The Cyber Physical Immune System: A Self-Healing V2X Framework for Global Defense and Healthcare

Babajide Asaju[1,2], Almustapha Wakili[1], Saugat Guni[1] and Woosub Jung[2]
[1]Towson University, USA
[2]Naval Postgraduate School, USA

basaju@towson.edu (corresponding author)
awakili2@towson.edu
sguni1@towson.edu
woosubjung@towson.edu

Abstract: The cyber-physical immune system (CPIS) is an important field in healthcare security, a chemistry reactor-based, AI-friendly framework that shields healthcare and urban structures like the human immune system. This self-sufficient network identifies a threat, contains it, and neutralizes it in minutes without any disruption to company operations. John Arquilla (2021) coined this era of social networks and" netwars." Cyberwarfare is on the rise around the world, and individuals, commercial companies, and institutions of all kinds are among the first to feel its sting. AI and real-time CPIS analytics allow for the expansion of coverage based on new threats, thus connecting cybersecurity and critical infrastructure protection. These ideas make it possible to identify the conceptual background, main components, and transformative characteristics of CPIS, as well as to consider its potential use in V2X communications, worldwide defense and medicine to overcome difficulties and facilitate further development. In this paper, we present the current threats in research with the prevailing challenges of current self-healing in CPIS for both global defense and healthcare systems. We explain the key components of the self-healing functionality of the CPIS in healthcare.

Keywords: AI-driven systems, Smart medical devices, Cybersecurity

1. Introduction

The current climate calls for an urgent need for a holistic investigation of the challenges that overwhelm the defense system and healthcare infrastructure. Every minute, numerous threats loom over the Internet of Things (IoT) and Cyber-Physical Systems (CPS) devices across all infrastructures. Within the IoT and CPS domains, many studies have been conducted on vehicle-to-everything (V2X) communications to help different forms of transportation applications for road safety, traffic accuracy, user threat information, and patient privacy. This technology facilitates direct communication between vehicles (V2V) and between vehicles and the traffic infrastructure (V2I) Rammohan et al. (2023). The proliferation of V2X communication systems raises fundamental questions regarding the protection of individual privacy rights Asaju (2024). Meanwhile, the digital environment has introduced many new threats, especially in the public and private healthcare infrastructure and systems that are vital to V2X communications and health security.

With the new and growing complex world of technology, there is a growing demand for sound cyberphysical systems. The combination of physical infrastructure, communication systems, and smart algorithms has introduced a new class of systems called cyber-physical systems (CPS), which have transformed various fields, including healthcare, transportation, and smart cities. However, the integration of these systems has exposed them to various cyber-risks, including malicious, accidental, and unintended disruptions. Due to this challenge, a novel technology called a cyberphysical immune system (CPIS) has been introduced as a fashionable solution Ferrag et al. (2018).

This study adopts a narrative research method within the qualitative methodology, using existing literature to highlight theories and machine learning algorithms to adapt AI and blockchain to cybersecurity in the healthcare and transportation sectors. The medical infrastructure must be robust against external threats and attacks due to the sensitive and personal information they collect Gatouillat et al. (2018). As these technologies advance, there is a need to expand security mechanisms to protect connected systems, such as medical facilities, from emerging risks. The study focuses on improving the scalability of these technologies and reducing their high computational requirements, which will open possibilities for their use. This study explores the complexity of cyber-physical information systems (CPIS) in the Internet of Things (IoT) and vehicle-to-everything (V2X) communication, examining potential opportunities for efficiency and functionality, especially in sensitive domains such as health and transportation. V2X technology is expected to offer various services to create a safer and more comfortable user environment Liu et al.(2020b).

To address these challenges, researchers have explored CPIS as a viable solution derived from the natural human immune system. This approach can detect, isolate, neutralize, and recover from cyber threats. The literature reveals that techniques have been developed to identify and control threats as they arise. In addition, blockchain technology has been investigated for its potential to provide enhanced data security and faultless messaging in distributed systems, helping to prevent advanced threats Morris et al. (2009). The study also examines various privacy-preserving schemes that have been suggested in the literature. Attaining a solution that satisfies the requirements of low communication overhead, real-time processing, and a high level of security while maintaining a lightweight size that can be deployed on edge devices is essential Boubaker et al. (2023). A side-by-side comparison of different security and privacy approaches for fog-based IoT medical applications was performed to evaluate their effectiveness in protecting sensitive information in healthcare settings Ponnambalam (2010).

