



AI in Motion: Securing the Future of Healthcare and Mobility through Cybersecurity

**Ahmad Bacha¹, Murad Khan², Abdul Mannan Khan Sherani³, Heta Hemang Shah⁴,
 Noman Abid⁵, Nahid Neoaz^{6*}, Mohammad Hasan Amin⁷**

^{1,2,3} Washington University of Science and Technology, United States

⁵ American National University, United States

⁴ Independent Researcher, United States

⁶ Wilmington University, United States

⁷ Kettering University, United States

Emails: abacha.student@wust.edu¹, khanm@students.an.edu², asherani.student@wust.edu³,
 Heta2973@gmail.com⁴, nomanabid12345@gmail.com⁵, nahidneoaz@yahoo.com^{6*},
 amin3672@kettering.edu⁷

ABSTRACT

The development of artificial intelligence (AI) is bringing significant transformation to the healthcare and mobility sectors, although it is creating new cybersecurity challenges. This research aims to analyze the cyber threats arising from the application of AI in health and mobility systems, and explore security measures to mitigate these risks. The qualitative research method included literature analysis and data collection from various relevant case studies. The results show that AI improves efficiency in the healthcare sector, such as more accurate diagnosis and personalization of patient care, but also presents threats such as patient data breaches and algorithm manipulation. In the mobility sector, AI plays a role in the development of autonomous vehicles and intelligent transportation systems that face the risk of hacking and data manipulation. Various solutions, such as blockchain, federated learning, and homomorphic encryption, have been identified as effective approaches to improve AI security. The implication of this research is the importance of cross-sector collaboration between policymakers, technologists, and cybersecurity experts to ensure the safe, ethical, and reliable use of AI. With strengthened security measures, AI can continue to provide significant benefits to society and industry sectors.

Keywords: Artificial Intelligence, Block Chain, Data Security, Healthcare, Security, Transportation.

INTRODUCTION

Artificial intelligence has been recognized as among the few technology this century that is gaining traction to revolutionize almost every operation in the mobility sector and beyond including the health industry. All of these sectors that were all segregated are now merging slowly under the context of integrated systems and internet of things. This convergence aims at promoting formation of efficient, accessible and personalized services. However, there is an

emerging difficulty in adding security as the foundation for artificial intelligence to work in an innovative society. Using Artificial Intelligence is now in the process of transforming healthcare starting with diagnosis and extending to treatment and lifestyle of the patients (Syed & ES, 2023). For instance, in the services of artificial intelligence, the automated algorithms can work for diagnosing imaging with better efficiency and work in prognosis of diseases and patient throughput. Nevertheless, with the progression in the healthcare system, there is, in the digital environment a number of threats as well. Telemedicine services together with electronic health records and medical devices with which large amounts of patients' identifying data are collected and transmitted attract hackers. Threatening any of these areas threatens the safety and privacy of patients hence why cybersecurity is important when using experts in healthcare (Reddy & Nalla, n.d.).

In mobility AI is improving the ability to drive automobiles autonomously, intelligent roads, and real time transportation network. These are all expected to redefine mobility of people and goods by enhancing safety, efficiency and availability. For instance, self-driving cars apply artificial intelligence to interpret data that a car sees and where it is to navigate properly. But this remains a blind spot because mobility solutions directly rely on the connected systems, thus are vulnerable to cyber threats. Hackers may take full control of this system, manipulate the transportation of vehicle, the PHISH, or whatever, or even acquire all the details of the specific user. This is why cybersecurity is now an important instrument in combating the threat to AI-dependent transport molarity to achieve meaningful outcomes (Rithin Gopal Goriparthi, 2023). The potential that both AI health care and mobility have are enormous but what it does is only showcase the plus side's then increase the negative impact on the other. How people can use self-driving automotive, for example, ambulances or drones to bring medical supplies in an emergency? While such innovations could go a long way in changing the healthcare delivery system some new challenges in cybersecurity ensue. Security regimes must exist and threats must be identified in a timely manner as well as healthcare and transportation sectors and technology influencers (Rithin Gopal Goriparthi, 2023). Following is an evolution of AI health care and mobility with special reference to the fact that security processes are still central to both. Reducing cybersecurity threats allow various stakeholders to achieve the optimum use of artificial intelligence systems with safety, ethical implication and reliability within an evolving technological environment held (Vijayakumar et al., 2024).

