Enhancing Cybersecurity in V2X Communication: A Blockchain and Machine Learning-Based Framework

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—Smart mobility in smart cities has been claimed over the last couple of years by integrating V2X communication systems to resolve interfacing of vehicles and 'the rest' as identified in. As with all such thrusts, these advancements bear cybersecurity perils – to wit, jammers, spoofers, Distributed Denial of Service (DDoS), and eavesdroppers. These threats have implications for the reliability and integrity of the data used and bring about essential challenges to improving V2X systems.**

This paper also proposes a more detailed cybersecurity framework, including blockchain and machine learning, for handling the challenges of V2X communication systems. Sophisticated methodology to its security and reliability of data dissemination, blockchain is advantageous as it only allows nodes to undertake transactions in the network system. Consequently, real-time restrictive ML methods allow for the determination of other variants of threats for an attack, namely jamming/skimming. Another recent addition that brings richness to the framework is an adaptive intrusion detection system responding to emergent significant threats in cyberspace with similar vigour.

The pragmatic conceptual methodology includes blockchain for a secure sharing of protected data, the use of machine learning algorithms for risk assessment, and the established general vulnerability through the use of scenarios [?]. Among the indicators that we employed above and that are relevant to measuring the effectiveness of the proposed framework are detection accuracy, response time, and its effect on the systems' performance.

The outputs that should be expected in this context include a world, effective and timely V2X systems security solution that, in the long run, enhances the safety of intelligent vehicles. This work benefits smart city cybersecurity by proposing a novel, secure V2X approach. The specific solution of the proposed framework will be implemented in the scope of the 5G network in connection with the big data streaming for scalability here. Therefore, this work will provide valuable answers to safety issues that would otherwise set the boundaries for using V2X systems in smart cities.

***Index Terms*—V2X Communication, Cybersecurity, Blockchain Technology, Machine Learning, Smart Cities**

I. Introduction

Solutions of the intelligent city today open up new possibilities for improving the quality of life of people in the towns by introducing intelligent methods for regulating transport, energy and security systems. The enablers of this change are known as Vehicle to Everything (V2X) solutions, which are new concepts toward realizing real-time information sharing between a vehicle and its environment [1] [2]. V2X communication types consist of V2V: Abbreviations used are V2V: Vehicle to Vehicle, V2I: Vehicle to Infrastructure, V2P: Vehicle to Pedestrian and V2N: Vehicle to Network. This created a mutually supporting arrangement for promoting collaborative work in motions like driving, traffic signal systems, and safety that generated smarter, safer, and more effective roads.

Nevertheless, the introduction and use of V2X communication need to be improved based primarily on security weaknesses. Present cars and transportation networks make the level of intellect higher and, thereby, are as susceptible to cyber risks. A jamming attack brings down the control link, a spoofing attack brings down the identity and data, and a Distributed Denial of Service attack brings down the network resources. Another way through which eavesdropping assists in placing user privacy in even greater danger is through the interception of sensitive information. They affect issues related to the various V2X systems, incorporating the advantages of this revolutionizing technology, such as efficiency, reliability, and security impact.

Since the V2X application is relatively new, and given that patterns of technology and threats are so fluid, it is due to the critical role played by V2X communication in enhancing the safety of road users and the efficient functioning of intelligent city precincts that more and more attention should be paid to cybersecurity in V2X communication. As mentioned in this research study, the cyber-attacks that target the V2X environment have disastrous effects, such as traffic jams, mishaps, and system integration distrust following one hack attack [17]. A typical part of the traditional security solutions, such as encryption and authentication, is relatively secure but cannot effectively satisfy [26] the need for V2X systems. These systems require positive, time-variant thinking, learning with load conditions, and managing known and potentially latent risks.