Although CPIS and blockchain technologies offer promising solutions for improving cybersecurity in healthcare and transportation, their high computational requirements and scalability issues currently limit their widespread implementation in sensitive domains, such as medical facilities and V2X communication systems. The Morris water maze test is a widely used behavioral task to assess spatial learning and memory in rodents. This test involves placing an animal in a circular pool filled with opaque water, where it must locate a hidden platform using spatial cues.

Figure 1 presents an example of the visualization of medical-based nodes within the framework of a comprehensive V2X CPIS. The model is an integral component of an interconnected healthcare security architecture designed to detect cyber-physical threats in real time, thereby enabling responsive threat management.

The purpose of this study encompasses the following key areas that aim to contribute to improvements in this field.

- The main goal of this study is to recognize the latest machine learning tools, methods, and algorithms to interceptframework for global defense and healthcare self-healing functionality into cyber–physical immune systems.
- The capability of cyber-physical immune systems will be analyzed with respect to state-of-the-art technology, and artificial intelligent tools and methods in carrying out the overall functionality of self-immunology will be explored.
- The current literature will be critically reviewed to identify current state of techniques, tools, algorithms, modelclassifications, methods, frameworks, networks, and architectures currently deployed for a cyber-physical immune approach.

The remainder of this paper is organized as follows. Section 2 provides a theoretical framework for the development of AI-based cyber-sensitivity surveys on how threats can be detected and confined. Section 3 presents an overview of IoT and V2X using Machine Learning Background, structures, and typical applications in the global defense healthcare infrastructure. Section 4 presents an overview of the background, machine learning, and blockchain applications of cyber-physical immune systems (CPIS) and their applications in healthcare infrastructure. In Section 5, we discuss how the protection of IoT and V2X using machine learning and blockchain in cyberphysical systems can have a greater impact on real-time threats to immune systems. Some significant open issues and research challenges for the Integration of ML and Blockchain in Cyber Security and much larger perspectives are addressed. In Section 6, we address how the scalability and cost of the solutions can be used to protect patient data privacy in the blockchain domain. Finally, we conclude this paper on the advancement of cyber-physical systems development of newer methods to make AI work easier to interpret data protection in Section 8.

2. Theoretical Framework for the Development of AI-Based Cyber Security

The cyber-physical immune system (CPIS) is inspired by the concept of a human immunological system, which entails the ability to identify threats, confine them, and eliminate them to preserve systemic health. In biological systems, the immune system operates through two primary layers: the natural defense, which is rapidly general, and the acquired defense, which becomes more specific over time Polo (2024). Therefore, a double-sorted strategy is necessary to prevent the development of new methods to avoid protection. Likewise, CPIS incorporates these ideas into a theory of cyber security and uses biological approaches to protect the infrastructure against different types of cyber threats.

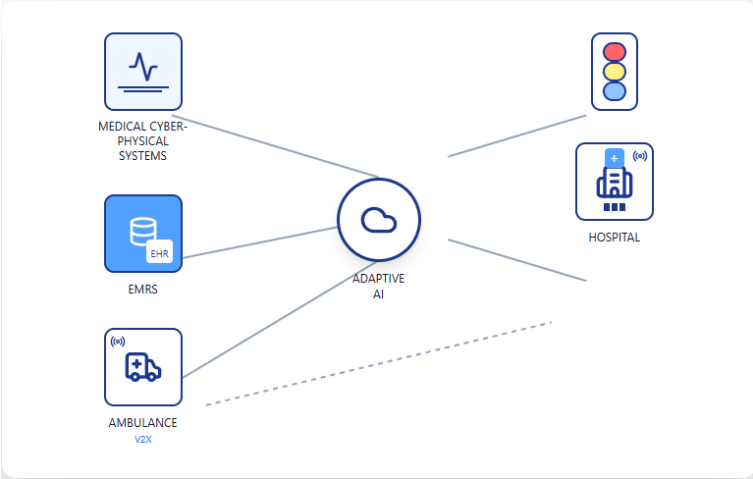

Figure 1: Simulation Visualization of a Hospital Based Node

In the human immune system, pathogen recognition is performed by pattern recognition receptors that grab foreign antigens that stick to body cells and create defensive mechanisms. This concept is also seen in CPIS, and in the system, the AI algorithms serve the purpose of the detection component, which monitors network activity and identifies signs of malicious activity.

