ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.1 / 2025 / pp.1-6
https://doi.org/10.69882/adba.cs.2025011

The Role of Technological Approaches in Cyber Security of Autonomous Vehicles

Ebubekir Seyyarer [*,1], **Faruk Ayata** [α,2] **and Selim Özdem** [β,3]

*Van Yüzüncü Yıl University, Computer Engineering, Van, 65090, Türkiye, [α]Van Yüzüncü Yıl University, Başkale Vocational High School, Van, 65090, Türkiye, [β]Hitit University, Alaca Avni Çelik Vocational High School, Çorum, 19030, Türkiye.

ABSTRACT Autonomous vehicles play a significant role in future transportation systems by enabling driverless travel. These vehicles offer advantages such as reducing accidents, improving travel times, and conserving energy. However, ensuring the independent operation of these technologies requires robust cybersecurity measures. Protecting autonomous vehicles against security threats they may face within their internal systems or during communication with other vehicles and infrastructure is crucial. This study examines the security measures used in autonomous vehicles. Encryption and data protection techniques safeguard information from unauthorized access during in-vehicle and inter-vehicle communication. Additionally, intrusion detection and prevention systems (IDS/IPS) detect abnormal activities to protect against potential threats. Machine learning-based anomaly detection methods analyze data from sensors and network traffic to identify emerging threats. Regular software updates help mitigate vulnerabilities, while network segmentation isolates different systems to protect critical components. Multi-layered security solutions ensure the safe operation of autonomous vehicles. These approaches contribute to the development of future security standards.

KEYWORDS
Autonomous vehicles
Cybersecurity threats
Autonomous vehicle security
Artificial intelligence

INTRODUCTION

Autonomous vehicle technologies have an important place among the transportation solutions of the future thanks to their ability to drive without driver intervention. Autonomous vehicles offer benefits such as reducing traffic accidents, optimizing travel times and increasing energy efficiency, and therefore have great potential for both individual users and social infrastructure. However, the ability of these vehicles to drive autonomously and safely requires the implementation of advanced safety measures. In particular, autonomous vehicles must be protected from cybersecurity threats that they may encounter both in their on-board systems and when communicating with other vehicles and infrastructure.

Cybersecurity methods developed to ensure the safety of autonomous vehicles provide a multi-layered structure that aims to protect vehicles against different types of attacks. This study discusses a wide range of solutions, from encryption techniques to enhance in-vehicle data security and communication security, to intrusion detection and prevention systems (IDS/IPS) used to detect anomalous behavior, to machine learning-based anomaly detection methods and physical security measures such as vehicle network segmentation. While encryption and data security prevent malicious individuals from intercepting data in the vehicle and in communication between vehicles, IDS and IPS systems provide protection against potential threats by detecting abnormal activity in the system.

In addition, anomaly detection based on machine learning analyzes the data obtained from vehicle sensors and network traffic, enabling the detection of unknown threats. In this way, an effective defense can be ensured even against previously unidentified types of attack. In addition, secure software and system updates enable the secure implementation of software updates for vehicles so that security gaps can be closed quickly. The segmentation of the in-vehicle network aims to isolate critical systems by dividing the network into different sections and preventing security risks from spreading to other systems.

Özarpa *et al.* (2021) examines the vulnerabilities in the wireless connectivity and operating systems of autonomous vehicles and states that these vulnerabilities should be detected using tools such as NMAP, Maltego and Metasploit. The study highlights that

Manuscript received: 10 December 2024,
Revised: 22 January 2025,
Accepted: 24 January 2025.

[1]eseyyarer@yyu.edu.tr (**Corresponding author**).
[2]fayata@yyu.edu.tr
[3]selimozdem@hitit.edu.tr

vehicles are vulnerable to external attacks and states that these vulnerabilities should be addressed with continuous monitoring and up-to-date security protocols. It is concluded that vehicle systems should be monitored regularly.

Çakal *et al.* (2021) addresses communication security issues between autonomous vehicles and explains the importance of lightweight security protocols, especially in vehicles with IoT sensors. The study evaluates cryptography algorithms and attack mitigation techniques, analyzes vulnerabilities in networks such as VANETs and recommends the use of lightweight encryption techniques. It concludes that lightweight cryptography algorithms support low-latency operation.