To eliminate these challenges, this paper develops a new cy-

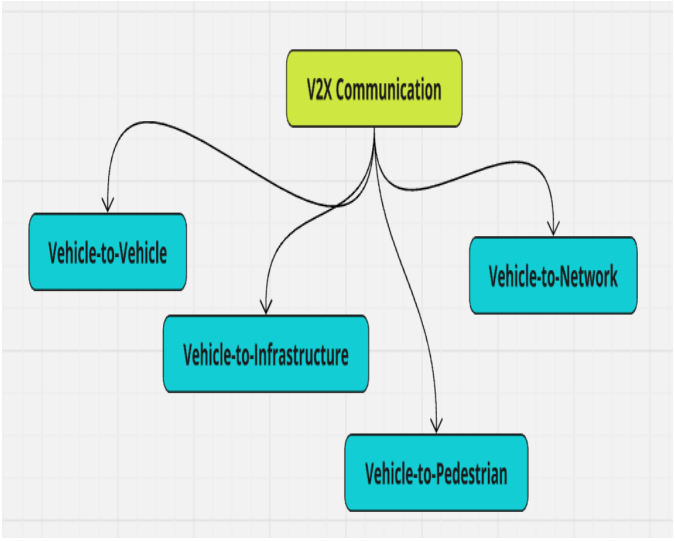

Fig. 1. This diagram illustrates the four key components of V2X communication: Introducing Vehicle-to-Vehicle , Vehicle-to-Infrastructure, Vehicle-to-Pedestrian, and Vehicle-to-Network. These communication types are the building block of connected vehicular networks in smart cities

bersecurity model integrating blockchain and artificial neural networks. As demonstrated in section II while discussing V2X, since it boasts of parading data exchange between players, its security is at the precipice of being compromised for data sharing purposes; for non-changeable and decentralized characteristics, blockchain technology can be harnessed as seen in section II. As such, by expanding the probability only allowed nodes connecting to a network, the reliability of the information shared is increased by blockchain. Furthermore, machine learning algorithms have introduced several new inputs to the frameworks, namely, the pointing process as put, its adaptivity and intelligence, and the ability to identify the emerging threats and their obviation during actual operation. These algorithms take change and fluctuation as the ways of detecting the presence of an attack in the form of, for instance, a jamming or spoofing attack while maintaining an acceptable level of sensitivity.

The proposed framework also has attributes allowing it to self-develop and accommodate emerging threats as an intrusion detection system. This differs entirely from other intrusion detection systems that rely on rules and analysis approaches. It can switch a strategy when some of the new types of attacks occur and ensure dependable operations to prevent ever-advancing threats. In integration, both blockchains have the best solution that will provide the security of the V2X communication.

The following works with this research are helpful since they may assist in deriving how progressively enhancing V2X systems are connected with the present cybersecurity issues. As anticipated, it has been expected that the proposed framework will work in a real-time scan, label and efficiently to cater to the present high-intensity vehicular networks by integrating with blockchain and machine learning methods. This makes the response of V2X communication safer and dependably secure; it comes under the umbrella of developing safe and sustainable smart cities.

The methodology for this study involves three key components: The channels of blockchain adoption, the formation and training of the machine learning model stages, and the machine learning model performance prognosis through the simulation and test. Security necessities on the data stream and the credibility of nodes will be supported by applying blockchain for enhancing V2X communication to V2X – 2 [1]. This will also create the real-time formulation of a soundly developed machine learning model that can point out the cyber threats and their risk levels. The framework will then be subjected to limited mimicry of the various attack types, including jamming and spoofing. In an attempt to evaluate the efficiency of the proposed framework, the system's capability to detect intrusions, time elapses, and overall performance under different categories of attack will be used for comparison.

The expected repercussions of this study are that such a firm cybersecurity model will improve V2X interaction safety and dependability when responding to these challenges. Always anticipating such swaps as jams, spoofing, and DDoS, the framework attempts to proactively establish secure operating space for safe AV and CV interactions [13]. The present study also adds more enhancements to the current and future development of cybersecurity in intelligent cities, as the outcomes and remedies for each academic area explored in this paper are to be utilized in future papers on this topic.