Based on the above background, the purpose of this research is to analyze the cyber threats arising from the application of artificial intelligence in the health and mobility sectors and explore security measures that can be applied to mitigate these risks. This research aims to provide a deeper understanding of how AI technology can improve efficiency and effectiveness in both sectors, but also potentially pose major cybersecurity challenges. The benefits of this research are to contribute to the development of science in the field of artificial intelligence, especially in the context of cybersecurity in the health and mobility sectors. This research can be a reference

for academics and researchers in understanding various aspects of threats and relevant security solutions. In addition, this research provides insights for policy makers, IT professionals, and medical personnel regarding the implementation of security strategies in the use of AI. By understanding the potential risks and solutions, the healthcare and mobility sectors can be better prepared for cyber threats. By raising awareness of the importance of cybersecurity in AI applications, this research will help create a safer and more trusted digital environment.

RESEARCH METHOD

This research uses a descriptive qualitative approach to analyze cybersecurity threats to artificial intelligence (AI) systems in the health and mobility sectors. This type of research was chosen because it aims to describe in depth the phenomena related to AI implementation and its impact on data security and related systems. Data was collected through a literature study that included scientific journals, official reports, and publications related to AI regulation and cybersecurity. Secondary data sources were used to provide a comprehensive overview of this research topic.

The data analysis technique used was content analysis, where the data was thematically analyzed based on relevant categories such as security threats, regulations, and mitigation technologies. The data is systematically analyzed to identify patterns and relationships between variables that support the research argumentation. The results of this analysis are expected to provide relevant insights to address the challenges faced in AI integration in the healthcare and mobility sectors, particularly in the aspect of cybersecurity.

RESULT AND DISCUSSION

AI in Healthcare: Transforming Patient Care

Artificial Intelligence (AI) is the future of the healthcare industry thanks to it learns and applies new models of treatment and services that make patients more comfortable and provide better outcomes. While in diagnostics, treatment and even in customizing the treatments according to the size of the patient's body, AI is gradually reintroducing itself into healthcare. This is important today mainly because most modern healthcare systems are tasked with much higher expectations due to ageing populations, chronic diseases, and dearth of resources in most regions of the world where AI can be of value (R G Goriparthi, 2023). However, for one of the most significant disciplines AI has identified an effective means of enhancing diagnostic capabilities. It may also be applied for radiologists, that is, for deciphering of roentgenograms, MRI, and CT, pathologists, as well as other specialists as they are capable to do it quicker and with almost comparable accuracy. The same fluorescent-based tools at one instance assist in diagnosing diseases like cancer, heart disorders, and neurological ailments in their preliminary stage that is compact for discrete survival. For instance, in training of models the large amount

of data, it can be easier to develop features that may be unnoticed when seeing the images in a diagnostic point of view of diseases (Damaraju, 2022).

It is also come up with an enhancement of the, the so called personal medicine where treatment is given according to the genetic information, starting from DNA pattern, life history and records of the patient. Big data methodology can assist with several aspects to enable the formation of proper treatment approach in reference to specific data types such as genomic data or clinical records. One of the main application areas is oncology with the help of AI to identify specific treatments corresponding to different types of cancer and not just prescribe certain drugs in the hope that they will somehow affect a particular disease (Chen et al., 2023). Furthermore, passive applications of diagnosis and treatment, AI is enhancing the patient surveillance and management. Wearable smart devices with an ML component can observe patients' states, and will have a stable foundation for early diagnosing. For instance artificial intelligence will assist the doctors in the management of the patient in the event that something abnormal such as irregular heart beating or high blood sugar levels is observed. A number of these technologies may be very wise for chronic diseases for instance diabetes, hypertension and heart diseases (Chirra, 2022).