Durlik *et al.* (2024) examines threats such as remote hacking, sensor tampering and denial of service (DoS) in autonomous vehicles and evaluates the defense methods against these threats. The study examines encryption, IDS systems, regular updates and authentication methods and points to the potential of advanced technologies such as artificial intelligence and blockchain for cybersecurity. It notes that security problems persist due to the complexity of vehicles.

Abouabdalla and Goyal (2022) analyzes the most vulnerable areas in autonomous vehicles and offers solutions for points of attack such as GPS, sensors and network connections. The study proposes machine learning and data encryption techniques, but notes that the success of these methods has not been directly tested. Hypothetical solutions for the security of autonomous vehicles are developed.

Saeed *et al.* (2023) examines the current cybersecurity threats to connected and autonomous vehicles (CAV) and provides applicable solutions to these threats. The study analyzes attacks on LiDAR, GPS and other sensors and highlights the importance of authentication, data encryption and IDS methods. It also states that cooperation between manufacturers should be strengthened.

The multi-layered cybersecurity approaches examined in this study have the potential to contribute to the reduction of security vulnerabilities in autonomous vehicles and the creation of a sustainable security infrastructure. This study offers the following contributions:

- Standardization of Cybersecurity Protocols: Multi-layered security measures such as encryption, attack detection and prevention systems, and machine learning-based anomaly detection methods developed for autonomous vehicles should be brought together within the framework of international standards. This will increase compatibility between vehicle manufacturers and software developers and ensure that security vulnerabilities are prevented more effectively.
- Optimisation of Artificial Intelligence-Based Threat Detection Systems: Machine learning and artificial intelligence techniques should be optimised to dynamically detect security vulnerabilities in autonomous vehicles. These systems should be developed to predict not only current threats but also complex cyber attacks that may arise in the future.
- The present study proposes a more comprehensive testing and integration process for the verification of security measures employed in autonomous vehicles. The integration of security systems with diverse in-vehicle network structures and infrastructures is intended to establish an ecosystem that exhibits enhanced resistance to cyber threats.

The remainder of the study is structured as follows: the second section provides an exposition on in-vehicle and inter-vehicle data encryption security. The third section provides information about attack detection and prevention systems in autonomous vehicles.The fourth section provides an explanation of anomaly detection in the security systems of autonomous vehicles using machine learning methods.The fifth, sixth and seventh sections explain the installation of secure software in autonomous systems, the updating of the system, in-vehicle segmentation and physical security measures that can be taken. The final section of the study presents the results of the research and puts forward recommendations for future research and development in this field.

MATERIALS AND METHODS

Data Encryption Security

Encryption of data in vehicle and vehicle-to-vehicle communication is one of the cornerstones of modern cyber security procedures. This method plays a crucial role in ensuring the security of both individual vehicles and vehicle networks. Encryption techniques prevent malicious individuals from intercepting or manipulating this data by ensuring that the transmitted data can only be read by authorized recipients. Particularly in autonomous and connected vehicle technologies, encryption applications provide an important layer of security for GPS location data, sensor data, driving commands and vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications (Stallings 2016; Schneier 2007).

Strong encryption algorithms use a combination of symmetric and asymmetric encryption techniques to secure data (Figure 1 and Figure 2). Symmetric encryption uses the same key to encrypt and decrypt data, while asymmetric encryption uses a different key for encryption and decryption. These methods offer advantages in terms of speed and security. For example, symmetric algorithms such as AES (Advanced Encryption Standard) are efficient in terms of speed; asymmetric algorithms such as RSA (Rivest-Shamir-Adleman) provide a higher level of security.

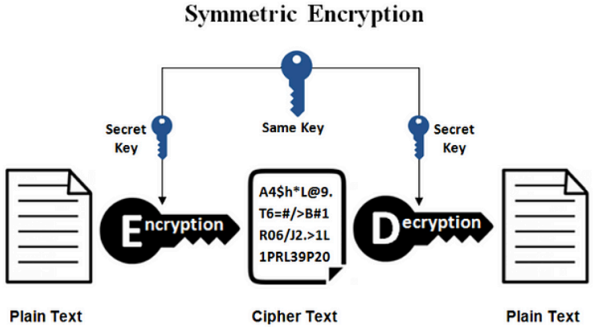

Figure 1 Symmetric encryption (Özkan 2020).

