International Journal of New Media Studies (IJNMS), ISSN: 2394-4331
Volume 6 Issue 2, July-December, 2019, Impact Factor: 6.466

A Survey on AI enabled security of Internet of Vehicles

Surendra Singh Chauhan

TIMIET, India

ABSTRACT

This paper offers a robust survey on the integration of Artificial Intelligence (AI) to enhance the security of Internet of Vehicles (IoV). Significant emphasis has been placed on identifying current security threats and vulnerabilities, prevalent in the IoV landscape, and how AI can be employed to mitigate these risks. The paper documents various concepts of AI, such as machine learning, deep learning, and neural networks, alongside their possible integration into IoV security. Safety, privacy, and data protection are the primary focal points; exploring how AI can promote efficient incident detection, prevention, and response. We also study AI's potential to analyze and comprehend intricate patterns, behaviours, and anomalies that could impact the safety, security, and overall functionality of IoV systems. Furthermore, this survey highlights the inevitable challenges and future research projections in AI-enabled IoV security, aiming to provide a comprehensive reference for stakeholders and researchers. The paper concludes with an anticipation of an improved IoV security landscape built on the pillars of AI technologies.

Keywords: AI, IoV, Safety, Privacy, Data Protection.

INTRODUCTION

The Internet of Vehicles (IoV) is a paradigm of Internet of Things (IoT) which integrates vehicular networks and internet connectivity to enhance on-road safety, traffic efficiency, and the overall driving experience [1]. Owing to its connectivity-oriented nature, IoV is pivotal in promoting Vehicle-to-Everything (V2X) communication, enabling the exchange of crucial data between interconnected vehicular nodes. However, the extensive connectivity of IoV also introduces complex security vulnerabilities and threats which need to be addressed meticulously [2,3].

Recently, there has been a surge in cyber-attacks targeting IoV systems, where attackers seek to breach security measures to manipulate vehicle controls, steal sensitive data, or disrupt V2X communication [4]. The consequences of such attacks can be catastrophic, leading to safety hazards, financial losses, and breach of privacy. Existing threat detection and prevention mechanisms often fail to cope with advanced and evolving threats due to their lack of scalability, adaptability, and real-time response [5].

Therefore, the focus has shifted towards leveraging the capabilities of Artificial Intelligence (AI) to enhance IoV security. AI, with its many subsets – Machine Learning (ML), Deep Learning (DL), and Neural Networks, offers high potential in understanding complex patterns, predicting behaviours, and adapting to evolving threats, thus making it well-equipped to deter advanced cyber attacks. AI can be incorporated into the IoV architecture in a manner that it continuously monitors, learns, and reacts to the environment to prevent potential threats effectively [6,7].

The purpose of this survey paper is to provide a comprehensive exploration of the current state of AI-enabled security in the IoV landscape. We aim to identify prevalent security threats and vulnerabilities, examine the potential of AI technologies in mitigating these challenges, and highlight the possible limitations and areas for future research in this domain [8]. By developing a deeper understanding of AI-enhanced IoV security capabilities, researchers and stakeholders can collaborate to build a safer, more secure, and privacy-preserving IoV landscape. This safer environment will result in a more reliable interaction platform for vehicles, leading to an improved driving experience and the optimization of V2X communication [9,10].

Integration of Machine Learning, Deep Learning, and Neural Networks into IoV Security.

The integration of Machine Learning (ML), Deep Learning (DL), and Neural Networks (NN) into Internet of Vehicles (IoV) security can create a robust framework that effectively detects and mitigates potential threats. This amalgamation unlocks new methods of securing vehicle-related data transfer and communication in real-time [11].

Here's a high-level overview of how they can be integrated:

Machine Learning (ML): In IoV, vast amounts of data are generated via various sensors embedded in vehicles. ML algorithms can be trained to recognize patterns within this data to predict potential security threats. For instance, ML can detect anomalies in driving patterns or system communications that may signify a security breach [12].

