather than individual compliance failures. Human-centered cybersecurity practices aim to shift the responsibility for enforcing security from reactive end-user actions to proactive system-level processes. Through the implementation of secure-by-default connectivity, automated verification, and context-aware prompts, the risk of high-risk interactions based on user discretion can be significantly reduced within CAV systems. As summarized in Table 5, these practices complement existing cryptographic protections by targeting vulnerability points at the interfaces where humans interact with automated systems. Furthermore, in a broader context, the behavior-driven cyber-risk layer has significant implications for trust management schemes in vehicular networks. Existing trust models typically assume that malicious behavior originates from malicious vehicles themselves. However, this study demonstrates that legitimate vehicles may unintentionally act as carriers of malicious data or unauthorized access due to compromised user-controlled interfaces. This blurs the distinction between benign and malicious nodes and complicates misbehavior detection mechanisms that rely solely on message-level observations. Consequently, future trust and reputation systems must incorporate behavioral context and device provenance when assessing participant reliability in vehicular networks. Moreover, current regulatory and certification efforts for CAVs place strong emphasis on hardware reliability and software integrity, with limited consideration of security risks arising from user–device interactions. The results of this study indicate that certification frameworks should extend beyond technical compliance to include evaluation of interface design, update enforcement mechanisms, and secure integration with personal devices. Without such measures, certified vehicles may remain vulnerable through their surrounding digital ecosystems.

Finally, although this paper focuses on transportation systems, behavior-driven cyber risks are also evident in other domains, including smart medical devices, industrial IoT, and smart home environments. However, the safety-critical nature of transportation systems magnifies these risks, making CAVs a particularly urgent domain for addressing human–system security interactions. Recognizing human behavior as a contributing factor to

system security is therefore essential not only from a cybersecurity standpoint, but also for ensuring public trust and long-term adoption of autonomous vehicle technologies.

## 8. Conclusion

In this research paper, the behavior-driven cyber-risk layer in Connected and Autonomous Vehicles has been introduced, and the way in which everyday user behavior leads to hidden, yet highly important, security risks has been explained. By understanding how this user behavior combines with the security features of secure Connected and Autonomous Vehicles, it is evident that the problem of cybersecurity is not just a technological issue, but also a matter of everyday behavior that, at the moment, is not considered highly convenient. Therefore, in order to meet this demand, a set of human-centered approaches, specifically designed for the use of Connected and Autonomous Vehicles, is proposed, and it is necessary to understand that the safety of Connected and Autonomous Vehicles is not just a technological problem, but also a behavior issue.

**Ethics Declaration:** This study did not involve human participants, personal data, or animal subjects; therefore, ethical approval was not required.

**AI Use Declaration:** No AI-based tools were used in the preparation of this manuscript.

## References


Almani, D., & Furnell, S. (2025, June). Assessing the Security Vulnerabilities and Countermeasures of Connected and Smart Devices. In European Conference on Cyber Warfare and Security (pp. 9-17). Academic Conferences International Limited.

Almani, D. An innovative reputation system for trustworthy and secure vehicle-to-vehicle communication (Doctoral dissertation, University of Nottingham).

Almani, D., Furnell, S., & Muller, T. (2022, June). Supporting Situational Awareness in VANET Attack Scenarios. In ECCWS 2022 21st European Conference on Cyber Warfare and Security. Academic Conferences and publishing limited

Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*, *24*(4), 3614-3637.

Butler, L., Yigitcanlar, T., & Paz, A. (2021). Factors influencing public awareness of autonomous vehicles: Empirical evidence from Brisbane. *Transportation research part F: traffic psychology and behaviour*, *82*, 256-267.

Chattopadhyay, A., Lam, K. Y., & Tavva, Y. (2020). Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems*, *22*(11), 7015-7029.

Decian, J. and Jaafar, F., 2024, November. Wiki-IoT: Registering and Evaluating the Security and Resilience of Internet of Things and Connected Devices Using a Collaborative Platform. In 2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC) (pp. 9-14). IEEE.

Falcone, P., Borrelli, F., Asgari, J., Tseng, H. E., & Hrovat, D. (2007). Predictive active steering control for autonomous vehicle systems. *IEEE Transactions on control systems technology*, *15*(3), 566-580.

Ignatious, H. A., El-Sayed, H., Khan, M. A., & Mokhtar, B. M. (2023). Analyzing factors influencing situation awareness in autonomous vehicles—A survey. *Sensors*, *23*(8), 4075.

Khanmohamadi, M., & Guerrieri, M. (2024). Advanced Sensor Technologies in CAVs for traditional and smart road Condition Monitoring: a review. Sustainability, 16(19), 8336.

Negash, N. M., & Yang, J. (2023). Driver behavior modeling toward autonomous vehicles: Comprehensive review. *IEEE Access*, *11*, 22788-22821.

SAE International. (2021, May 2). *SAE levels of driving automation™ refined for clarity and refinements.* SAE International. https://www.sae.org/news/blog/sae-levels-driving-automation-clarity-refinements

Sevinch, Q. (2024, June). NETWORK SECURITY IN THE INTERNET OF THINGS (IOT): CHALLENGES AND PROSPECTS. InE Conference Zone (pp. 35-42).

Tekkesinoglu, S., Habibovic, A., & Kunze, L. (2025). Advancing explainable autonomous vehicle systems: A comprehensive review and research roadmap. *ACM Transactions on Human-Robot Interaction*, *14*(3), 1-46.

Tu, S., Zhou, X., Liang, D., Jiang, X., Zhang, Y., Li, X., & Bai, X. (2025). The role of world models in shaping autonomous driving: A comprehensive survey. *arXiv preprint arXiv:2502.10498*.

Wu, J., Xu, X., Cui, G., Zhang, Y., Qi, L., Dou, W., & Cai, Z. (2025). Fairness-Aware Budgeted Edge Server Placement for Connected Autonomous Vehicles. *IEEE Transactions on Mobile Computing*.

Xu, Z., Wang, C., Jiang, T., Liu, Z., & Zheng, N. (2024). Impediments to environmental awareness in autonomous driving systems and its effect on user adoption. *IEEE Transactions on Intelligent Vehicles*.

Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). Autonomous Vehicle Security: A Deep Dive into Threat Modeling.arXiv preprint arXiv:2412.15348.

Zhang, Q., Wang, X., Li, Z., & Wei, Z. (2021). Design and performance evaluation of joint sensing and communication integrated system for 5G mmWave enabled CAVs. IEEE Journal of Selected Topics in Signal Processing, 15(6), 1500-1514.