Journal of Computer Science and Electrical Engineering
ISSN: 2663-1938
DOI: 10.61784/jcsee3017

ENHANCING AUTONOMOUS VEHICLE SECURITY THROUGH ADVANCED ARTIFICIAL INTELLIGENCE TECHNIQUES

Rana Hassam Ahmed, Majid Hussain, Hassan Abbas, Samraiz Zahid, Muhammad Hannan Tariq*
Department of Computer Science, The University of Faisalabad, 38000 Pakistan.
Corresponding author: Muhammad Hannan Tariq, Email: a.hannan17008@gmail.com

Abstract: As the technology behind autonomous vehicles advances at breakneck speed, ensuring their safety has become a critical concern for engineers and policymakers alike. While numerous security measures have been proposed to mitigate risks associated with cyberattacks or hardware malfunction, artificial intelligence (AI) algorithms offer promising solutions to enhance anomaly detection capabilities within these systems. This research paper delves into precisely this area of interest, exploring how AI algorithms can improve anomaly detection in autonomous vehicles. Through an examination of various AI techniques--including machine learning, deep learning, and anomaly detection algorithms--this study examines their potential for bolstering the security of autonomous systems and mitigating potential risk factors. To achieve its aims effectively, the study focuses on analyzing large datasets using advanced AI models that can identify anomalies accurately and efficiently. This approach will enable timely responses to detected threats by allowing for the swift implementation of responsive measures. The development of robust frameworks for protecting autonomous vehicle networks represents one significant contribution to this research's findings. By utilizing AI techniques previously unexplored in this area, this study enables a more thorough understanding of exactly how vulnerabilities may develop within these complex systems–-and offers viable strategies for moving forward. Ultimately, producing findings capable of significantly strengthening established protocols can help those designing processes based around autonomous devices deploy them more confidently. In doing so–-by contributing insights explicitly tailored to securing connected infrastructure components like self-driving cars–-we aspire toward better outcomes through innovative technology applications while keeping people safer than ever before.
Keywords: Autonomous vehicle; Artificial intelligence; Anomaly detection; Security and privacy

1 INTRODUCTION

The Industrial Revolution, a phenomenon renowned for the diversification and improvement of technology all around the globe has powered us to an era that was once considered impossible to reach. Uniquely shaping society in diverse ways but between these adaptations, there has been no greater shift than what we are now experiencing – eliminating the need for human presence within them. With Artificial intelligence leading the way, slowly drones, intelligent robotics, and machine learning have started their takeover phase with statistics indicating that people might just be getting replaced in various spheres such as manufacturing, medicine, economics, education, and public safety [1]. As we look toward the future of autonomous driving systems, it's clear that their adoption would lead to a host of benefits. For one, they would drastically reduce human errors that can often lead to accidents or other hazards on the road. In addition to this, AVs promise more efficiency in areas like fuel utilization, which could help mitigate environmental concerns and save money for drivers. Of course, we mustn't forget about passenger welfare- with autonomous driving technologies in control of vehicles, passengers can sit back and enjoy a pleasant entertainment-rich experience. However, there are important issues to consider as well when thinking about implementing these systems. Despite all the potential advantages of using AVs on a wide scale, there remain security vulnerabilities that must be dealt with before they can truly become viable options for everyday use. Additionally- and perhaps even more pressingly- there are serious concerns surrounding privacy when it comes to autonomous driving technology. These issues will need careful thought and planning if AVs are going to achieve widespread implementation without putting people at risk [2].
The success of an autonomous driving system is, without question, owing to the importance of networking. Proper communication between AVs and both other vehicles and the Internet remains a fundamental necessity for their navigation. In addition, these AI technologies require regular firmware updates, along with involvement in traffic management systems that necessitates direct access to network connectivity [3] . The implementation of artificial intelligence algorithms promises to boost the anomaly detection capacities of autonomous vehicle security systems significantly. By leveraging advanced machine learning techniques, input data from various sensors installed in the vehicle can be analyzed more intelligently to provide a comprehensive understanding and predict any unusual activity. This modern technology ensures efficient tracking and monitoring of intrusions that can be detrimental to the safety of passengers as well as other fellow motorists on the road. Besides, AI-powered algorithms supply timely information with utmost accuracy and consistency, enabling prompt corrective actions which help guarantee reliable safety features for autonomous automobiles. Therefore, it is essential to emphasize further research into these emerging technologies such that they are optimized fully for providing secure transport solutions in an exciting era of mobile autonomy. Securing autonomous vehicles using AI requires a multidimensional approach that encompasses threat assessment, data security, intrusion detection and prevention, adversarial attack mitigation, system integrity and safety, continuous

© By the Author(s) 2024, under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0).

monitoring, and compliance with regulations. Autonomous vehicle manufacturers can enhance the security of their vehicles and ensure the safety and trust of passengers and other road users.