AI is a critical solution to enhancing the functioning of healthcare systems. Asked how artificial intelligence fits in healthcare, Dr Tomar said: 'AI fosters productivity in many industries including working in the hospital and in supply chains.' Virtual assistant, or virtual health assistant and natural language processing chatbots are employed for constant patient support, answering patients' questions, appointment scheduling and healthcare consultation (Gadde, 2022). However, the integration of AI in healthcare as we seek to find out in this paper has some negatives. On this we concur, issues some of which include but data privacy, how these algorithms is going to be fair, good measures in cybersecurity and some other need to deliberate on so as to come up with safe artificial intelligence. On one hand, we can explain this by the fact that in today's world the focus in AI technology development is made not on the expansion of its spheres of application but on the development of new systems and their improvement (Syed & ES, 2023).

AI in Mobility: A new generation in mobility

Modern and complex technologies referring to artificial intelligence AI, are innovating mobility, developing transport, substituting the previous typical intelligent systems. Beginning with automated automobile transport to the adaptive traffic management, the integration of AI is slowly altering the way in which people and goods traverse cities and countries. Not only has the elements of utility and freedom in movement, but it is also providing solutions to the typical difficulties, such as traffic congestion, contamination of the environment, and security. Lighting and traffic signals, are perhaps possibly one of the greatest use cases of how AI can be used to enhance the environment and traffic (Reddy & Nalla, n.d.). These vehicles rely on high-level AI to process information coming from such devices as sensors, cameras and LiDARs to co-drive or

rather to merely observe and make decisions regarding road conditions and situations at the time of time, on the go. Today, the application of the self-driving cars and trucks for the commercial business is highly believed to reduce the rate of the fatal road accident which is mostly as a result of carelessness. In addition, spontaneous fleets may cause developing a delivery cycle and reduce the delivery time in general, for instance, in e-commerce and supply chain. However, to encourage more extensive use of the AVs in our society their cybersecurity needs to be improved so that they cannot be hacked or be involved in any other unlawful operation (Javaid et al., 2023).

AI is also making a massive contribution to public transport through various aspects like the issues of route, schedules and operating. Current ITS uses AI involves the analysis of information obtained from the GPS, sensors, and traffic cameras to provide sufficient prediction of traffic patterns. For example: Currently, traffic light can be programmed to change as per the rush hours or Cortex can control over the Road transports like Buses, Trains etc., can change their path depending on delay or event . Of such systems, the general result is that it increases reliability and decreases time for the commuter. Companies like Uber and Lyft that offer hailing rely on artificial intelligence for qualifications of customers and drivers, route and demand forecasts (Paul et al., 2023). In transportation AI is enabling the development of smart city structures that have interconnected transport systems. By applying movement concepts, numerical population data and environmental factors, AI assists urban lists to effectively propose efficient low-emission and environmentally-friendly transportations alternatives. Other standalone electric and shared mobility markets such as e-scooters and bike are also expected to be supported by AI in terms of operation and management of fleet, as well as in prediction of maintenance requirements (Merlo et al., 2023).



Figure. 1 showing challenges of AI in mobility

Two more critical areas where AI needs to function efficiently in mobility include disaster and managing health facilities. Mobile clinics with auto-drive and drones can effectively transport patients or medicine, carry organs to the transplantation place, etc., which is urgent for saving time in case of emergencies. The following innovations not only transform the way health care is delivered but also reveal the connection between AI, mobility and others (Cen et al., 2024). This paper will endeavor to disseminate the information that similar to any other novel endeavor, AI mobility has its problems and the person can think of the specimens such as; inadequate regulation, adoption, and cybersecurity threats. Premium self-driving vehicles and smart automobiles be vulnerable to attack, the car's safety and confidentiality are in peril. All these gaps will only be responsive if policy makers, technologists and cybersecurity experts collaborate closely together. This special section examines current AI trends and how they are likely to shape the future of mobility: this is making it safer, more efficient and sustainable, as AI alters movement in a connected world (Desai & Desai, 2023).