Intrusion Detection and Prevention Systems

In order to ensure network and system security in autonomous vehicles, intrusion detection and prevention systems are used. These systems identify abnormalities by learning normal behaviors and apply the necessary precautions (Scarfone and Mell 2007; Modi *et al.* 2013).

Intrusion Detection System (IDS): Intrusion Detection System (IDS) is a security solution used to detect threats by monitoring network traffic and system activities. IDS plays a critical role in detecting security breaches or attacks that may occur in a system. However, IDS provides a passive defense; it only detects and reports threats, but does not have the authority to directly

Table 1 Comparison of symmetric and asymmetric encryption (Avaroğlu 2022)

Subject	Symmetric	Asymmetric
Confidentiality	Provides	Provides
Integrity	-	Provides
Authentication	-	Provides
Non-repudiation	-	Provides
Performance	Fast	Slow
Security	Depends on key length	Depends on key length

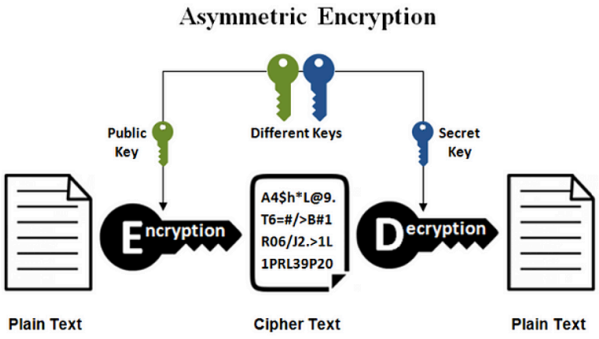

Figure 2 Asymmetric encryption (Özkan 2020)

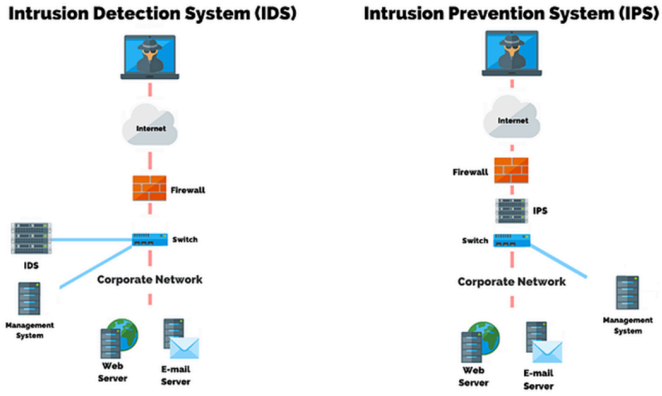

Figure 3 IDS and IPS working architecture (Aydogan 2022).

block or stop these threats. Therefore, IDS usually requires manual intervention by security teams (Northcutt and Novak 2002).

IDS has two basic modes of operation: Network-Based IDS (NIDS) and Host-Based IDS (HIDS). NIDS analyzes network traffic to detect anomalous behavior or known attack patterns. For example, it scans data packets on the network to identify intrusion or malicious traffic Roesch (1999). HIDS, on the other hand, works on a specific device or host. This type of IDS detects possible changes or anomalies in the system by monitoring file integrity and transaction logs (Scarfone and Mell 2007).

IDS uses two different methods to detect attacks: Signature-Based Detection and Anomaly-Based Detection. Signature-based detection identifies attacks using known threat signatures. The system compares data packets with predetermined signatures and sends an alert when there is a match (Modi *et al.* 2013).

On the other hand, anomaly-based detection learns the normal behavior of the system and detects threats when there is a deviation from these behaviors. This method is especially effective in detecting previously unidentified types of attacks (Chandola *et al.* 2009).

When IDS detects threats, it sends reports to security teams or system administrators. However, due to the passive nature of these systems, they cannot directly intervene in threats. This shows that IDS should be supported by active defense systems such as IPS (Scarfone and Mell 2007).