In addition to representing some aspects that should embrace the future of V2X communication, the above framework has implications which can be extended to other areas within intelligent city solutions [12]. Thus, with the help of machine learning, it is also possible to expand the use of blockchain further to other fields, including energy management, public security, and healthcare, where the issue of data exchange security is critical. Intelligent cities of the third generation are still being designed and built, so there can be no question of strengthening cybersecurity.

The research interest of this proposed framework for further study is extending and implementing a 5G network with cloud-based big data analytics. Thanks to the low latency and high data rate, future fifth-generation systems shall ensure improved real-time interaction in V2X communication [11]. On the other hand, cloud computing can spread the news regarding improved diagnosis of traffic flow and cyber threats. With these technologies in the framework, practical use is possible in meeting the novel higher-order systemic requirements essential to innovative city systems.

II. Related Work

With the rising application of V2X, there has been an upsurge in the search for V2X security to protect this network from cyber-attacks. Present-day solutions for protecting V2X systems must primarily depend on conventional measures against threats or risks bearing very much resemblance to

the following: While these methods provide some degree of security, a higher level is required, especially for realization in real-time for large-scale vehicle communication networks [1] [10]. These conventional approaches do not maintain low latency and high reliability, for example, when transmitting other critical data such as collision and traffic signals.

Blockchain and artificial intelligence (AI) may answer these limitations. In light of this, this paper recommends applying blockchain as an efficient decentralized solution for V2X communication with secure data integrity, readability, and non-tampering aspects detailed in resource [4]. For that reason, based on the ability of blockchain to maintain the record of credible and solved transactions, it may be utilized in the trust management of the V2X network. However, blockchain integration into V2X systems is full of challenges, which may include computational burden issues or scalability issues for real-time.

The units of V2X systems have also utilized the ML algorithms for threat recognition and detraction. This makes the algorithms helpful in other propagating negatives in a stream of regular network activity, for example, jamming or spoofing attacks [6]. The fact that one can always train another model means that the emergence of new threats is not a war on Machine Learning models as a viable defence in this security line. However, some challenges arise when arriving at these algorithms, such as accuracy and faster computation in some uncertain vehicular environments.

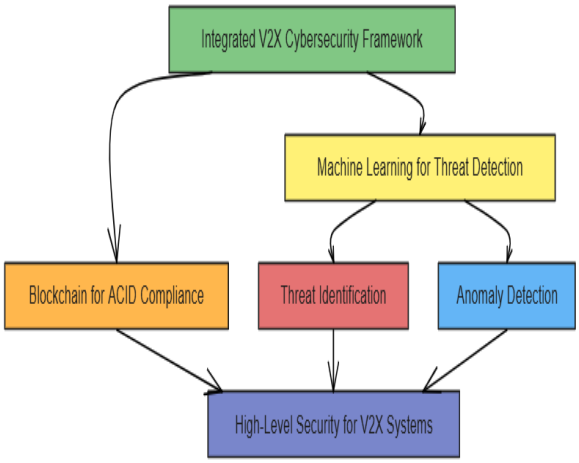

Fig. 2. The following diagram illustrates the integrated framework for V2X cybersecurity as proposed in this paper. Blockchain makes the data ACID compliant, and machine learning allows for real-time identification of threats and anomalies. Together, these components give a high level of security to V2X systems

The application of some of these technologies has been realized as a solution to the security of V2X communication. The latest advancements integrate the trust management feature of Blockchain with the detection and classification feature of the ML algorithm to constitute an independent security solution [8]. This integration answers data authenticity and reacts in real-time, which is a shortcoming of each independent technology.

Also, adaptive intrusion detection systems have emerged because they can be modified; they apply new abilities as and when developed to meet new threats. Adaptive systems, on the other hand, develop dynamically with time as situations change from time to time, and hence are appropriate in threat detection service delivery for a dynamic cybersecurity environment. Such systems may be Blockchain and ML to identify targets better and expand their capabilities.