In CPIS, isolation entails cordoning off affected nodes in a network to avoid the extension of threats to other parts of the network. More specifically, Farooq and Zhu (2020) noted that network segmentation could be a valuable way to prevent cyber risks, as well as using concepts reminiscent of biological containment. Neutralization is the last reaction to threats that exist in the environment, through specific actions carried out on objects. Similarly, in CPIS, AI countermeasures neutralize threats, after which the system quickly restores operations Hasan et al. (2020), and provides information on secure and reliable recovery concepts in cyber-physical domains to achieve operational continuity, such as the body's ability to work after defeating an infection.

AI is central to the CPIS and is responsible for the defense adaptability of the system. Such algorithms allow CPIS to analyze vast quantities of raw data, which, when analyzed, will show signs of possible threats that are in their early stages. Machine learning models could be extremely good at discovering new and previously unknown use cases of IoT, which is quite important for the complexity of CPIS. The ability of AI to learn means that CPIS continues to be potent when marked threats change, in the same way adaptive immunity fortifies itself with lessons from previous exposure. Chen *et al*. (2020) showed that another positive change element is self-healing which is helped by AI to allow CPIS to react and patch up an attack with barely any input from people. With embedded real-time analysis, the system can quickly assess damage and team responses and formulate a response. Chaterji *et al.* (2018) highlighted the importance of such capabilities to protect themselves from more advanced cyberattacks. At the same time, Bajpai *et al.* (2020) noted that real-time decision management enables us to minimize risks and maximize response effectiveness and efficiency.

As shown in Figure 3, the CPIS cybersecurity framework was designed as a voluntary risk-based framework to improve cybersecurity in critical global defense healthcare infrastructure. Credit goes to the former President Barrack Obama's executive order calling for the establishment of a brand-new set of standards, guidelines, and practices to help organizations charged with providing the nation's financial, energy, healthcare, and other critical systems to better protect their information and physical assets from cyberattacks Ajakwe et al. (2022).

As observed in deliberations regarding IoT security threats, machine learning is increasingly being used in analytics and countermeasure detection Weingart (2000).

To ensure safety and optimize efficiency, it is imperative to establish a connection between vehicles and external systems through secure data exchanges. If these systems are not reinforced with secure mechanisms, they can be attacked and the results can be horrendous. Studies in this field have described different measures, including cryptographic solutions, safe network connections, and additional applications of intelligent technologies for the real-time discovery of inconsistencies [Rao et al. (2023)].

3. Protecting IoT and V2X using Machine Learning and Blockchain

Modern computing machine interactions can take on different forms of remote connectivity to IoT environments, where remote computing can function as a standalone microsystem by ensuring the security of V2X communications, which is essential to facilitate access to network resources. Various solutions have been proposed to address the security challenges most common to blockchain applications, which can be classified into cryptography-based and trust-based schemes. Compared to the data, Hakeem et al. Hakeem et al. (2020) suggested that authentication and preservation of privacy are among the most pressing concerns in V2X communication. Their application can be seen in different industries, protecting them from future cyber threats.

3.1 Healthcare Systems

The concept of CPIS plays an important role in protecting defense technologies from cyber threats. Emerging healthcare systems interact with critical medical networks, autonomous systems, and important infrastructures, which involve defense threats and require protection against cyber threats that can potentially cause interference or threaten national security. The CPIS can then observe these channels and block the threats identified in system exposure [Dorn (2023)]. Self-healing is more critical in cyber warfare environments, where attackers can proactively and strategically launch precise attacks on important infrastructures such as drones, unmanned aerial vehicles (UAVs), and defense communication networks.

3.2 Healthcare Infrastructure

Several IoT-based systems have permeated the healthcare industry, including remote health monitoring devices, wearable health monitoring devices, and IoT-connected imaging systems. They gather and send patient information, which, to some extent, is pertinent and, therefore, a target for cyber attackers. A threat to cyber security could result in poor patient care, stolen or lost medical records, or the failure of essential devices. CPIS acts as a workaround for these effects by constantly monitoring these devices and protecting patient data from intruders, Das et al. (2021)]. The self-healing capability of the system means that it can identify threats on unique devices, quarantine, and eliminate the threat without interrupting healthcare services. For example, a hospital can protect its medical device system against ransomware attacks that can inevitably paralyze its functions. Thus, CPIS can also help to keep the infrastructure of healthcare facilities secure and functioning during severe attacks, including DDoS, as it can detect the source of the attack and redirect traffic.