The Role of Cybersecurity in AI-Driven Systems

Therefore, there is a great fear as artificial intelligence technologies emerge, and its relevance to operations such as healthcare and mobility is considered susceptible. It was already pointed out that AI systems rely on data and networks, thus, the larger the amount, the more vulnerable it becomes to cyber threats. The loss of cybersecurity is still an important problem because with newer technologies like AI, not only can the core formations of its capability be destroyed but also any data, user security protocols and overall trust in the AI systems (Vasani et al., 2023). All of this goes to show that cybersecurity must continue to appropriately implement its uses across industries including healthcare and mobility. In the context of the practical application, AI-engineered solutions are transforming the sphere of patient care by means of such tools as diagnostic equipment and treatment and health solutions for individual patients. However, as medical data is usually private, such systems become highly appealing to hackers in their turn. Causative attacks in a health records setting can be devastating, which is depicted by the very high ripper effect; the fruits of a successful attack encompass identity theft, alteration of data in record, manipulation of AI algorithms used in diagnosing patients and choosing treatment regimens (Ali & Mijwil, 2024). For example, a hacker can gain unauthorized access to a healthcare organization and modify the result in a diagnostic AI and end up providing dangerous diagnoses to the lives of people. It is therefore important for the safety of medical practice and the privacy of the patient that Health care related AI systems be protected. Several steps which may include data encryption, executive authentication and surveillance in real time are some of the steps that is being taken to eliminate any form of attack on healthcare AI systems (Gupta et al., 2023).

Also, in mobility AI technologies include self-driving car and smart traffic and transportation management and connectivity which can revolutionary's urban mobility. However these are combined or AI systems are greatly dependent on the data from GPS, sensors and clouds etc.

This makes it very easy for the hackers to do all forms of cybercrimes; hacking, data manipulation and even denial of service attack (Y. Yang et al., 2023). A specific AI car might also be some sort of victim in the hack attack or the operational systems of the car might also be captured. Consequently, protection and enhancement of cybersecurity of mobility solutions with the help of artificial intelligence is the necessary condition for safety and flawless operation of transport systems. However, recent developments in Information Technology have shifted the focus to the defense of the AI systems on which the conventional Information Technology systems are built (Alchi & Dodiya, 2023). Roughly, the current AI models and, particularly, the models based on machine learning algorithms have a weakness called adversarial attack, and an attacker can feed the model with specific input that the attacker wants the model to make wrong conclusions or decisions at. For example, adversarial attack has the ability to fool an AV AI to not observe a pedestrian or even misread a traffic sign. To avoid such a shocking incidences of such an attack of this nature, the AI developers are employing techniques such as the adversarial training in which an AI goes through several attack processes in the training process (Zhang et al., 2023).

With the growth of the use of AI systems and with the decision making authority of an organization transferring to the AI systems, accountability for cybersecurity becomes more important. Improvement of the problems concerned with the absence of both the ideal explanation and the rules of the regulators is vital in order to create appropriate AI ethical contract and make AI systematic really clear and to be responsible as the tool which has to gain public trust and cannot be used as the tool of manipulation (Zhang et al., 2023). Major stakeholders in AI systems cannot afford to work individually when it comes to minimizing cyber security threats. Moreso, it means the joys of potential uses of healthcare or mobility can be realized if everyone starts seeing cybersecurity as the process that can help to either enhance or mitigate the benefits of the new technology (Argaw et al., 2020).

Cybersecurity Risk Challenges in Healthcare, New Mobility

As the use of AI in health and mobility aspects expand, new cyber threats become apparent, which threatens everyone. These shifts towards connected, AI based systems have offered a number of opportunities across these industries. But at the same time it voices primary flaws that have to be solved to avoid misuse of the new perspectives the union offers. They become the focuses for developing countermeasures on the new threats as such to safeguard the efficiency of such developments. In healthcare, one of the most significant cybersecurity threats stem from the r[acomple:he increasing demand for adopting electronic records, networked medical devices as well as healthcare systems (Thomasian & Adashi, 2021). EHRs are now firmly embedded in practice and are resulting in improved access and coordination of patient's records. But EHRs are also very attractive to the hacker because he will get the chance to steal the data that is useful for identity theft or fraud. Also, health facilities are potentially vulnerable to ransom ware attacks in which attackers are likely to demand for money after locking data. Now that the current healthcare regulations show that most healthcare systems globally are incapable of

investing much on strong cybersecurity the risks of data violation and disruption of operations are very high (Kalid et al., 2018).