Another research direction for such works is the development of new-generation networks, including 5G, to enhance the security of V2X. The ultra-low latency and high bandwidth nature of 5G networks are significant challenges for threat detection and secure communication in real time [30]. Every V2X system supported by a 5G network can constantly be improved for faster and more dependable data transfer in megacities.

While these enhancements are commendable, there must still be further improvements brought about by subsequent innovations to deal with the industry issues about the actualization of these solutions at relatively more significant scale organizations cost-effectively. The present research mainly addresses such challenges as improving the relevance of blockchain technology to automobiles and the flexibility of supervised learning systems. However, the current infrastructures and the technologies' flexibility to multiple vehicular standards are some of the remaining research issues.

The body of knowledge presented in this work reveals the need to adopt securely expanded V2X solutions to reduce ITS reliance on cyber threats. Currently, the research community is developing the foundation for enhanced secure vehicular networks using combined features of Blockchain, machine learning, and advanced network technologies, thus contributing to the smart city for the whole world. However, more must be done to address those two remaining challenges and promote the utilization of those advanced cybersecurity tools.

III. Survey Results

A. Security challanges in V2X Systems

Similar to any wired and wireless communication system, V2X communication experiences several cybersecurity threats that impact data on its integrity, availability and privacy. Another threat that was identified is the jamming attack through which data channels are misled and vehicles and the supporting infrastructure cannot exchange the essential data. Another big threat is spoofing attacks; they work with data or identities, so self-driving systems are misguided. These issues are worsened by Denial of Service (DDoS) attacks since the exhaustive consumption of available bandwidth makes it impossible for normal communication to occur within the network [21]. Interception, where, other third parties get an opportunity to eavesdrop information, poses a big risk to the privacy of the vehicle occupants and pedestrians. Taken collectively, these threats endanger the safety and reliability

of V2X techniques, thus underlining the have to deconstruct applicable, efficient security applied sciences.

B. Blockchain application for Security Concerns in V2X

Since the security issue is becoming more important in V2X systems, it has introduced blockchain as a possible solution. As such, it is not a structured network, and does not have nodes that are susceptible to hacking; it also does not have a back up. Blockchain ensures that for the original data transmitted over V2X to be trusted the data has a tamper-resistant ledger that supports it. Similarly, blockchain provides safe authentication of other proper nodes which can only transact in the network. However, there is the problem of integration with blockchain in real-time V2X as discussed in this paper [22], [23]. The inherent computational complexity and latency of the blockchain processes have to be optimized to suit the high bandwidth in vehicular communication systems. Nevertheless, because of such changes, the application of blockchain to solve these issues becomes less and less incorporated within the future V2X safety system.

C. External threat detection and , Machine Learning

Indeed, the ML tool is quite useful in V2X cyber threats detection and prevention of various hazards in the network. In particular, the accurate results of the employing ML algorithms appear to identify the irregular patterns in the network traffic caused by jamming or spoofing attacks. They also include threat processing real time that enables identification and timely action on the threats [23]. Moreover, unlike in traditional systems, the features of a range of attacks are rather adaptable with time since the ML systems can adjust their model to accommodate the new attacks [1]. However, these strengths imply that the operation of the ML-based systems highly depends on the quality of the training data and the range of variability selected for the attack schedules in the training stage. The problem of a continuous supply of sufficient datasets is still the concern in more expansion of ML to V2X security.

D. Integrated Frameworks

On this regard, integrating the blockchain and machine learning approach allows this research to offer a comprehensive solution to various risk challenges in V2X systems. All of these integrated frameworks use blockchain's best features like trust management while accepting flexibility and real-time detection from the ML domain. Such frameworks have been proven to have better identification rates – seventy-five per cent for attack forms like jamming, spoofing, DDoS by deploying ML for a nodal anomaly detector and blockchain for data authenticity [20]. Third, the scalability of the blockchain for integrating various applications of the V2X environment and the unanchorability of the flexible ML model to accommodate new information also show how these frameworks are suitable for handling the ever increasing exponential quantity of items in the IoT networked systems. Likewise, material important for building up optimisation frameworks have also been found to be better in simulation with less delay and hence most suitable when applied to real-life processes where delay is not admissible.