3.3 Urban Infrastructure and V2X Frameworks

Due to the actively developing concepts of smart cities, highly intelligent cars, and interconnected urban components, questions arise about cyber security. Urban areas have become dependent on digital systems for traffic control, electrical supply, waste removal, and security. The operational complexity has increased because today's autonomous vehicles (AV) and vehicle-to-everything (V2X) communication systems require real-time data exchange between vehicles, infrastructures, and other smart sensors. The former can improve the reliability of urban critical infrastructure by safeguarding V2X communication networks, which is paramount for the safety and efficacy of driverless vehicles. These networks may also be an open door for hackers and information technology criminals, which can cause crashes or traffic interference [Kiela et al. (2020)].

4. Protecting IoT and V2X using Machine Learning and Blockchain in Cyber-Physical Immune Systems

CPIS mechanisms were developed to protect complex systems from cyber threats, like human immune systems. These systems are extremely important for the Internet of Things and communication between cars and everything else. CPIS uses machine learning and blockchain to improve information security against cyber threats. CPIS combats cyber threats by learning and changing, like the defenses of the body. This is a major step in cybersecurity due to the blending of biology and advanced technology, which is extremely helpful for connected systems and essential services. (W Yu et al., 2025). The IoT also plays an important role in business. IoT has been reported to be one of the most important technologies that will affect US interests in 2025. It defines why organizations seek to improve their ISO 27001 ISMS. These reasons include looking for a way to provide proof of activities, due care, due diligence, and regulatory compliance.

4.1 Real-time Threat Detection and Mitigation

Mitigation in risk management and disaster preparedness encompasses two key objectives: reducing exposure and minimizing possible loss. Each of these categories can contribute to the enhancement of early warning

capability systems. Likewise, infrastructure protection can be strengthened to withstand the potential impacts that can occur with implementable response plans.

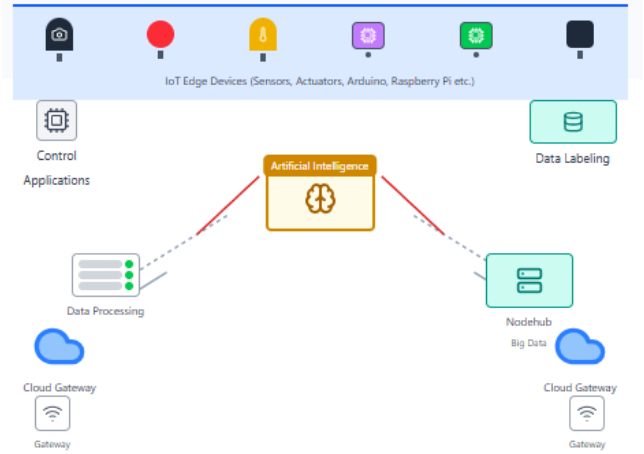

Figure 2: Cyber-Physical Security for IoT Networks

In addition, machine learning can continuously monitor systems to detect any behavior that does not match the typical trends or symptoms of a cyber-attack. This capability enables detection to be performed in real time, providing authorities with the opportunity to intervene before an attack is performed. Automation of Security Responses

The second major benefit of using AI-powered machine learning algorithms in CPS and IoT security is automation. It can provide immediate defensive actions that can be executed when a threat is recognized, such as quarantining a certain component or blocking certain traffic patterns without human intervention. This response minimizes impact and maintains system integrity, which is vital in real-time systems such as health or transportation, where system downtime has disastrous implications [Pandey and Misra (2016)].

4.2 Reduction in System Downtime and Operational Disruptions

Using automated, real-time responses are worked on, thereby lowering the chances of extended system offline time. These systems can bounce back from an attack or several disruptions by reproducing data and rerouting circulation efficiently, thus incurring minimal damage. This benefit is especially valuable in industries where end-user uptime is critical, particularly in healthcare, where interruptions can directly cause patient harm [Farooq and Zhu (2020].