2 RELATED WORK

In this paper, the authors supply a broad survey of how EVs operate and expound on plausible attacks as well as counterstrategies. Additionally, they elaborate on undetermined difficulties present in the EV ecosystem and suggest feasible paths for future inquiries. By analyzing security and privacy problems in EVs from a cyber-physical systems standpoint, the authors assert that we can bolster safety measures across the entire spectrum of this evolving industry [4] . The authors of this paper have conducted a categorization of attacks into three distinct categories: assaults on autonomous control systems, intelligent driving system parts, and on vehicle-to-everything (V2X) operations[5]. The defense mechanisms introduced were also classified into three areas; security architecture, intrusion detection, and anomaly detection. As stated in the paper, forthcoming advancements in autonomous car safety are expected to utilize artificial intelligence combined with tremendous data sets to combat external cyber-attacks [6]. The rapid technological advancements in the automotive industry have enabled over 100 MB of binary code to be installed on approximately 50-70 independent computers within each vehicle. Undeniably, this progression has demonstrated significant strides in innovation. Nevertheless, with these much more complicated services and communication features integrated into the vehicles, there is a growing concern regarding a larger attack surface area for hackers to exploit. To examine these potential risks further, this study conducted active experiments against two late-model passenger cars. Specifically, the study's approach involved testing individual components under controlled settings and closed courses [7]. In this paper, the application of Artificial Intelligence (AI) in creating Autonomous Driving vehicles is explored with a specific focus on Vehicle to Everything (V2X) communication. V2X communication concerns the ability of cars to detect, communicate and act based on information from technological sensors and driving regulations. To develop autonomous driving effectively, it is imperative that three technological pillars are addressed – sensing, mapping and driving decision-making. This paper highlights the significance of AI in driving decision-making and delves into reinforcement learning and other machine learning methods which can be employed to generate effective real-world policies for driverless car programming [8] . This article concerns the obstacles confronting self-driving vehicles, specifically regarding their security measures. It offers a potential solution in the form of a cutting-edge system that utilizes deep learning methods to safeguard autonomous vehicle networks against cyber threats. This high-performance software uses pre-processing techniques to convert categorical data into numerical values and leverages both convolutional neural network (CNN) and CNN-LSTM hybrid models to identify malicious messages aimed at compromising the network's defenses. The study findings indicate that this model is highly effective, as evidenced by its accuracy scores and precision metrics [9] . This paper suggests an advanced technique for identifying potential cyber-attacks in vehicles, using deep learning methods. Specifically, this approach applies generative adversarial network (GAN) analysis to scrutinize the message frames passing from the electric control unit (ECU) and other installed hardware within the vehicle. The article underscores the significance of safeguarding automobiles from cyber threats while also highlighting some obstacles related to securing them [10]. In this paper, a novel framework for CAV cyber security that utilizes the Unified Modelling Language (UML), is presented. To support the proposal, a dataset detailing communication cyber-attacks was produced. In an effort to develop precise detection models for these types of attacks, machine learning algorithms are used to create Decision Tree and Naive Bayes classification models. Authors compare runtime alongside precision and accuracy results and conclude that the Decision Tree model is best suited for detecting CAV communication attacks. Furthermore, the authors discuss CAVs features and how they have been categorized into different levels of automation designated by the Society of Automotive Engineers (SAE) [11]. This paper takes a closer look at the security challenges posed by Connected and Autonomous Vehicles (CAVs) and assesses how cyber threats can impact their overall performance. By combining autonomous vehicle (AV) technology with that of connected vehicles (CVs), CAVs offer more dependable, efficient, and secure traffic. However, this innovation also opens up new avenues for potential vulnerabilities and hacking attacks. According to the findings of the study, fortifying CAVs' perception and operations is crucial in ensuring their safety and reliability on the road [12] . The article exposes the vulnerability of machine learning in connected autonomous vehicles (CAVs) and the potential implications of these attacks. A proposed strategy for tackling this issue is to employ adversarial examples that can create attacks on CAVs that are difficult to detect by current ML techniques for misbehavior detection. This paper additionally elaborates on how these adversarial models were created and trained using a two-phase approach. The results demonstrate the effectiveness of such techniques in identifying and preventing attacks on CAVs[16]. In conclusion, safeguarding critical infrastructure requires examining opponent tactics and retraining multiple models with real-world data from pilot CAV sites[17]. It's critical that we protect our future systems against all sorts of technological threats delivered through cyber espionage or external interference since they could pose deadly consequences if left unchecked [13]. The significance of safeguarding information systems has become increasingly important with the advent of Internet of Things (IoT) devices that have connectivity to the Internet. Specifically, in the automotive industry, GPS-based monitoring solutions can be at risk from hackers who may breach and interfere with their workings; this poses potential dangers such as exposing sensitive data as well as substantial harm[5]. This research paper covers important security issues that relate to