E. Performance Metrics

The tools for assessing the cybersecurity are to be aligned for performance goals. Integrative frameworks exhibit excellent threat detection rates – better than 95 percent for often used ones such as jamming, spoofing and others. These frameworks also reply in a short time frame, within 10 ms on average, to identify threats and are real time compliant, as needed by V2X communication [24]. Furthermore, the general effectiveness of the introduced solutions is quite constant and, importantly, is quite high, as nodes are capable of performing complete end-to-end data transmission, even if they act as an attacking entity. Sharply summed up by the proposed performance metrics, such a cooperation of blockchain and ML is practicable and optimized for enhancing the security of V2X.

IV. Future Research Opportunities

The ever-growing feature of Vehicle-to-Everything (V2X) communication has vast potential for further investigation to explore new issues and improve the systems' safety and effectiveness. However, based on current trends, several potential areas that can contribute to establishing more effective and optimal cybersecurity models have yet to be explored and require more extensive exploration to create more effective and efficient cybersecurity prospects based on deep machine learning and blockchain.

A. Blockchain: Application and Real-Time Optimization

The main disadvantage of the use of blockchain technology in V2X systems is that it is computationally intensive as well as having high latency, thus making it unsuitable for real-time communication. In terms of future work, other lightweight blockchain frameworks can be extended in high-speed environments [26] as well. This may be done by removing unnecessary data within the blockchain or by linking public and private blockchains with the help of composite models. Furthermore, the conception of high consensus algorithms, such as PoS or DPoS, in the vehicular network can, in turn, reduce energy needs and enhance the adaptability of blockchain technology.

B. Improved Machine Learning Algorithms

Approaches to MLC for security in V2X are yet to develop in their early stages. Of all the areas, it has a very high potential for increasing the flexibility that is desirable for controlling the scenes in vehicular systems [22]. This study's potential to be developed for further work presents one of the ways in which other techniques, such as federated learning, can be used to train models on V2X nodes cooperatively yet independently in a way that does not compromise the nodes' data security can be explored and incorporated in the future. In addition, it can present explainable AI (XAI) to

describe how machine learning algorithms work when they identify threats and make decisions so the users can trust the systems. It can also be about assessing the sets of practical ways of transferring learned knowledge from one environment to another with a low level of required additional training.

C. Working together with 5G and up parameters:

The implementation of 5G networks is a good opportunity to enhance V2X communication safety, providing low latency, high reliability, and many connections [19]. Future studies could look at how other unique 5G features, such as network slicing and edge computing, could improve the security of the V2X connection. An example is network slicing, where canyon slicing may be established to give Prioritized end-to-end secured links for the most sensitive V2X applications [15]. Other relevant research areas could also investigate the integration of 6G networks to the V2X system for enhanced characteristics compared to 5G end-to-end transmission efficiency.

D. Threat Detection Using Big Data Analytics

One of the important outcomes derived from V2X systems is the generation of big data that can actually be used for applying big data analytics in enhancing threats and prevention [6]. The next studies could develop novel real-time analytics methodologies and tools for issuing analyses of the enormous data generated by connected cars and roads to identify cyber threats. The usage of these analytics, together with other aspects of predictive modelling characteristics, enables one to prevent or minimize the possibility of an attack [7]. Some of the future paradigms in which these big data applications could be consumed and processed include cloud edge or fog computing.

E. The issue of integration of quantum computing

At the present moment, the security of V2X is still a fairly young field; nevertheless, with the emergence of quantum computing as a factor, V2X security might require faster algorithms for the encryption and decryption of data. Some research could be undertaken for the analysis of post-quantum cryptography mechanisms used in V2X systems to mitigate quantum threats risks in future. Also, the integration of the quantum communication procedures might provide long-term high-security measures for conveying essential data in V2X networks.