4.3 Improved Resilience to Evolving Threats

Blockchain enhances the reliability of distributed systems in connected environments, proving the reliability of data and network connections. For example, its structure is decentralized, which eliminates the problem of broken control. Due to decentralization and the impenetrable characteristics of the blockchain, no one can manipulate the data, which makes it quite secure and easily checked after a while Rao et al. (2023). This makes it an ideal solution for encrypting sensitive data stored in various systems that must meet the highest trust requirements, including IoT systems in the healthcare and transport industries. In the context of vehicle-to-everything (V2X), the blockchain guarantees that only genuine information is allowed for vehicle and infrastructure data exchange; it prevents the interference of false data from malicious actors, traffic signals, vehicle status, or navigation data [Catrina et al. (2020)].

5. Challenges for the Integration of ML and Blockchain in Cyber Security

The application of machine learning and blockchain in existing protective cyber security systems is not only challenging but also faces several technical and organizational barriers. ML can optimize blockchain networks by improving consensus mechanisms, reducing computational overhead, and facilitating intelligent smart contracts for efficient transaction validation Liu et al.(2020a). Current applications in areas such as health, transport, and finance have not been developed with the input/output requirements of today's technologies, such as blockchain and machine learning. In turn, these systems can be incompatible with advanced solutions, encountering compatibility problems, slowness, and additional costs along the way Zhang et al. (2019).

Blockchain is very advantageous in terms of improving cybersecurity due to its distributed and decentralized properties, such as offering an efficient means to make secure and transparent transactions. However, the use of technology entails a high storage and processing capacity for the database.

5.1 Biased Risks in the Decisions Taken by AI

In the case of AI systems in cybersecurity and healthcare, which are based on data used for training, this problem is rather acute. Poor data used while developing AI models lead to the development of biased models, negatively leading to either insecurity or poor health service delivery. In cybersecurity, for example, if the training data include a single type of threat, the resulting model will also focus on this type of threat and will not notice new or regional ones. This could open systems to cyber-attacks, taking advantage of previously untouched threats. For example, an AI model trained using attack data from one region or a specific network environment is unlikely to identify emergent threats in a different region or a different technological environment of operation from the same threat-actor group.

This also applies to the type of data collected, where certain forms of attack are overly representative, while others receive little representation.

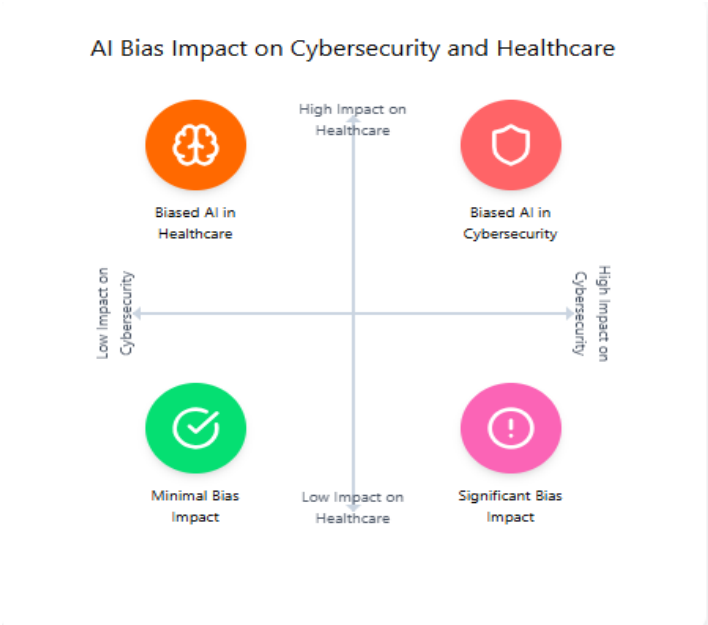

Figure 3: AI Bias Impact on Cybersecurity and Healthcare

A diagram showing the impact of AI bias on cybersecurity and healthcare. which further exacerbates health inequalities. In addition, powered estimation models might be counterintuitive to professional healthcare providers' estimates and might pose ethical issues. The AI system may reproduce bias if it learns from the data that a disparity existed in previous healthcare or security structures. In such cases, AI models use preferential bias, for example, in favor of a certain group, thus reducing fairness in the distribution of items such as healthcare and security.

5.2 Solving Scaling and Cost Problems

The popularity of machine learning and blockchain raises the problem of cost and scalability for many organizations that want to implement these technologies into their security systems. Owing to its decentralized nature, each participant in the blockchain network must process, store, and verify transactions, increasing the rate of storage and computation as the complexity of the network increases Alghamdi et al. (2024). Because every node in the network is required to replicate the entire blockchain ledger and is involved in the consensus mechanism, the cost of the infrastructure increases, preventing the effective massive deployment of blockchain solutions. This is even more difficult in sectors with huge networks of connected devices, such as the health and transport sectors, where every device and system must be secure.