GPS-based monitoring in the auto industry and offers initial suggestions for counteractive measures that could help address these concerns [14,15].

3 PURPOSED MODEL

Ensuring the safety and reliability of autonomous vehicles is critical, and one way to achieve this goal is by securing them. Artificial Intelligence (AI) technology can be highly effective in enhancing security for these advanced transportation systems, doing so through identifying and mitigating potential threats that could pose risks to passengers or other drivers on the road. By integrating AI technology into their systems, manufacturers can create a systematic approach toward securing autonomous vehicles and be better prepared for any challenges that may arise. This approach will not only ensure passenger protection but also allow greater confidence in using autonomous vehicles as a reliable mode of transportation in the future, thus contributing to the improvement of the overall quality of human life as shown in fig 1.

3.1 System Architecture

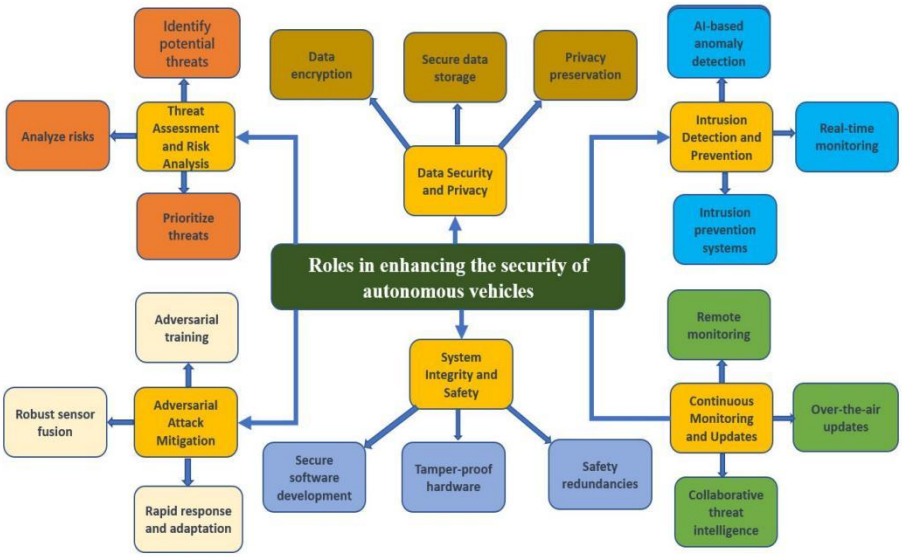

Figure 1 Proposed Architecture

3.2 Threat Assessment and Risk Analysis

Autonomous vehicles (AVs) face a range of security threats that must be carefully identified, analyzed, and prioritized to ensure the safety and integrity of the system. One of the key threats is cyber-attacks, where unauthorized access to the vehicle's software or communication systems could result in data breaches, hijacking, or operational failures. Another significant threat is sensor tampering; AVs rely heavily on sensors like LIDAR and cameras for navigation, and interference with these sensors, whether physical or digital, could lead to inaccurate data and accidents. Additionally, malicious software poses a serious risk, as malware can infiltrate the AV's operating system, causing malfunction, altering navigation, or shutting down safety-critical functions. Physical intrusions, where attackers gain direct access to the vehicle's hardware, could also disrupt operations, disable safety features, or grant control over critical systems. To mitigate these threats, it is essential to analyze the risks by assessing the potential impact and likelihood of each threat. For example, a cyber-attack could compromise passenger safety, while sensor tampering could lead to fatal accidents. Cyber-attacks and malware are more frequent in highly networked systems, making them more likely than physical intrusions, which are possible but less common in certain environments. When prioritizing threats, both severity and probability must be taken into account. Threats with a high probability and high severity, such as cyber-attacks or sensor tampering, should be top priorities due to their potential to cause severe consequences like crashes or data theft. Low-probability but high-severity threats, such as physical intrusions