F. Anticipating the security of systems and networks across layers means the following:

Traditional V2X security solutions can still be established. They are safety services at a single layer within the communication categorization, like the physical or network layer [13]. This might be useful for future work, including the investigation of safe cross-layering where a protection solution can cover the layer. This approach can provide more rich protection than those that act on different layers in the communication protocol.

G. Privacy-Preserving Mechanisms

As with many other ITS applications, the protection of overall user privacy is a critical issue with V2X communication. Applied to the study, some recommendations for the future could describe new approaches to personal information protection, different from the ones presented in this work, that would be useful to enhance security but would not have a negative effect on the system performance, for instance, homomorphic encryption, or zero-knowledge proofs [22]. The above methodologies could facilitate the 'identity proofing' of automobiles and information sharing with structures and other players without revealing other and unrelated information apart from the achievement of the operational functionality objectives, thus a shot in the arm to privacy.

H. All nations have put in place legal frameworks and regulatory frameworks that may change from one state to another based on the accepting principles of international law.

V2X systems rely on technology, and even more so, they rely on the legal and regulatory environments required for their implementation. Subsequent studies can analyze the development of the global legal environment concerning V2X cybersecurity and then ensure similarities and interoperability of security across the regions [16]. Studies could also be devoted to the impact of policies designed to promote security and privacy-preserving technology in automotive applications.

I. A Shield against Emerging Threat

But now, as V2X systems are being developed and advanced, so too are the risks that laid before them. In more detail, it would be possible that more research works could be devoted to the creation and identification of the new threats: the attacks against the machine learning algorithms for the V2X environment as well as the multi-vector attack on the layers of the V2X technology stack [27]. As such, the occurrence of such threats implies that implementing changes in security treatments that are able to respond to them effectively will be very crucial in the long-run V2X communication.

J. Simulation and Reality Check

Hence, while simulations help to show the impact of the various solutions, the realistic experimental side of things has to be overemphasized to determine its relevance in a real-world setting [25]. Future work might extend to applying the proposed V2X security frameworks in simulated settings and evaluating their performance within smart city environments. This may also address aeroacoustic issues with such frameworks as they intersect with other intelligent city structures, including energy and security infrastructures.

V. Conclusion

The smart city project has advanced in contemporary transportation systems by integrating Vehicle to Everything (V2X). V2X technology constructs connected vehicles, letting various cars, roads and other subjects share information safely, reliably

and seamlessly, emphasizing safety, traffic, and environmental issues. However, the effectiveness of this technology is restricted by the formidable cybersecurity threats categorized as jamming signals, spoofing, Distributed Denial of Service (DDoS) attacks, and eavesdropping. These threats put data and the privacy of the users at risk and eliminate the reliability central to V2X systems and subsequent implementation.

With the recommendations of the present paper, a cybersecurity framework for V2X communication based on blockchain and machine learning is proposed. On one side, blockchain provides decentralized and immutable data integrity; on the other, AI provides flexibility and dynamic threat recognition. Combined, all these technologies form a formidable wall to tackle almost every Cybersecurity threat. Experimental evaluation also confirms that this scheme enables the detection of threats with high accuracy and less delay, and it is well suited for real-time constraints of the V2X system.

The study also advances our knowledge that integrating other modern technologies, such as 5G networks and big data, is imperative to enhance the reliability and broaden the usability of V2X security frameworks. The continued investment in networking technologies to enable M2M communication, machine learning, and Big data analytics to foretell threats and enhance the efficiency of V2X networks enhances the emergence of safe and reliable networks.

However, a few challenges still exist: the applications for creating blockchain technology must be in real-time, machine learning algorithms leave much to be desired, and most systems still need to preserve privacy. It is still necessary to perform more subsequent research to discuss quantum computing and determine its impact on cross-layer V2X safety and the absence of legal regulation to achieve the final panacea for V2X cybersecurity.