5.3 Scalability and Costs of Solutions

The use of AI and blockchain in sensitive domains such as medicine and warfare raises grave ethical problems for the institute or system that makes the decision and is responsible for it, as well as possible negative impacts

that can be devastating. In the sphere of healthcare care, the immutability feature of blockchain technology, despite the opportunities it opens to improve the integrity of the data, can suggest ethical questions. If an error is made in the medical records, the records are permanent on the blockchain, and this can be a disadvantage because there can be no corrections once the medical record is recorded this way. For example, a blockchain can lock information in permanent records. Although there is transparent and secure management of patient data via blockchain, this fixed schema creates a conflict between the security management of the patient database and the need to provide up-to-date patient records. Although machine learning and blockchain can increase security, they are not impermeable to security threats.

Most AI algorithms learn from the data fed to the system and therefore reproduce bias. For example, algorithms that act in healthcare facilities might inefficiently diagnose the level of some demographic groups because the training data samples contain insufficient diverse information, which can lead to ethical issues such as fairness and equality. W. Jung et al., (2023), healthcare systems have also used outdated legacy software that is still in use owing to its critical functionality but is often no longer supported by manufacturers, making them vulnerable to security risks and compatibility issues Affia et al. (2023).

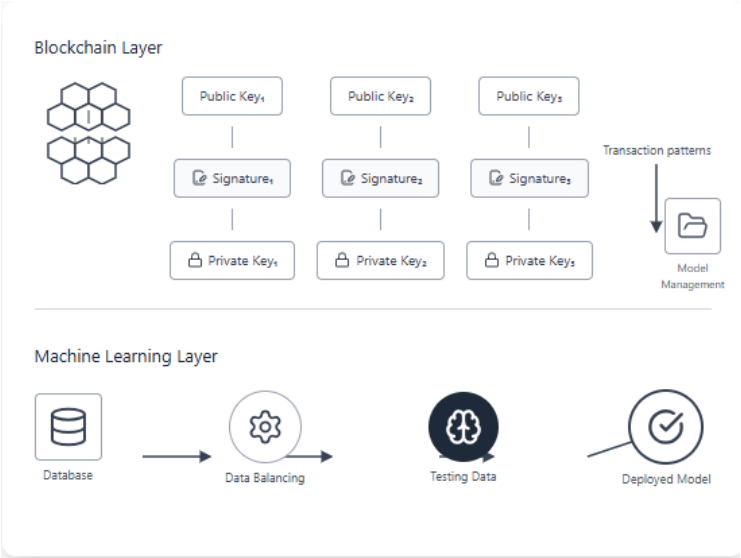

Figure 4: Challenges in Blockchain and Machine Learning

6. Advancing Cyber-Physical Systems

The creation of universals of where CPISs should be deployed has resulted in the problem of interoperability and security, given that the application is implemented haphazardly in different sectors. Such standards would standardize these processes by establishing normative measures for data protection, secure information exchange, and system links. Some of these standards could reduce the level of difficulty associated with deployment and guarantee the level of standardization needed, hence enhancing the availability and reliability of CPIS worldwide.

The modularity of CPIS is sometimes restricted by the associated need for computational, energy, and infrastructure resources. Future research efforts should focus on algorithms with low energy requirements and the corresponding system structures, in addition to edge computing, to facilitate the large-scale implementation of B-MAC. Improved scalability will create a new CPIS that can address different application requirements on different scales and regions.