Deep Learning (DL): Deep Learning, a subset of ML, is particularly powerful for processing high-dimensional data, such as images and time-series data, which are common in the IoV sphere. DL can be leveraged in IoV security for complex tasks such as image recognition (e.g., identifying unauthorized drivers via inbuilt cameras) or speech recognition (e.g., voice-command-based breaches) [13].

Neural Networks (NN): Artificial Neural Networks are used to recognize patterns through a process that mimics the human brain in a simplified way. NNs can be used to create a deeper understanding of regular vehicle behaviour by leveraging multiple factors such as speed, location, time, and other telemetry data. If unusual behavior is detected, it could signify a potential security risk and trigger preventative measures [14,15].

Moreover, the three technologies can be combined to use multiple layers of defense, creating an even more reliable and safe IoV environment. For example, in a cybersecurity context, ML algorithms can be employed to filter out potential threats, DL techniques can further analyze these risks by assessing their potential impacts, and NNs can then predict the possible changes in IoV operations if these threats become a reality [16,17].

To effectively integrate ML, DL, and NN into IoV security, continuous training and updating of these technologies with the latest data and recognized threats is necessary. This will help keep the safety measures effective against new potential hazards that might arise [18].

The use of these technologies also brings up considerations pertaining to privacy and the ethical use of data. Ensuring these technologies respect user privacy rights, proper anonymization techniques, and compliance with regulations such as GDPR are vital for their beneficial deployment in IoV security [19].

How AI can Promote Efficient Incident Detection, Prevention, and Response for the Security of IoVs.

There are multiple ways that Artificial Intelligence (AI) can boost the security of Internet of Vehicles (IoVs) by aiding in efficient incident detection, prevention, and response.

Incident Detection: AI can greatly enhance incident detection in IoVs by using machine learning algorithms to identify patterns in vast amounts of vehicle data. This incorporates anomalies, behavioral patterns, and potential security threats. For example, if a vehicle deviates from its normal driving characteristics in a way that suggests possible tampering or hacking, an AI-based system can promptly identify it as a security incident [20].

Prevention: AI can support IoVs in preventing security threats by implementing predictive analysis. By using past data and learning from it, AI can predict potential threats or faults before they occur, enabling security systems to implement preventive steps. For instance, machine learning algorithms could detect unusual changes in communication patterns between vehicles and the network which might indicate the early stages of a cyber-attack.

Incident Response: AI can make responses to security incidents more efficient and effective by automating response procedures and decision-making processes. For instance, in case of a possible cyber attack, the AI can rapidly choose a course of action such as isolating the affected vehicles or communications to minimize potential damage.

Constant Learning: AI is not static, it constantly evolves. This property is highly beneficial in the security context. Patterns of threats evolve over time and machine learning algorithms can adapt to new threats by learning from new incidents, bolstering the protection system's resilience.

Real-time Monitoring: AI allows continual real-time monitoring and analysis of vehicle data, which is critical for IoVs. This is advantageous for quick threat detection and response, preventing potential incidents before they culminate into serious issues [21-24].

Enhanced Authentication: AI and ML can facilitate multi-factor authentication or even behavioural biometrics to verify the users, reducing the risk of unauthorized access.

While the integration of AI in IoVs greatly enhances security, it also increases complexity. Therefore, it is essential to proceed with a thorough understanding of the potential security implications, including those that may arise from the AI systems themselves [25].

AI's Potential to Analyze and Comprehend intricate Patterns, Behaviours, and Anomalies that could Impact the Safety, Security, and Overall Functionality of IoV Systems.

Artificial Intelligence (AI) indeed has significant potential to analyze, comprehend, and predict intricate patterns, behaviors, and anomalies that might affect the safety, security, and overall functionality of Internet of Vehicles (IoV) systems.