Intrusion Prevention System (IPS): IPS monitors network traffic and system activities similar to IDS, but takes a more active approach. IPS not only reports threats after detecting them, but also automatically intervenes in them. This feature makes IPS an effective system in quickly stopping security threats. For example, when suspicious activity is detected on the network, IPS can stop this traffic and prevent malicious interactions (Bace *et al.* 2001).

IPS usually works at a central point where network traffic passes and analyzes this traffic to identify potential threats. The system is integrated with firewalls to examine incoming packets and block suspicious movements. Thanks to detailed analysis of traffic, IPS increases system security and prevents malicious packets from entering the network (Modi *et al.* 2013). This structure makes it possible to detect threats at an earlier stage and neutralize them. IPS can respond quickly to threats with detection methods. Signature-based detection methods are used to identify known threats, while anomaly-based methods learn the normal behavior of the system and perceive deviations as threats. In order to intervene in detected threats, IPS applies methods such as stopping malicious packets, blocking specific IP addresses, or redirecting traffic. In this way, harmful effects on the system are minimized (Sommer and Paxson 2010).

The effectiveness of IPS is more clearly seen in practical examples. For example, in a Distributed Denial of Service (DDoS) attack, IPS can analyze excessive traffic and eliminate this load and ensure uninterrupted operation of services (Mirkovic and Reiher 2004). In addition, malicious files or suspicious traffic detected in the network can be quarantined by IPS, preventing damage to the system (Amini and Qian 2017).

IDS and IPS Working Together: Most modern security systems combine IDS (Intrusion Detection System) and IPS (Intrusion Pre-

vention System) functions to provide more effective protection. While IDS detects and reports threats on the network or system, IPS intervenes immediately to prevent attacks. This combination creates a fast and proactive defense mechanism against security threats (Modi et al., 2013). Thanks to this compatible structure, IDS and IPS work together, allowing security teams to identify threats faster. Suspicious activities detected by IDS can be automatically stopped by IPS. In this way, threats are effectively prevented. This collaboration offers a great advantage in providing real-time protection, especially in institutions with complex network structures or critical infrastructures.

Machine Learning Based Anomaly Detection

Autonomous vehicles provide independent movement capability by working with advanced sensors, complex algorithms and continuous data exchange. While this technological structure provides great advantages in terms of security, it can also become vulnerable to various security threats. Machine learning-based methods stand out as an effective defense mechanism against these threats (Ayata and Seyyarer 2022). These methods undertake important functions such as detection of abnormal behavior, attack prediction and prevention of potential threats (Hodge and Austin 2004; Chandola *et al.* 2009). Table 2 provides the pros and cons of these methods.

Anomaly Detection: Autonomous vehicles use machine learning algorithms to detect anomalous behavior in their systems. For example, data from sensors are continuously analyzed to establish normal behavior patterns of the system. Anomaly detection algorithms detect deviations from this normal flow and warn of potential threats. For example, sudden speed changes or unexpected GPS data can be a sign that the system may be targeted. These algorithms increase vehicle safety by detecting potential threats at an early stage (Ahmed *et al.* 2016).

Intrusion Detection and Prevention: Machine learning plays an important role, especially in detecting and preventing cyberattacks. Unsupervised learning methods are used to detect unknown types of attacks in network traffic (Seyyarer and Ayata 2023). These algorithms learn the normal flow of network traffic and evaluate deviations from this flow as attacks. For example, during vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication, machine learning-based systems can automatically flag suspicious data packets (Chandola *et al.* 2009; Sommer and Paxson 2010).

Real-Time Threat Management: Real-time data analysis is crucial for the safety of autonomous vehicles. Deep learning models, in particular, can detect threats in real time by analyzing complex data sets. For example, recurrent neural networks (RNN) or autoencoders process data from vehicle sensors to identify potential security threats. These models can predict future threats by examining past data. This ability allows vehicles to be better prepared for environmental risks (Goodfellow 2016).

Secure Software And System Updates

Safe software updates in autonomous vehicles are a critical requirement to ensure system security. Over-the-air (OTA) updates allow regular and protected updates of software and security patches in vehicles (Macher *et al.* 2017; Medvedev and Vybornova 2018). This method provides a flexible and secure solution for the smooth operation of autonomous vehicles.