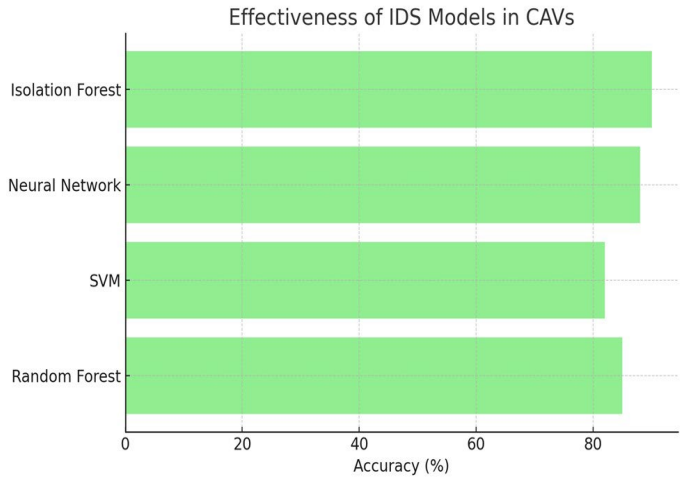

Figure 5: Effective of IDS Models in CAVs

7. Discussion

7.1 Connected and Automated Vehicles and Safety

Safety is the least we can expect from Connected and Automated Vehicles (CAVs), with many promising advances that come with performance improvements by the automotive industry and research findings, together with enhanced user experience developed through new services to help with traffic flow integration. (e.g., development of new information services) when CAVs become a part of everyday commuting. The "core" of road planning modules for a CAV system is algorithmically described within the system Ahmad et al. (2024).

CPIS is a form of bio resilience, and cybersecurity interface developed to identify recoverable common threats to cyber-physical threats in interconnected designs, which can mimic a biologically immutable system that can only be useful alone. infrastructures such as healthcare networks, smart cities, and connected automated vehicles (CAVs).

7.2 Policy Implication and Challenges

The importance of cybersecurity and road safety, as noted in previous sections, must be put into action by policymakers to increase the implementation of CAVs in traffic during medical emergencies. This study presents a summary of key cybersecurity problems in connected and automated vehicles (CAV) and their long-term impact on road safety, as well as the solutions proposed in the current literature. The significance of cyber-attacks and malicious information. The deployment of Connected and Automated Vehicles (CAVs) in traffic scenarios during medical emergencies requires policymakers to address essential cybersecurity and road safety issues. This study emphasizes several critical aspects of the problem.

8. Conclusion

The coupling of physical systems with AI can help CPIS leverage threat detection and mitigation, outperforming conventional methodologies to propose preventive measures against evolving threats. For the maximum effectiveness of the CPIS concept, its implementation requires interdisciplinary cooperation. We explain that AI and cyber security, engineers, policymakers, and social science professionals are critical and essential to join forces. Future studies propose the integration of better AI defense systems into existing CPIS models. As novel technologies continue to emerge in this field, they can shift from reactive to predictive security, allowing organizations to protect themselves from new threats in global markets. However, AI-based patient-oriented CPIS can provide real-time threat data learning, thus improving the use of ML algorithms for threat assessment. In the long run, these systems will develop the capacity to minimize the significant impact of cybercrimes and system failures.

AI and Ethics Declaration: This research was conducted in accordance with established academic ethical standards. Artificial intelligence tools were used solely to support language refinement formatting consistency and structural clarity. No AI systems were used to generate original research findings experimental results datasets or technical conclusions. All system designs methodologies simulations analyses and interpretations were conceived, developed and validated by the authors. The study did not involve human subjects' personal

data or clinical interventions and therefore did not require institutional ethics approval. The research focuses on cybersecurity risk analysis system modeling and controls experimental evaluation of connected cyber physical and medical technologies. All experiments were conducted in simulated or laboratory-controlled environments without impact on operational or patient-facing systems. The authors affirm full responsibility for the integrity, originality and accuracy of the work and confirm compliance with the ethical guidelines of the ICCWS ACI conference.

References

Ajakwe, S.O., Nwakanma, C.I., Kim, D. and Lee, J.M. 2022. Key wearable device technologies parameters for innovative healthcare delivery in B5G network. A review. IEEE Access, 10, pp. 49956 to 49974.

Alghamdi, T.A., Khalid, R. and Javaid, N. 2024. A survey of blockchain based systems. Scalability issues and solutions, applications and future challenges. IEEE Access, XX(YY), pp. xx to yy.

Alnasser, A., Sun, H. and Jiang, J. 2019. Cyber security challenges and solutions for V2X communications. A survey. Computer Networks, 151, pp. 52 to 67.

Asaju, B.J. 2024. Privacy preservation techniques in V2X ecosystems. Safeguarding individual privacy in connected vehicle environments. Journal of Artificial Intelligence Research, 4(1), pp. 58 to 72.

Arquilla, J., 2021. *Bitskrieg: the new challenge of cyberwarfare*. John Wiley & Sons.