Detecting Patterns and Anomalies: Machine learning algorithms can analyze vast amounts of data generated by IoV systems. These algorithms can learn from data patterns and understand the norms of operation. Any deviation detected from this learned pattern would be flagged as an anomaly, thus providing proactive alerting about potential issues. For instance, AI could identify an unusual traffic pattern that could lead to a traffic jam or accident and

reroute other vehicles accordingly to avoid or mitigate the potential incident [26].

Predictive Maintenance: By analyzing data such as engine performance, battery life, part wear-and-tear, AI can predict when a vehicle is likely to require maintenance, minimizing unexpected breaks and further ensuring the safety of the network.

Cybersecurity: AI algorithms can play a crucial role in identifying and mitigating potential cybersecurity threats. By learning network traffic patterns, AI can identify suspicious behavior, like DDoS attacks, data breaches, or unauthorized access attempts, to secure IoV systems.

Traffic Management: AI can interpret real-time data from IoV systems to manage traffic more efficiently. Predictive models can anticipate traffic flow, optimize routes, and even coordinate traffic signals to reduce congestion and enhance safety.

Autonomous Vehicles: AI is essential for the function and safety of autonomous vehicles in the IoV system. Through sensors, connectivity, and machine learning, vehicles are able to navigate, understand their environment, and make complex decisions [27-29].

Environment Impact: AI can also help minimize the environmental impact of transportation, by making traffic flow more efficient and reducing idling and congestion, and optimizing fuel consumption.

It's worth noting, however, that while AI offers immense benefits, certain challenges and ethical implications need to be considered, particularly around data privacy, AI bias, and accountability in AI decision-making. As these technologies continue to evolve, it will be important to create comprehensive regulatory and ethical frameworks to guide their use [30].

The inevitable Challenges and Future Research Projections in AI-enabled IoV Security, aiming to provide a Comprehensive Reference for Stakeholders and Researchers.

AI-enabled Internet of Vehicles (IoV) security has advanced significantly in recent years, transforming the automobile industry and enhancing vehicular communication. However, this enhancement has brought about various challenges that require meaningful dialogue among stakeholders and researchers [31]. Here are some of the challenges and possible future research directions to keep in mind:

Challenges:

Privacy and Data Security: Protecting personal and sensitive data is essential in the IoV. While AI enhances data generation, management and utilization, securing this data from breaches poses significant challenges that must be addressed.

Infrastructure Setup: Implementation of AI in IoV requires strong infrastructure support, such as robust cyber-physical systems, advanced AI models and high-speed telecommunication networks. However, building this setup requires huge capital investment and time [32-34].

Standard and Policy Establishment: There are currently no universal standards or policies for AI-enabled IoV security. This makes the implementation and operation of AI in the IoV difficult and uneven across different regions and countries.

Scalability Issues: The increasing number of connected vehicles will exacerbate the scalability issues, making it challenging for the existing platforms and algorithms to efficiently manage the influx of data.

Future Research Projections:

Advanced AI Modelling: Research into developing advanced and secure AI models for IoV is needed. This could include models for data encryption, risk-based authentication, and intrusion detection to enhance the security of IoV systems [35].

Blockchain Integration: Investigators can explore the application of Blockchain technology. Blockchain has been recognized as a promising solution to drive IoV security due to its transparency, integrity, and resistance to data alterations.

Cross-Domain Collaboration: Encouraging collaboration between AI experts, IoV professionals, standardization bodies, and policy-makers would help standardize regulations and policies, in addition to resolving inconsistencies in the application and operation of AI across the IoV [36-38].

Privacy-Preserving Techniques: With the explosion of data in the AI-enabled IoV, preserving privacy will be critical. Research into privacy-preserving algorithms such as differential privacy, homomorphic encryption, and federated learning could help address these concerns.

Human-AI Interactions: AI applications in IoV need to consider the human aspect. Future research could focus on user experience, trust and acceptance, and ethical implications of AI-powered IoV [39].