Update Process:

- Preparation of Update Package: Developer teams create software updates and add security patches. The update package is usually compressed and uploaded to the server. For security, the authenticity and identity of the package is verified using a digital signature (Nguyen *et al.* 2020).
- Secure Data Transmission: The update is securely transferred from the server to the devices. Data transfer is provided using encryption methods such as HTTPS or TLS. The device checks whether an appropriate update is available by sending software version information to the server (Hossain *et al.* 2015).
- Installing the Update on the Device: The update package is downloaded to the device's memory and stored in a temporary area. The integrity of the file is checked with digital signature verification. The device can continue to operate during the update, so there is no operational interruption. When the installation is complete, the device is restarted and the new software is put into operation (Macher *et al.* 2017).
- Rollback Mechanism: If the update fails or an error is detected, the rollback function is activated. In this way, the device can return to the previous software version and be ready for the update again (Nguyen *et al.* 2020).
- Post-Update Reporting: After successful updates, the device sends an update report to the server. This report is used to analyze statistics and investigate possible problems (Medvedev and Vybornova 2018).

Safe OTA Update Principles:

- Digital Signature: Digital signing is used to protect update packages against counterfeit software (Nguyen et al., 2020)
- Rollback Function: Allows the device to revert to the previous version if a problem occurs after the update (Medvedev and Vybornova 2018).
- Network Security: Encryption protocols such as HTTPS or TLS should be used to increase security during data transfer (Hossain *et al.* 2015).
- Verification Mechanisms: Version and device information must be verified to ensure that the update package is compatible with the device (Nguyen *et al.* 2020).

In-Vehicle Segmentation

Segmentation of the network within the vehicle is a critical method used to increase system security. Network segmentation prevents the attack from spreading to other components if one component is attacked. In particular, isolating critical systems such as braking and steering from less critical systems such as entertainment or navigation increases the overall security of the vehicle (Wolf and Serpanos 2017; Bosch *et al.* 1991) .

Network Segmentation: The network inside the vehicle is divided into separate sections for different systems and functions. Each network section is isolated from other sections, limited to a specific system. For example, critical safety systems such as brakes and steering operate independently of less important systems such as entertainment and navigation. This structure prevents security breaches in one area from spreading to other areas. Thus, a higher level of security is provided throughout the system (Groll and Rumez 2019).

Use of Different Network Protocols: The different systems in the vehicle are usually separated by various protocols such as CAN (Controller Area Network), LIN (Local Interconnect Network), FlexRay and Ethernet. Critical systems use CAN and FlexRay

Table 2 Pros and Cons of machine learning based methods

Method	Pros	Cons
Anomaly Detection	Increases security by detecting potential threats at an early stage; provides rapid data analysis.	False positive rates can be high; requires accurate and high quality dataset for training.
Intrusion Detection and Prevention	It can detect unknown attacks and offers adaptive protection with its ability to continuously learn.	Requires high processing power; may affect the normal operation of the system.
Real-Time Threat Management	It analyzes complex data sets, can predict future threats and respond quickly.	Deep learning models are costly; real-time operation may experience delays.

protocols because they require fast and reliable communication. In contrast, entertainment and information systems that require high data rates usually operate on Ethernet. Communication between these protocols is provided through special gateways or firewalls (Koscher *et al.* 2010).

Gateway Usage: Devices called "gates" are used to regulate data exchange between segments. Gates control data transfer between two different networks and block risky data packets. For example, gates that prevent direct data transmission from the entertainment system to the brake system protect sensitive systems. These devices limit unauthorized access to critical data while allowing certain data packets to pass through (Checkoway *et al.* 2011).

Firewalls and Filtering: Firewalls are activated to protect critical systems. These systems allow only authorized data packets to pass through and filter requests from external networks. Access requests, especially from internet-connected devices, are controlled by in-vehicle firewalls. Data exchange is only allowed within the framework of specified protocols, thus neutralizing attack attempts (Macher *et al.* 2017).

Access Control and Monitoring: Specific access controls are applied for each segment. For example, only certain devices can access the entertainment system, while the braking system is only open to approved electronic control units (ECUs). In addition, network traffic within the vehicle is constantly monitored. If unusual data transfers or abnormal behaviors are detected, the system issues warnings or activates automatic defense mechanisms (Wolf and Serpanos 2017).

