Work	Count	Location taxonomy	Count	Type taxonomy	Paper Title
Ours	**3** (8)	**Outside-vehicle** (Cloud platform, APP, Charging pile)**, In-vehicle** (IVI, ECU, T-Box, Radio)**, Network**	**9** (31)	**Authorization** (Unauthorized accessing, Weak password, Privilege escalation, Identity spoofing)**, Information leakage, Injection** (SQL injection, Command injection)**, OS** (Kernel, Arbitrary software installation, USB, Debug interface exposure, Upgrade forgery)**, DoS, File operation** (File accessing, File download, File tampering, File upload, File traversal, File delete)**, Interception** (Relay, Replay, Man-in-the-middle, GPS spoofing, Traffic hijacking, DNS hijacking)**, Web-specific** (XSS, Deserialization, Phishing, XXE), Memory (Buffer overflow, Integer overflow)	Uncovering Vulnerabilities in Intelligent Connected Vehicles

Paper\cite{pekaric2021taxonomy}	**3** (20)	**Physical Access** (On-board diagnostic port, ECUs, On-board computers, Modules, Media systems, Navigation system, dashboard)**, Close Proximity** (Bluetooth, Key/ignition, Sensors, Tire pressure monitoring system, Dedicated short range communication, Wi-Fi, WAVE, Voice controllable, Speech recognition system)**, Remote Access** (GPS, Radio, Cellular or mobile network, Internet)	**21** (48)	**Content spoofing** (Message tampering, Audio attack, Replay, GPS spoofing, GPS time spoofing, Camera/Radar/LiDAR spoofing)**, Identity spoofing** (Sybil attack, Falsified entities attack, Node impersonation, Repudiation attack, Key/Certificate replication)**, Manipulation of human behavior** (Illusion attack)**, Flooding** (Flooding attack, Routing table overflow)**, Sustained client engagement** (Bus-off attack, Spamming attack)**, Protocol manipulation** (TCP ACK storm)**, Software integrity attack** (ECU tampering, Rogue software update, Map database poisoning)**, Infrastructure manipulation** (Traffic control attack, Routing request modification, Routing cache poisoning, Black hole attack, Gray hole attack, Wormhole attack, Byzantine attack, Rushing attack)**, Obstruction** (Channel interference attack, GPS jamming, Camera/Radar/LiDAR jamming, Radio signal jamming, Key fob jamming)**, Traffic injection** (Message injection attack, Message fabrication attack)**, Local code execution** (Malware attack)**, Code inclusion** (Remote code execution)**, Exploiting trust in client** (Man-in-the-middle attack)**, Privilege abuse** (Man-at-the-end attack)**, Exploitation of trusted credentials** (Session hijacking)**, Interception** (Eavesdropping)**, Reverse engineering** (Side-channel attack)**, Footprinting** (ID disclosure attack, Location tracking attack, Trajectory tracking attack)**, Packet fuzzing, Password/Key attack, Timing attack**	A taxonomy of attack mechanisms in the automotive domain

Paper\cite{sommer2019survey}	**2** (28)	**Remote** (WLAN, Bluetooth, Cellular, GPS, digital video broadcasting-terrestrial (DVB-T)/digital video broadcasting-terrestrial, 2nd generation (DVB-T2), digital audio broadcasting (DAB), Radio, Tire pressure monitoring system (TPMS), Radio frequency identification (RFID), Infrared)**, Internal** (USB, Auxiliary, CD, DVD, ECU, Component, OBD, CAN, CAN FD, LIN, media oriented system transport (MOST), desktop-bus (D-Bus), FlexRay, Ethernet, Camera, LiDAR, radio detection and ranging (Radar), Software)	**6** (26)	**Spoofing** (Brute force, Man-in-the-middle, Hijacking, Replay)**, Tampering** (XSS, SQL injection, Firmware modification, Virus, Worm, Fuzzing, Adversarial attack)**, Repudiation** (Repudiation attack, Stealth attack)**, Information disclosure** (Eavesdropping, Trojan, Spyware, Reverse engineering, Cryptoanalysis, Portscanning, Side-channel-attack, Fingerprinting)**, Denial of service** (Distributed DoS, Jamming)**, Elevation of privilege** (Buffer overflow, Rootkit, Backdoor)	Survey and classification of automotive security attacks