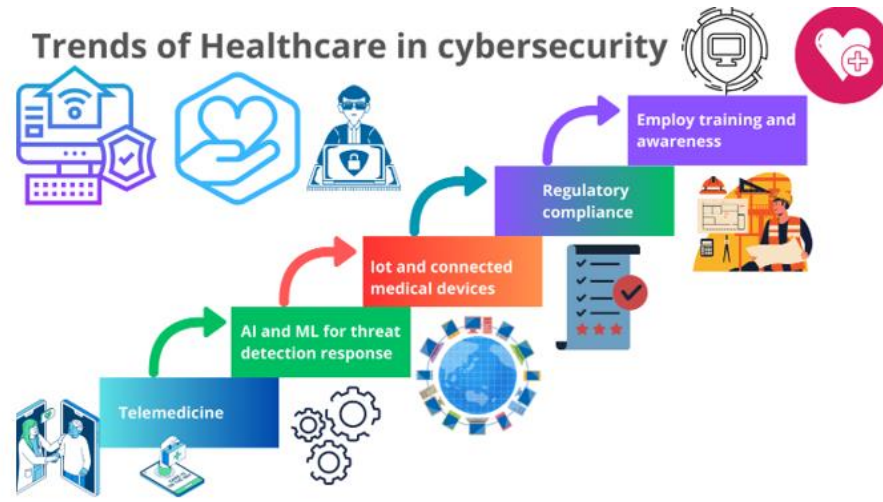


Figure 2. showing trends of healthcare in cybersecurity

IT infrastructure is in risk by new types of diagnostic and treatment instruments based on artificial intelligence, regarding cybersecurity in the healthcare industry. The increased adoption of such tools increases the concern for the AI systems—the circuit breakers, as it were, in these support structures are vulnerable to blowing, meaning Covid patients may be misdiagnosed, given incorrect treatment recommendations, and worst of all, be affected. For instance, a different attacks could make AI model to classify medical images to the wrong categories and hence cause high rates of misdiagnosis or false positives (Banos et al., 2014). Similarly in the mobility segment, artificial intelligence such as self-driving cars, intelligent traffic systems and transport infrastructure and networks expose the system to cybersecurity threats. Self-driving cars still become another sweet spot for hackers because they used the network of a set of sensors and communication system. In the case of an attack on an AV, the best results for the attackers were complete control of the car, changing the route, or leading to an accident. Besides, one can easily resemble that insufficient security in V2V and V2I networks can turn the same flow control into a way of manipulating traffic, interrupting transport means, or threatening public security. This often means an incident can go a lot more viral because these platforms are relatively open and heavy on the data (Shukur et al., 2023).

A new concern in mobility is that giant cities' artificial intelligence impact is exposed to risks, this which governs traffic, energy products, and services. An act of cyber terrorism, for instance if performed on the central control center of the city, may cause serious transportation hitches affecting several services or even lead to citizens' deaths. For example, an attacker could specifically change traffic signals to misprogram, or make them nonfunctional, or even install fake data into smart self-driving platforms to cause disruption of services (Saini et al., 2022). As societies adopt more of smart technologies, they would merge into a single network and because

this is under development, the security of such system must be well considered. Also, data created by AI systems in healthcare and mobility is a relatively new field and it has created a new threat to cybersecurity. The other issue is related to the protection of data: more and more specific user data is transferred through the networks and devices. Policies regulating governance have to ensure that the data is protected and that AI solutions operate in compliance with GDPR within Europe or HIPAA within the United States of America (Saini et al., 2022).

To counter the new threats, organizations have to use sophisticated security paradigms that are distributed across multiple levels. These measures cover everything from enhancing the encryption paradigms, getting secure techniques of communication, periodical security evaluation, and using of the AI based threat profiling techniques to recognize the threats in an organization in real time. However, to reduce the effects of adversarial attacks there is need to enhance models that can withstand adversarial attack, application of secure software engineering, and cooperation between healthcare, transport and cybersecurity experts. The use of artificial intelligence in the procurement of healthcare and mobility is to totally revolution the most vital sector of our lives with new possibilities of regularity. Regarding these issues, the stakeholders can be in a position to ascertain the secure as well as ethical usage of the newer technologies to protect sensitive information, enhance system reliability and gain approval from the public in regard to embracing the newer technologies (A. H. Khan et al., 2024).