Physical Security Measures

The physical security of autonomous vehicles is of critical importance in preventing unauthorized access and physical interventions. Secure hardware components, secure boot mechanisms, and physical tamper detection systems are the basic security solutions used to prevent threats to vehicle hardware (Wolf and Serpanos 2017).

Secure Boot: Secure Boot verifies the reliability of the device's software components, allowing only authorized software to run. This mechanism ensures that malware or unauthorized changes are disabled during system startup. Working Principle: Secure Boot creates a hardware-supported trust chain (Root of Trust). During system startup, each software component is verified with a digital signature by the previous component. For example, components such as the bootloader and the operating system kernel are only run when the verification is successful. If the digital signature cannot be verified, the system startup process is stopped, thus preventing unsafe software from running (Wolf and Serpanos 2017).

Physical Intervention Detection Systems: Physical tamper detection systems detect unauthorized access or interventions by protecting the physical security of the device. These systems detect physical tampering attempts and take appropriate security measures to ensure the protection of sensitive components.

Working Principle: These systems detect physical interventions through sensors and detectors located on the device. Components such as magnetic sensors, optical sensors, pressure sensors and light sensors are placed on the external structure of the device or on hardware components. When an unusual physical change is detected on the device, the system automatically gives an alarm, applies a process interruption or puts sensitive data into protection mode (Van Eck *et al.* 2017).

Interoperability; Secure Boot and Physical Tamper Detection: Secure Boot and tamper detection systems are used together to ensure both software and physical security of a device. Secure Boot ensures that only verified and trusted software is run, while physical tamper detection systems ensure that the device is protected from external tampering. This combination is particularly popular in security-critical areas such as autonomous vehicles, financial sector devices (e.g. ATMs), and healthcare systems. For example, in an autonomous vehicle, Secure Boot ensures that the vehicle is operating in a secure software environment, while physical tamper detection prevents unauthorized access to components on the vehicle (Van Eck *et al.* 2017).

CONCLUSION

The integration of autonomous vehicle technologies within future transportation systems is of paramount importance, given the safety, efficiency and environmental benefits they offer. However, in order to ensure the safe and smooth operation of these vehicles, it is imperative to implement robust cybersecurity measures. A comprehensive approach to cybersecurity is necessary to safeguard both in-vehicle systems and inter-vehicle communication networks. Multi-layered cybersecurity methods contribute to the creation of a sustainable infrastructure by reducing the security vulnerabilities of autonomous vehicles.Encryption techniques, intrusion detection and prevention systems (IDS/IPS), machine learning-based anomaly detection, secure software updates and in-vehicle network segmentation are among the main methods used

to increase autonomous vehicle security.These technologies not only detect threats, but also prevent potential attacks and prevent damage to the functioning of the systems. Of particular note are the innovative solutions offered by artificial intelligence and machine learning-based technologies, which demonstrate superior performance against dynamic and complex threats. As autonomous vehicles become more prevalent, there is an increasing necessity for the continuous development of security standards and their integration into vehicle designs. This study provides a framework for meeting security requirements, thereby facilitating the safe and effective introduction of these innovative technologies into society. Cybersecurity is an indispensable element for the adoption of autonomous vehicles and their potential social benefits.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Abouabdalla, K. O. and S. B. Goyal, 2022 Autonomous vehicles: Improving cyber security. International Journal of Advanced Research in Technology and Innovation **4**: 118–126.

Ahmed, M., A. Naser Mahmood, and J. Hu, 2016 A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**: 19–31.

Amini, S. and C. Qian, 2017 A survey on network security monitoring in high-speed networks. IEEE Communications Surveys & Tutorials **20**: 3271–3290.

Avaroğlu, E., 2022 Bilgi güvenliğinin temel yapi taşi: Kriptoloji. Düşünce Dünyasında Türkiz **8**: 53–65.

Ayata, F. and E. Seyyarer, 2022 *The Most Important Defense System of the Technology Age: Cyber Security. Yenilenebilir Kaynaklardan Elde Edilen Malzemeler ve Uygulamaları*. Artikel Akademi, İstanbul.

Aydogan, M., 2022 Saldırı tespit sistemleri (ids) & İzinsiz giriş Önleme sistemleri (ips). Erişim tarihi: 25 Ocak 2025.