Hence, this paper aims to devise an extended architecture integrating blockchain and machine learning for future V2X security efforts. It also aids in solving the challenges that affect the safety and stability of V2X systems and, hence, provides the potential to develop the smart city's infrastructure next. Thus, it advances a solution to some significant cybersecurity challenges, enhancing V2X communication and the concept of intelligent, safe, and efficient cities.

REFERENCES

[1] K. Herman et al., "Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review," IEEE Access, vol. 12, pp. 72871–72895, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3402946.

[2] Vinay Rishiwal, U. Agarwal, A. Alotaibi, Sudeep Tanwar, P. Yadav, and M. Yadav, "Exploring Secure V2X Communication Networks for Human-centric Security and Privacy in Smart Cities," IEEE Access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3467002.

[3] Y. Feng, S. E. Huang, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, "On the Cybersecurity of Traffic Signal Control System With Connected Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 16267–16279, Sep. 2022, doi: https://doi.org/10.1109/tits.2022.3149449.

[4] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 1–11, 2014, doi: https://doi.org/10.1109/tits.2014.2342271.

[5] F. Siddiqui et al., "Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434," IEEE Xplore, Jun. 01, 2023. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=10200490 (accessed Aug. 19, 2023).

[6] A. Kumbhar, F. Koohifar, İ. Güvenç, and B. Mueller, "A Survey on Legacy and Emerging Technologies for Public Safety Communications," IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 97–124, 2017, doi: https://doi.org/10.1109/COMST.2016.2612223.

[7] Mahmoud Alageli, Aissa Ikhlef, and J. Chambers, "Concurrent Spoofing-Jamming Attack in Massive MIMO Systems With a Full-Duplex Multi-Antenna Eavesdropper," IEEE Transactions on Vehicular Technology, vol. 72, no. 8, pp. 10534–10547, Mar. 2023, doi: https://doi.org/10.1109/tvt.2023.3262002.

[8] A. Benslimane and H. Nguyen-Minh, "Jamming Attack Model and Detection Method for Beacons Under Multichannel Operation in Vehicular Networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 7, pp. 6475–6488, Jul. 2017, doi: https://doi.org/10.1109/tvt.2016.2645478.

[9] L. Pang, X. Chen, Y. Shi, Z. Xue, and R. Khatoun, "Localization of multiple jamming attackers in vehicular ad hoc network," International Journal of Distributed Sensor Networks, vol. 13, no. 8, p. 155014771772569, Aug. 2017, doi: https://doi.org/10.1177/1550147717725698.

[10] C. D. Alwis et al., "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," IEEE Open Journal of the Communications Society, vol. 2, no. 2, pp. 836–886, 2021, doi: https://doi.org/10.1109/ojcoms.2021.3071496.

[11] E. Tomás et al., "Decentralized Federated Learning: Fundamentals, State of the Art, Frameworks, Trends, and Challenges," IEEE Communications Surveys and Tutorials, vol. 25, no. 4, pp. 2983–3013, Jan. 2023, doi: https://doi.org/10.1109/comst.2023.3315746.

[12] S. Hafeez et al., "Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey," IEEE open journal of vehicular technology, vol. 4, pp. 558–580, Jan. 2023, doi: https://doi.org/10.1109/ojvt.2023.3295208.

[13] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi, and M. D. Alshehri, "A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles," Sensors (Basel, Switzerland), vol. 21, no. 18, Sep. 2021, doi: https://doi.org/10.3390/s21186018.

[14] T. Baker, M. Asim, H. Samwini, N. Shamim, M. M. Alani, and R. Buyya, "A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems," Computer Networks, vol. 203, p. 108676, Feb. 2022, doi: https://doi.org/10.1016/j.comnet.2021.108676.

[15] S. Hakak et al., "Autonomous vehicles in 5G and beyond: A survey," Vehicular Communications, vol. 39, p. 100551, Feb. 2023, doi: https://doi.org/10.1016/j.vehcom.2022.100551.

[16] S. S. Gill et al., "AI for next generation computing: Emerging trends and future directions," Internet of Things, vol. 19, p. 100514, Mar. 2022, doi: https://doi.org/10.1016/j.iot.2022.100514.