The book *Information Technology Solutions to Cyber Security*

It remains a necessity and has arguably never been more important since as much as AI is transforming healthcare and mobility it also poses new threats to cyber security. In recent complex AI systems, based on data-sets and frequently quite selective algorithms new threats arise that must be shielded. As a result, many emerging new technology solutions that are being developed targets to counter the current cybersecurity threats. Of these innovations, these are not developed with the primary intention of stopping third parties from breaching the system and attacking it, but for the security of the methods and information that is used in developing these smart systems (M. Yang et al., 2023). More specifically, this paper recommends identifying and integrating artificial intelligence threat detection and prevention systems as one of the key technologies improving cybersecurity to AI systems. In traditional security the tools and mechanisms utilized are program oriented they function according to designated plan and signature based detection takes time to respond once a new variant of virus or threat comes up (Y. Khan et al., 2016). To generate and analyze vast sets of data, plenty of time is needed in the human system, while AI integrated applications can monitor and spot erratic behaviors that may look like a hint to a cyber-attack interface. For example, AI is being applied to enhance the speed of threat detection to help the current security initiatives that scan for the new types of attack when they emerge. With AI in risk management of hacker opportunities, organizations are able to enhance security on their AI enriched health and movement applications (Chen et al., 2023).

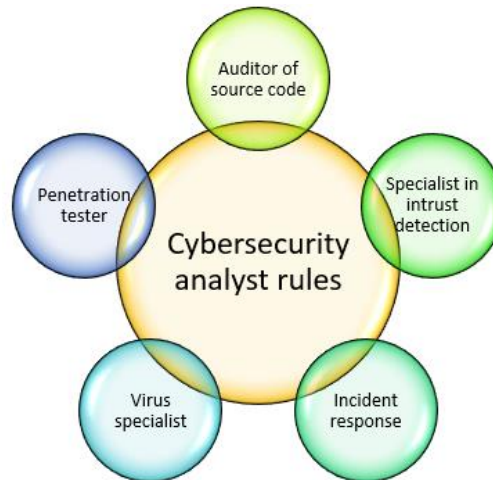


Figure. 3 showing cybersecurity analyst rules

Another new idea, also in the process of being incorporated to enhance AI security, is block chain technology as it starts being applied. Consequently they assert that the simplest use of block chain is to prevent or reduce incidents of data manipulation since it is distributed and its core feature is immutability. In healthcare it has been suggested that block chain for the protection of the data of the patents and in a way that their records and other personal data cannot be hacked or altered by other people. To this end, in mobility, block chain can help in the safeguard of exchange of data between self-driving vehicles, the traffic signals and other smart formations (Qayyum et al., 2023). By integrating block chain in generation of transparent record of data sharing, the stakeholders can enhance accountability of the AI systems with the two sectors. Another great technique of making the AI protection even stronger is the federated learning. In most conventional artificial learning approaches data tends to be centralized, therefore indicating that very sensitive details are compiled and archived. This of course raises big questions on the privacy and security of data; and these concerns are especially valid in the health care scenario where most data is sensitive. Federated learning, on the other hand, makes it possible to develop AI models through training at such decentralized devices while the data is still local. This means that the data remains where the data is generated so that the data cannot be exposed or breached. However, only the more recent findings of the models or new improvements of models as well are being revealed. This is especially useful in helping to improve the state of the art of care in the health sector, as it maintains the patient's privacy while at the same time training the artificial intelligence from large amounts of data within various settings. As for mobility it may allow enhancing the AI algorithms responsible for Autonomous Vehicle control decisions while considering the data backup & preservation (Flynn et al., 2023).