Overall, the future of AI-enabled IoV security requires a multidisciplinary approach to address the pressing challenges and explore robust, reliable, and ethical solutions. Stakeholders and researchers need to work collaboratively to overcome these hurdles and ensure the safe and efficient implementation of AI in IoV [40-41].

CONCLUSION

In conclusion, the implementation of AI in IoV security showcases great potential and transformative capabilities for vehicular communication and the broader automobile industry. As we have surveyed, despite the array of benefits the combination of AI and IoV promises, it also raises critical challenges. These include privacy and data security concerns, infrastructure setup hurdles, the need for standards and policy establishment, and scalability difficulties with the growing number of connected vehicles.

Future directions and research should focus on overcoming these challenges. Advanced AI modelling, Blockchain integration, cross-domain collaboration, privacy-preserving techniques, and a deep focus on human-AI interactions represent promising paths of exploration. However, the resolution of these issues will require a concerted multidisciplinary approach and active engagement from AI experts, IoV professionals, regulators, policy-makers, and users.The goal must be to strike a balance between leveraging the capabilities of AI to maximize IoV security while mitigating associated risks and problems. As we continue to innovate and push boundaries, our journey will undoubtedly generate novel insights and strategies to ensure the secure, reliable, and ethical use of AI in the IoV landscape. This ongoing exploration represents an exciting frontier for both technology and policy, promising substantial benefits to society through increased safety, efficiency, and novelty in transportation.

REFERENCES

[1]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.

[2]. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and El-Horbaty, E. (2014) 'A comprehensive survey on vehicular Ad Hoc network', Journal of Network and Computer Applications, 37, pp.380–392.

[3]. Sarkar, S., Misra, S. and Haldar, R. (2015) 'Towards a secure service provisioning framework in a vehicular network', Computer Networks, 91, pp.311-331.

[4]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. IUP Journal of Computer Sciences, 4(3).

[5]. Khan, R., Khan, S.U., Zaheer, R., and Khan, S. (2012) 'Future internet: the Internet of Things architecture, possible applications and key challenges', Future Generation Computer Systems, 89, pp.2-11.

[6]. Jin, J., Gubbi, J., Marusic, S. and Palaniswami, M. (2014) 'An Information Framework for Creating a Smart City Through Internet of Things', IEEE Internet of Things Journal, 1(2), pp.112-121.

[7]. Herbaut, A., Negru, D., Almeida, B., Barhamgi, M. and Bandara, A. (2017) 'A model for collaborative blockchain-based video delivery relying on advanced network services chains', Computer Networks, 109, pp.92-106.

[8]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In 2009 Second International Conference on Emerging Trends in Engineering & Technology (pp. 1143-1150). IEEE.

[9]. Luan, T.H., Gao, L., Li, Z., Xiong, N., and Sun, L. (2015) 'Fog Computing: Focusing on Mobile Users at the Edge', IBM Journal of Research and Development, 41(4), pp.615-629.

[10]. Cui, Y., Zhang, Z., Liu, N., and Jin, S. (2012) 'Network Coding in Relay-based Device-to-Device Communication Underlaying Cellular Networks', IEEE Wireless Communications and Networking Conference, pp.6-10.

[11]. Li, Y., Qian, H., Suo, H., and Zhu, L. (2013) 'Secure D2D Communication in Large-Scale cognitive Cellular Networks: A Wireless Netowrking Perspective', IEEE Wireless Communications Magazine, 20(2), pp.62-67.

[12]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. International Journal of Computer Applications, 61(19).

[13]. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and El-Horbaty, E. (2014) 'A comprehensive survey on vehicular Ad Hoc network', Journal of Network and Computer Applications, 37, pp.380–392.

[14]. Sarkar, S., Misra, S. and Haldar, R. (2015) 'Towards a secure service provisioning framework in a vehicular network', Computer Networks, 91, pp.311-331.