or rare software vulnerabilities, must also be addressed due to their potential for significant damage. High-probability but low-severity threats, such as minor software bugs or sensor misalignments, can be mitigated more easily and thus rank lower in priority. Finally, low-probability and low-severity threats may be deprioritized as their occurrence and impact are minimal. By categorizing and prioritizing threats in this way, resources can be allocated efficiently to address the most significant risks in AV systems as shown in fig 2.

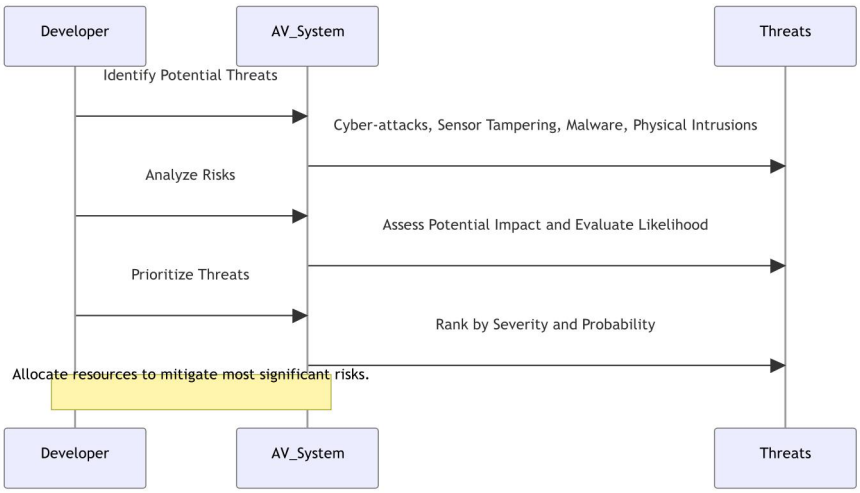

Figure 2 Risk Analysis

3.3 Data Security and Privacy

As the integration of autonomous vehicles on our roads increases, ensuring the security of data exchanged between these vehicles and external systems is crucial. One essential measure is the implementation of robust encryption mechanisms. Encrypting data prevents potential attackers from intercepting or interpreting sensitive information exchanged during a vehicle's journey. Additionally, secure data storage is a top priority due to the reliance of self-driving cars on advanced technology and software. Employing secure storage solutions, such as encryption or specialized hardware, helps safeguard critical information, including socially identifiable data collected by the vehicles. Furthermore, protecting the privacy of individuals in the autonomous vehicle ecosystem can be achieved by employing privacy-preserving techniques, such as anonymization or differential privacy, which ensure that personal data is protected while maintaining the system's functionality.

3.4 Intrusion Detection and Prevention

Deploy As autonomous vehicles become more prevalent, safeguarding them from cyber threats is vital for ensuring the safety of both passengers and the broader transportation ecosystem. A comprehensive intrusion detection and prevention system is necessary to defend against potential attacks targeting the complex software, hardware, and networks that these vehicles rely on.

3.4.1 AI-based anomaly detection

Artificial Intelligence (AI) can be pivotal in securing autonomous vehicles by detecting anomalies that may indicate potential intrusions. By deploying sophisticated AI algorithms, it is possible to analyze sensor data, network traffic, and system behavior to identify deviations from the vehicle's normal operational patterns. These anomalies might arise due to attempts to tamper with the vehicle's software, malicious cyber-attacks on communication systems, or unauthorized access to onboard systems. AI-based anomaly detection systems continuously learn from the vehicle's operations, improving over time to distinguish between benign irregularities and genuine threats. This dynamic approach ensures that even emerging, previously unknown attack vectors can be identified before causing significant damage.