At the moment, two of the most discussed approaches in AI cybersecurity are, indeed, federated learning and differential privacy. A method of noise addition and removal within the differential privacy approach prevents the accentuation of the specific data records. Employing

such technique, data can be trained on AI models in organization without exposing the identity of the users or patients. Perhaps, especially in the use framework in healthcare where patient anonymity must be maintained and use framework in mobility where some private data of trip during commuting is sensitive (Arefin et al., 2017). However, encryption can still be considered one of the fundamental premises in cybersecurity in the case of the application of AI systems. New developed encryption approaches such as homomorphic encryption allows the AI models to process the encrypted data without decrypting them. This is especially important especially in areas such as the health sector because the information filed under a patient should not be disclosed. Homomorphic encryption promises that if data is ever leaked, it is as yet safe and used by AI systems to perform some computations on it without imparting it to others. This innovation helps to achieve safe ways of transferring data in order to work with other sites such as the hospitals, research facilities and many other health care facilities without revealing the identity of patients (Tröster, 2005).

AI is also being used in extending cybersecurity to protect AI models against adversarial attacks. In these kind of attacks, the attackers exploit their knowledge about the vulnerability of the design of an AI system to feed the latter with the wrong inputs for the purpose of getting the wrong outputs. To minimize these risks, researchers are developing processes as adversarial training, in which an AI is trained with probable harm scenarios (Mazhar et al., 2017). This will allow the system to learn how to classify adversarial examples before the latter can be defended. In addition, there is the model robustness testing that is used to identify the security vulnerabilities in the AI algorithms to enable the developers to apply fix on the vulnerabilities before the vices are exploited by the wrong minds. This has policy implications in another sense because the diseases that threaten cybersecurity as a result of applying AI in some major spheres, including healthcare and mobility ones, require the introduction of completely new facility (Qayyum et al., 2024). They also incorporate new technologies including Artificial Intelligence on threat detection, Block Chain, Federated Learning, Differential Privacy, Encryption, and Adversarial Robustness among others. Cybersecurity solution also has to evolve concurrently with AI to be the authentic one that will support the progressive technologies' real growth and productive application in healthcare and mobility fields. Thus for organizations to get the best potential it deserves those two fields are worth for organizations to continue to invest in and develop these innovations hence reducing the risks associated with the two fields (Mijwil et al., 2023).

Burden of Regulation: Has terrorism also triggered new regulatory standards to cybersecurity of artificial intelligence systems?

That is why, it is important to build a stable and effective legal regulation of cybersecurity when AI is introducing in the spheres of healthcare and mobility. These frameworks are needed to protect against appalling incorporation of AI technologies and to actively counter the opportunities that exist within systems-level connections. While more different kinds of AI tools

or applications are applied in different enterprises, data leakage, hack attacks, system or network failures' threats are more severe (Neprash et al., 2022). This is why it becomes most appropriate to establish regulatory benchmarks concerning these risks in order to effectively address them and ensure important data, patients and members of the public's confidence in service delivery. Now, let review the gaps and issues in healthcare industry that impelling the legal demands of AI cybersecurity to shift based on concerns current issues present in healthcare industry, AI deploying Medical Device, EHRs, and clinical decision-making. The modern codes and rules meaning Health Insurance Portability and Accountability Act existing in the United States of America is oriented on the protection of the patient's information (Wright et al., 2016). However, numerous AI implementations in health care require new rules meeting the new challenges that use of AI algorithms entails. For instance, the diagnostic or treatment recommendation AI models have to meet certain standards to uncompromisingly call for quintessential standards of non-ethnic bias and are categorically unsuitable for patient health risk. AI regulation for the healthcare subsector must also take into account processes of how operations are explained and how the regulator holds the operator to account, as well as the behavioral psychology of applying algorithmic systems to clinical decision-making (M. Khan et al., 2024).

That is why by regulating cybersecurity of AI in the sphere of healthcare together with the protection provided by the advanced privacy laws it is possible to ensure that AI systems meet the standards and respond properly to the privacy, protecting the data of the patients. [click here](#) The use of any AI tools that acts commercial on health data implies the regulation compliance with a great number of data protection norms and canons such as encryption, access management, and others. In addition, any regulatory authorities need to provide definite opinions regarding the direction of defending this data emerging from the AI systems in healthcare organizations, generating big data, hack able or otherwise (Lee, 2022). As with most industries, the regulation of part of the AI value chain is essential for the safe application of AI technologies in the mobility sector as their tools – Self-driving vehicles, intelligent roads, and connected transportation systems. According to the level of the development of emerging technologies in the automotive market, cybersecurity in self-driving automotive vehicles is one of the most complex problems as such automobiles consist of interconnected systems of sensors and communication platforms as well as artificial intelligence algorithms. Several academic programs in cybersecurity are required as self-driving cars will be on the road and constantly communicating with other cars and traffic infrastructure – these MAY BE vulnerable to cyber-attacks that endanger the lives of passengers and disrupt the functioning of cities and their transportation networks (Husnain & Saeed, 2024).