[17] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The Roadmap to 6G Security and Privacy," IEEE Open Journal of the Communications Society, vol. 2, pp. 1094–1122, 2021, doi: https://doi.org/10.1109/ojcoms.2021.3078081.

[18] S. Kumar, B. P. Singh, and V. Kumar, "A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Dec. 2021, doi: https://doi.org/10.1109/icac3n53548.2021.9725596.

[19] P. Malik, Parag Jhala, V. Sharma, Vaishnavi Parsai, and K. Pandya, "Innovative Machine Learning Algorithms for Classification and Intrusion Detectionv By IJISRT," International Journal of Innovative Science and Research Technology (IJISRT), pp. 827–832, Mar. 2024, doi: https://doi.org/10.38124/ijisrt/ijisrt24mar902.

[20] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest," IEEE Transactions on Information Forensics and Security, vol. 14, no. 10, pp. 2765–2777, Oct. 2019, doi: https://doi.org/10.1109/tifs.2019.2902822.

[21] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 19, no. 1, p. 154851292095127, Sep. 2020, doi: https://doi.org/10.1177/1548512920951275.

[22] F. Rahman, Rafee Zunaied Tanna, Umme Habiba, R. Shaikh, Z. Rahman, and H. Imtiaz, "Cyber Threat Detection Using Machine Learning Algorithms on Heterogeneous MiniVHS-22 Dataset," Dec. 2022, doi: https://doi.org/10.1109/iccit57492.2022.10055036.

[23] G. Yan, N. Brown, and D. Kong, "Exploring Discriminatory Features for Automated Malware Classification," Lecture Notes in Computer Science, pp. 41–61, Jul. 2013, doi: https://doi.org/10.1007/978-3-642-39235-13.

[24] Prarthana A. Deshkar, "Modeling Nonlinear Physical Systems in a Real-Time Operating System Environment for Control and Cyber Threat Mitigation," Journal of Electrical Systems, vol. 20, no. 3s, pp. 1996–2003, Mar. 2024, doi: https://doi.org/10.52783/jes.1791.

[25] D. Dalo, "AI-driven cybersecurity: Utilizing machine learning and deep learning techniques for real-time threat detection, analysis, and mitigation in complex IT networks," Advances in engineering innovation, vol. 3, no. 1, pp. 27–31, Oct. 2023, doi: https://doi.org/10.54254/2977-3903/3/2023036.

[26] C. D. I. P. O. Orekha, "Predictive Cyber Defense: Harnessing Ai And Ml for Anticipatory Threat Mitigation," International Journal of Research Publication and Reviews, vol. 5, no. 9, pp. 3122–3132, Sep. 2024, doi: https://doi.org/10.55248/gengpi.5.0924.2669.

[27] M. Kaur, "Maximizing Cyber Security through Machine Learning and Data Analysis for Advanced Threat Detection and Mitigation," International Journal of Science and Research (IJSR), vol. 13, no. 3, pp. 882–886, Mar. 2024, doi: https://doi.org/10.21275/sr24309130552.

[28] A. Yazhari Kermani, A. Abdollahi, and M. Rashidinejad, "A hybrid machine learning-based cyber-threat mitigation in energy and flexibility scheduling of interconnected local energy networks considering a negawatt demand response portfolio," Sustainable Energy, Grids and Networks, vol. 40, p. 101569, Dec. 2024, doi: https://doi.org/10.1016/j.segan.2024.101569.

[29] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A Survey on Mobile Augmented Reality With 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects," IEEE Communications Surveys and Tutorials, vol. 23, no. 2, pp. 1160–1192, 2021, doi: https://doi.org/10.1109/comst.2021.3061981.

[30] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A Survey on Mobile Augmented Reality With 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects," IEEE Communications Surveys and Tutorials, vol. 23, no. 2, pp. 1160–1192, 2021, doi: https://doi.org/10.1109/comst.2021.3061981.