3.4.2 Real-Time monitoring

To enhance the security framework of autonomous vehicles, real-time monitoring is essential. This involves continuously overseeing the vehicle's internal systems, including its sensors, actuators, and decision-making algorithms, as well as its external connections, such as communication with other vehicles, traffic infrastructure, or remote servers. Real-time monitoring enables immediate detection of suspicious activities, such as unauthorized access, unusual sensor readings, or unexpected changes in the vehicle's behavior. Any deviation from expected patterns of operation can be flagged for further investigation, ensuring potential threats are detected and responded to instantly. This proactive approach reduces the likelihood of attacks going unnoticed and increases the response time to neutralize potential risks.

3.4.3 Intrusion Prevention Systems (IPS)

Beyond detection, it is equally critical to actively prevent intrusions. AI-driven Intrusion Prevention Systems (IPS) can be integrated into the vehicle's security architecture to automatically block and mitigate identified threats. These systems use machine learning algorithms to not only identify suspicious activity but also take preemptive measures to prevent attacks from escalating. For example, if the IPS detects unusual network traffic or an attempt to breach a vehicle's control system, it can immediately isolate the compromised system, block unauthorized access, or reroute critical operations to maintain vehicle safety. Furthermore, AI-enabled IPS can continually evolve by learning from new attack patterns and vulnerabilities, thus maintaining robust defense mechanisms even in the face of rapidly evolving cyber threats.

3.5 Adversarial Attack Mitigation and Safety

To ensure the security and resilience of autonomous vehicles, multiple layers of protection must be in place. Adversarial attacks, such as sensor spoofing or the use of adversarial examples, pose a significant risk to AI-powered vehicles. Mitigating these threats begins with **adversarial training**, where AI models are trained on diverse datasets that include a variety of attack scenarios to enhance their robustness. Additionally, **robust sensor fusion** algorithms are essential for reliable perception, combining data from multiple sensors to minimize the impact of any one compromised sensor. Equally important is the development of **AI systems** that can adapt and respond rapidly to emerging threats in real-time, ensuring continuous protection. Maintaining **system integrity and safety** is another critical aspect, achieved through **secure software development** practices like rigorous testing and safe coding, alongside **tamper-proof hardware** that utilizes features such as secure boot and encrypted communication channels. In case of a breach, **safety redundancies** such as fail-safes and backup systems ensure the protection of passengers. Furthermore, **continuous monitoring** of security status, facilitated by **remote monitoring** systems, is vital to detect vulnerabilities early. These systems can be updated through **over-the-air (OTA) updates**, which allow patches and security enhancements without physical intervention. Lastly, **collaborative threat intelligence** enables the sharing of information about new threats across the autonomous vehicle ecosystem, allowing for a collective response to emerging cyber risks. These combined measures form a robust framework to safeguard the integrity and safety of autonomous vehicles as show in fig 3.

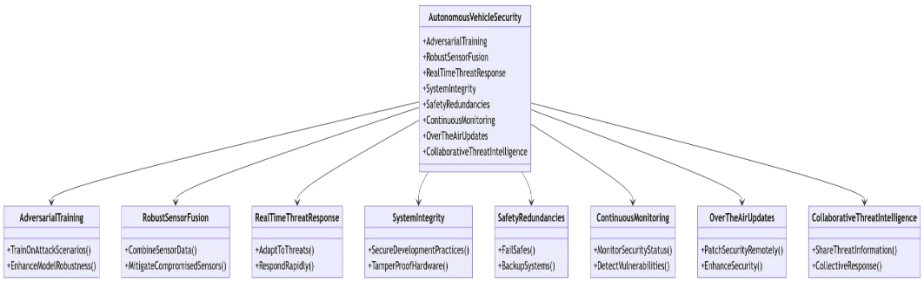

Figure 3 Attack Mitigation and Safety

4 CONCLUSION

In summary, this research paper highlights the immense potential of utilizing AI algorithms to improve anomaly detection and enhance autonomous vehicle security. Through leveraging machine learning and innovative anomaly detection strategies, AI can efficiently analyze large amounts of data and accurately identify anomalies, which can lead to timely responses when dealing with potential threats. the proposed multidimensional approach integrates threat assessment, data encryption, intrusion detection as well as system integrity reinforcement in order to guarantee passenger safety and trust while taking other road users into consideration. The extensive analysis presented here advances robust frameworks for securing autonomous vehicle networks by providing further insights into vulnerabilities observed and mitigation strategies with regard to risk management.