Bajpai, A., Pandey, R., Singh, A.P., Jain, M. and Mishra, S. 2020. Article title placeholder. International Journal of Intelligent Communication and Computer Science, 1(1), pp. xx to yy.

Boubaker, S., Alsubaei, F.S., Said, Y. and Ahmed, H.E. 2023. Lightweight cryptography for connected vehicles communication security on edge devices. Electronics, 12(19), p. 4090.

Chaterji, S., Modi, A. and Singh, R. 2018. Impact of technology enablement on employee engagement. Corporate Communications: An International Journal, 25(1), pp. 132 to 153.

Chen, L., Zhang, C. and Ness, S. 2020. AI based intrusion detection for IoT. Obstacles, resolutions and prospective changes. Journal of Computer Science and Technology, 35(3), pp. 447 to 460.

Das, S., Siroky, G.P., Lee, S., Mehta, D. and Suri, R. 2021. Cybersecurity and the need for data and patient safety with cardiac implantable electronic devices. Heart Rhythm, 18(3), pp. 473 to 481.

Dorn, T.M. 2023. US critical infrastructure. Its importance and vulnerabilities to cyber and unmanned systems. Page Publishing Inc., New York.

Farooq, M.U. and Zhu, Q. 2020. Blockchain in emerging IoT applications. Review and open research challenges. Internet of Things, 11, p. 100240.

Ferrag, M.A., Derhab, A., Maglaras, L., Mukherjee, M. and Janicke, H. 2018. Privacy preserving schemes for fog based IoT applications. Threat models, solutions and challenges. In Proceedings of the International Conference on Smart Communications and Networking Technologies SaCoNeT. IEEE, New York, pp. 37 to 42.

Gatouillat, A., Badr, Y., Massot, B. and Sejdic, E. 2018. Internet of Medical Things. A review of recent contributions dealing with cyber physical systems in medicine. IEEE Internet of Things Journal, 5(5), pp. 3810 to 3822.

Hakeem, S.A.A., Abd El Gawad, M.A. and Kim, H. 2020. Comparative experiments of V2X security protocol based on hash chain cryptography. Sensors, 20(19), p. 5719.

Hasan, H.R., Salah, K. and Jayaraman, R. 2020. A blockchain based framework for secure and trustworthy smart manufacturing. Blockchain Research and Applications, 1(1 to 2), p. 100001.

Jung, W., et al. 2023. IoT health devices. Exploring security risks in the connected landscape. IoT, 4(2), pp. 150 to 182.

Liu, J., Zhang, W., Badr, J., Wang, L. and Qingjin. 2020. Cyber security challenges and solutions for V2X communications. A survey. Computer Networks, 151, pp. 52 to 67.

Morris, R., Trivedi, M.M. and Pan, S.J. 2009. Preferences for treatment outcomes among patients with panic disorder. IEEE Transactions on Wireless Communications, 58(5), pp. 1 to 14.

Pandey, R.K. and Misra, M. 2016. Cyber security threats in smart grid infrastructure. In National Power Systems Conference NPSC 2016. IEEE, New York, pp. 1 to 6.

Pantopoulou, L., Kritikos, K. and Magoutas, B. 2020. Machine learning in IoT security. Current trends and future directions. Future Generation Computer Systems, 112, pp. 1 to 13.

Polo, L. 2024. Revolutionizing sales and operations planning with artificial intelligence. Insights and results. International Journal for Multidisciplinary Research, 6(6), pp. xx to yy.

Rammohan, A., et al. 2023. Revolutionizing intelligent transportation systems with cellular vehicles to everything technology. Current trends, use cases, emerging technologies, standardization bodies, industry analytics and future directions. Vehicular Communications, 43, p. 100638.

Rao, P.M., Jangirala, S., Pedada, S., Das, A.K. and Park, Y. 2023. Blockchain integration for IoT enabled V2X communications. A comprehensive survey, security issues and challenges. IEEE Access, 11, pp. 54476 to 54494.

Yogeswaran, M. and Ponnambalam, S.G. 2010. Swarm robotics. An extensive research review. In Advanced Knowledge Application in Practice. InTech, Rijeka, pp. 259 to 278.

Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J. and Yang, X. 2017. A survey on edge computing for the Internet of Things. IEEE Access, 6, pp. 6900 to 6919.

Zhang, X., Jiang, X. and Yang, X. 2019. Blockchain for IoT. A survey and research directions. Future Generation Computer Systems, 92, pp. 268 to 283.