Bace, R. G., P. Mell, *et al.*, 2001 Intrusion detection systems .

Bosch, R. *et al.*, 1991 Can specification version 2.0. Rober Bousch GmbH, Postfach **300240**: 72.

Çakal, K., İ. Kara, and M. Aydos, 2021 Cyber security of connected autonomous vehicles. Avrupa Bilim ve Teknoloji Dergisi pp. 1121–1128.

Chandola, V., A. Banerjee, and V. Kumar, 2009 Anomaly detection. ACM Comput. Surv. **41**: 1–58.

Checkoway, S., D. Mccoy, B. Kantor, D. Anderson, H. Shacham, *et al.*, 2011 Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the USENIX Security Symposium*, pp. 77–92.

Durlik, I., T. Miller, E. Kostecka, Z. Zwierzewicz, and A. Łobodzińska, 2024 *Cybersecurity in Autonomous Vehicles-Are We Ready for the Challenge?*, volume 13. Electronics.

Goodfellow, I., 2016 Deep learning.

Groll, A. and M. Rumez, 2019 Security aspects of automotive over-the-air updates. In *IEEE International Conference on Vehicular Electronics and Safety*, pp. 1–6.

Hodge, V. J. and J. Austin, 2004 A survey of outlier detection methodologies. Artificial Intelligence Review **22**: 85–126.

Hossain, M. M., M. Fotouhi, and R. Hasan, 2015 Towards an analysis of security issues, challenges, and open problems in the internet of things. IEEE World Congress on Services pp. 21–28.

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, *et al.*, 2010 Experimental security analysis of a modern automobile. In *IEEE Symposium on Security and Privacy*, pp. 447–462.

Macher, G., H. Sporer, E. Armengaud, and C. Kreiner, 2017 OTA updates in automotive systems: Why and how to ensure safety and security. Journal of Automotive Software Engineering **3**: 45–58.

Medvedev, K. and E. Vybornova, 2018 Over-the-air update protocol for internet of things. In *IEEE Conference Proceedings*.

Mirkovic, J. and P. Reiher, 2004 A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review **34**: 39–53.

Modi, C., D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, 2013 A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications **36**: 42–57.

Nguyen, T. K., T. T. Hoang, and T. Q. Ha, 2020 Securing over-the-air software updates for IoT and autonomous vehicles. International Journal of Security and Networks **15**: 1–12.

Northcutt, S. and J. Novak, 2002 *Network intrusion detection*. Sams Publishing.

Özarpa, C., İ. Avcı, and S. A. Kara, 2021 Otonom araçlar için siber güvenlik risklerinin araştırılması ve savunma metotları. Avrupa Bilim ve Teknoloji Dergisi pp. 242–255.

Roesch, M., 1999 Snort - lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX Conference on System Administration*, pp. 229–238.

Saeed, Z., M. Masood, and M. U. Khan, 2023 A review: Cybersecurity challenges and their solutions in connected and autonomous vehicles (CAVs). JAREE (Journal on Advanced Research in Electrical Engineering) **7**.

Scarfone, K. and P. Mell, 2007 *Guide to intrusion detection and prevention systems (IDPS)*. NIST Special Publication.

Schneier, B., 2007 *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.

Seyyarer, E. and F. Ayata, 2023 Siber güvenlikte makine öğrenimi dönemi .

Sommer, R. and V. Paxson, 2010 Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy*, IEEE.

Stallings, W., 2016 *Cryptography and network security: Principles and practice*. Pearson.

Van Eck, W., B. Kuijper, and L. Wagemans, 2017 Physical tamper detection in electronic devices: Technologies and application. Journal of Electronic Protection and Security **12**: 132–145.

Wolf, M. and D. Serpanos, 2017 *Embedded systems security: Foundations and applications*. Morgan Kaufmann.

Özkan, H., 2020 Simetrik ve asimetrik anahtarlı Şifreleme algoritmaları. Erişim tarihi: 25 Ocak 2025.

How to cite this article: Seyyarer, E., Ayata, F. and Özdem, S. The Role of Technological Approaches in Cyber Security of Autonomous Vehicles. *ADBA Computer Science*, 2(1), 1-6, 2025.