[15]. Liu, J., Wan, J., Wang, Q., Deng, P., Zhou, K. and Qiao, Y. (2016) 'A survey on position-based routing for vehicular networks', Telecommunication Systems, 62(1), pp.15–30.

[16]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. J. Comput. Eng. Intel. Syst, 3(7), pp.32-41.

[17]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. International Journal Of Engineering Development And Research.

[18]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. International Journal of Computer Applications, 119(2).

[19]. Mahmud, M.S., Rahman, M.A. and Shamim Hossain, M. (2018) 'Cognitive and AI-Enabled Wireless Sensor Networks for Internet of Vehicles', IEEE Wireless Communications, 25(5), pp.48-55.

[20]. Lu, R., Lin, X., Zhu, H. and Ho, P.H. (2017) 'An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications', IEEE Transactions On Vehicular Technology, 59(6), pp.2772-2785.

[21]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. International Journal of Computer Applications, 116(19).

[22]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. International Journal on Computer Science and Engineering, 2(3).

[23]. Amini, S., Gerla, M. and Kleinrock, L. (2014) 'Toward an internet of vehicles: A backpressure algorithm for smart intersections', IEEE Vehicular Technology Conference, pp.1-5.

[24]. Cho, J.H., Waluyo, I.B. and Pardede, E. (2018) 'A Hybrid Model for Predicting the Internet of Things (IoT) Traffic in Smart Cities Using AI-Based Approach', IEEE Access, 6, pp.4045-4056.

[25]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. Recent Developments in Computing and Its Applications, p.155.

[26]. Liu, J., Wan, J., Zeng, B., Wang, Q., Song, H., and Qasim, K. (2016) 'A Scalable and Quick-Response Software Defined Vehicular Network Assisted by Mobile Edge Computing', IEEE Communications Magazine, 55(7), pp.94-100.

[27]. Vinel, A. (2012) '3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications?', IEEE Wireless Communications Letters, 1(2), pp.125-128.

[28]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11). International Journal of Computer Science & Communication, 1(1), pp.25-28.

[29]. Bhatnagar, D. and Rathore, R.S.,2015. CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES. International Journal of Advance Research in Science And Engineering, 4(01), pp.683-690.

[30]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. International Advanced Research Journal in Science, Engineering and Technology, 3(4), pp.83-86.

[31]. Gerla, M., Lee, E.K., Pau, G. and Lee, U. (2014) 'Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds', IEEE World Forum on Internet of Things, pp.241-246.

[32]. Atiquzzaman, M. and Hasan, S. (2015) 'Internet of Things (IoT) Applications to Telemedicine', IEEE Internet Initiative, 1, pp.1-6.

[33]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. International Journal of Computer Applications, 138(8).

[34]. Mallick, A. S. B. and Rathore, R. K. Survey on Database Design for SaaS Cloud Application. International Journal of Computer Engineering and Technology, 6(6), 2015, pp. 64-71.

[35]. Ketki, S.K. and Rathore, M.R.S., 2015. A Novel Study for Summary/Attribute Based Bug Tracking Classification Using Latent Semantic Indexing and SVD in Data Mining. International Journal of Advanced Technology in Engineering and Science, 3(1), pp.214-220.

[36]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. International Journal on Computer Science and Engineering, 2(5), pp.1439-1444.

[37]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. IJCST, 6, pp.93-95.

[38]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. International Journal of Computer Applications, 1(13), pp.26-31.

[39]. Kumar, V. and Rathore, R.S., 2018, October. Security issues with virtualization in cloud computing. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 487-491). IEEE.

[40]. Azees, M., Vijayakumar, P. and Debojyoti, D. (2016) 'Comprehensive survey on security services in vehicular ad-hoc networks', IET Intelligent Transport Systems, 10(6), pp.379-388.

[41]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. International Research Journal of Engineering and Technology (IRJET), 4(5), pp.153-155.