Paper\cite{7917080}	7	ECUs, Sensors, GPS, Intra-vehicular links, V2V communication links, V2I communication links, V2IoT communication links	**2** (8)	**Physical Access** (Side-channel, Code modification, Code injection, Packet sniffing, Packet fuzzing, In-vehicle spoofing)**, Remote Access** (External signal spoofing, Jamming)	Autonomous Vehicle Security: A Taxonomy of Attacks and Defences

Paper\cite{9447840}	14	GPS, Lidar, Camera, Radar, CAN and SAE J1939 busses, Integrated business services, Machine learning systems, Password and key, Communicated data, ECUs, TPMS, Bluetooth, Key fob and keyless entry, Vehicle to everything network	**3** (17)	**In-vehicle network attacks** (Remote sensor attacks, GPS spoofing, Location trailing, Close proximity vulnerabilities, CAN and SAE J1939 buses vulnerabilities, ECUs software flashing, Integrated business services attacks)**, Vehicle to everything network attacks** (DoS, Impersonation, Replay, Routing attacks, Data falsification, Eavesdropping, Password and key attacks)**, Other attacks** (Infrastructure attacks, Slight attacks, Attacks on machine learning systems)	A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)

Paper\cite{LIMBASIYA2022100515}	**6** (13)	**Wireless Interfaces** (DSRC, Wifi, LTE, Bluetooth)**, Physical Ports** (USB, OBD-II)**, Keyless Entry Systems** (Remote Key)**, In-vehicle Network** (ECUs, CAN buses)**, Infotainment system** (Firmware-over-the-air Update)**, Perception Sensors** (Radar, LiDAR, Cameras)	10	Impersonation, DoS, Sybil, Modification, Replay, Injection, Side-channel, Fuzzing, Bus-off, Remote sensor	A systematic survey of attack detection and prevention in Connected and Autonomous Vehicles

Paper\cite{10226207}	**3** (23)	**CLOUD** (AI-based data analysis, Device management, Microservices management, Data management, Network management)**, FOG** (Software defined networking (SDN)/Time sensitive networking (TSN), Heterogeneous computing platform, Time series database, AI-based data analysis, Power management)**, EDGE** (Powertrain controller, Chassis safety controller, Body electronic controller, Infotainment system, Navigation system, Internal control bus, Artificial intelligence, Onboard computer systems, Onboard diagnostics systems, Data analysis and management, Network systems, Sensors, Power management)	**3** (19)	**SOFTWARE** (Fake node or sybil attack, Replay, AI/ML attack, Social engineering attack, System's availability, Denial of Sleep, Malicious code, Injection)**, NETWORK** (Man-in-The-Middle, Eavesdropping or sniffing, DoS, Routing attack, Gray hole, Black hole, Wormhole)**, HARDWARE** (Node-capture, Side-channel attack, Timing attack, Cryptanalysis attack)	An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles

Paper\cite{10500196}	**2** (7)	**Automotive Control System** (ECU, CAN)**, Automotive Driving System** (OBD, RADAR, Vision, LiDAR, GPS)	8	False Data Injection, Time Delay Switch, Denial of Service, Communication Jamming, Man in the Middle, Vehicular Ad-hoc Networks, Infotainment, Machine Learning based Attacks	Security of Connected and Autonomous Vehicles: A Review of Attacks and Mitigation Strategies

Paper\cite{10.1007/978-3-030-68887-5_15}	**3** (9)	**Vehicle** (Sensors, In-vehicle network, Vehicular communications)**, Environment** (Road signs, Traffic lights, Charging stations, Neighbor vehicles)**, Software and mobile applications** (Firmware updates, Internet-connected features)	6	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges	Autonomous Vehicle Security: Literature Review of Real Attack Experiments

Paper\cite{luo2022cybersecurity}	**2** (19)	**Penetration Testing** (GNSS, keyless entry, Cellular, Wifi, Bluetooth, IVI, Mobile app, Sensors, ECU, In-vehicle network, Debug interfaces, OBD), **Fuzzing** (Automotive system, SOME/IP, ECU Firmware, UDS, CAN FD, CAN, Bluetooth)	17	DoS, Channel attack, Privilege escalation, Heap overflow attack, Jamming, Blinding attack, Malicious app installation, Wireless attack, Replay attack, Spoofing, Data extraction/modification, Diagnostic attack, Injection attack, Tampering, Unauthorized access, Reverse engineering, Sniffing/Eavesdropping	Cybersecurity testing for automotive domain: A survey

Paper\cite{pham2021survey}	**8**	**OBD, ECUs, CAN, liDAR, Radar, GPS, Cameras, Communication mechanism**	-	-	