COMPETING INTERESTS

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

REFERENCES

[1] M, Hataba, A, Sherif, M, Mahmoud, et al. Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey. IEEE Open Journal of the Communications Society, 2022, 3, 811-829. DOI: 10.1109/OJCOMS.2022.3169500.

[2] R, Hussain, H, Oh. On secure and privacy-aware sybil attack detection in vehicular communications. Wirel Pers Commun, 2014, 77(4): 2649-2673. DOI: 10.1007/s11277-014-1659-5.

[3] S, Ucar, S C, Ergen, O, Ozkasap. IEEE 802.11p and visible light hybrid communication based secure autonomous platoon. IEEE Trans Veh Technol, 2018, 67(9): 8667-8681. DOI: 10.1109/TVT.2018.2840846.

[4] A, Brighente, M, Conti, D, Donadel, et al. Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs. 2023. DOI: https://doi.org/10.48550/arXiv.2301.04587. Available: http://arxiv.org/abs/2301.04587

[5] S, Jabbar, A H, Akbar, S, Zafar, et al. VISTA: achieving cumulative VIsion through energy efficient Silhouette recognition of mobile Targets through collAboration of visual sensor nodes. EURASIP Journal on Image and Video Processing, 2014, 32. DOI: https://doi.org/10.1186/1687-5281-2014-32.

[6] K, Kim, J S, Kim, S, Jeong, et al. Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers and Security, 2021, 103. DOI: 10.1016/j.cose.2020.102150.

[7] K, Koscher, A, Czeskis, F, Roesner, et al. Experimental security analysis of a modern automobile. 2010 IEEE Symposium on Security and Privacy, , Oakland, CA, USA. 2010, 447-462. DOI: 10.1109/SP.2010.34.
[8] N, Mazher, G, Krishna Sriram, B, Namatherdhala, et al. USES OF ARTIFICIAL INTELLIGENCE IN AUTONOMOUS DRIVING AND V2X COMMUNICATION. 1932. Available: www.irjmets.com
[9] T H H, Aldhyani, H, Alkahtani. Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. Sensors, 2022, 22(1): 360. DOI: 10.3390/s22010360.
[10] A, Kavousi-Fard, M, Dabbaghjamanesh, T, Jin, et al. An Evolutionary Deep Learning-Based Anomaly Detection Model for Securing Vehicles. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(7): 4478-4486. DOI: 10.1109/TITS.2020.3015143.
[11] Q, He, X, Meng, R, Qu, et al. Machine learning-based detection for cyber security attacks on connected and autonomous vehicles. Mathematics, 2020, 8(8): 1311. DOI: 10.3390/MATH8081311.
[12] Z, Wang, H, Wei, J, Wang, et al. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. Sustainability (Switzerland), 2022, 14(19): 12409. DOI: 10.3390/su141912409.
[13] Institute of Electrical and Electronics Engineers, 2019 IEEE International Symposium on Technologies for Homeland Security : Crowne Plaza Boston - Worcester. 2019, Woburn, MA USA.
[14] G R, Andreica, L, Bozga, D, Zinca, et al. Denial of Service and Man-in-the-Middle Attacks against IoT Devices in a GPS-Based Monitoring Software for Intelligent Transportation Systems. 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2020, 1-4. DOI: 10.1109/RoEduNet51892.2020.9324865.
[15] S, Ubaid, M F, Shafeeq, M, Hussain, et al. SCOUT: a sink camouflage and concealed data delivery paradigm for circumvention of sink-targeted cyber threats in wireless sensor networks. Journal of Supercomputing, 2018, 74(10): 5022-5040. DOI: 10.1007/s11227-018-2346-1.
[16] M. Ahmad, M, Hussain, B, Abbas, et al. End-To-End Loss Based TCP Congestion Control Mechanism as a Secured Communication Technology for Smart Healthcare Enterprises. IEEE Access, 2018, 6, 11641-11656. DOI: 10.1109/ACCESS.2018.2802841.
[17] R M A, Latif, M, Farhan, O, Rizwan, et al. Retail level Blockchain transformation for product supply chain using truffle development platform. Cluster Comput, 2021, 24(1): 1-6. DOI: 10.1007/s10586-020-03165-4.