Therefore, the right authorities should develop cybersecurity standards for connected and autonomous vehicles (CAVs). These standards should therefore aim at providing preventive measures against the threats like: remote hacking, GPS spoofing and data manipulation amongst others. Further, it must be required for the manufacturers to maximize, and bi-safeguard the

higher levels of cybersecurity characterizing AV during their construction as well as operation. But the public policies needed to support and ensure that the information sharing between automobiles, roads, other entities, and automobiles and other systems are secure and are protected from invasions of the privacy rights of violation of the private data. Next, there is the use of Artificial Intelligence in traffic and energy in smart cities; and use of AI in Public service delivery is also another regulatory consideration (Rawat et al., 2022). These are measures that have to be undertaken to avoid utilization of any loophole within the various components of the whole smart city system by the cyber criminals; hence the regulation structure for smart cities has to incorporate certain specific rules concerning data protection, manner of communication in smart cities and risk management. Imperative to these frameworks is the shielding of the current and potential smart city environment from cyber security risks; therefore, engage cross-sectional multi-stakeholders, including government ministries, technology developers, and city planners (Husnain et al., n.d.).

In addition to Sector specific regulation, there is also a provision on international cooperation for cyber security matters connected with AI. Every country and every geographical area has its legislation in place regarding the protection of the data as well as cybersecurity, which finally does not give a chance to establish the particular list of norms regarding the safety of artificial intelligence at the international level. The GDPR in European Union and other regulations in correspondent countries are precedent for cybersecurity of AI based on the principles of data protection and privacy (Chernyshev et al., 2019). I found, nevertheless, that to counter threats that imply global participation one must call for international participation in the creation of predictable and easily enforceable rules for AI safeguard. This includes the establishment of principles, regulation and the application of best practice, layered security features and the demonstration that the AI technologies that underpin the solutions are applied in an open, ethical and secure, without prejudice to location. An example of Aval's international cooperation is an AI Cybersecurity Initiative that was launched by the Organization for Economic Co-operation and Development (OECD), the purpose of which is to ensure the AI technologies are used safely and securely in other countries (Shihab & AlTawy, 2023). This has to be present; because with the creation of such systems, the developers and users of such artificial intelligence based system will be forced to engage in banking related activities within stipulated ethical standards; there are always risks of hacking that would make these systems irrelevant.

In this regard, there is an adequate demand for regulating measures for cybersecurity of AI systems to minimize risks of artificial intelligence technologies Is linked to risks for the health care section and mobility CLU. These frameworks should present answers on issues to do with privacy, protection, transparency, and responsibility concerning the artificial intelligence technology for the safety, efficiency, and resourceful use of AI (Saeed et al., 2024). As AI technologies continue being adopted further and as they advance, it shall be important for the governments, other regulatory authorities, as well as the industries come up with kinds of cybersecurity regulations

that should cater for the dynamic, complex nature of AI structures. By so doing, it creates an environment that will ensure people are safe, one can build credibility as well as offer a way through which the enhancement of AI within various fields can be enhanced.

CONCLUSION

The research highlights the transformative potential of artificial intelligence (AI) in various sectors, including healthcare, mobility, and city management. The integration of AI has significantly enhanced efficiency and innovation, but it has also introduced critical cybersecurity challenges. Sensitive patient data, smart car systems, and connected urban environments face risks from malicious actors who may exploit vulnerabilities in these systems. This underscores the importance of robust preventive measures, such as Threat Intelligence, Blockchain technology, Federated Learning, and advanced Encryption methods. These cybersecurity solutions are critical for safeguarding AI systems, ensuring data integrity, and maintaining the trust required for the responsible use of AI across sectors.

The findings of this study contribute to a better understanding of the interplay between AI advancements and cybersecurity, providing a framework for future research and innovation. In the health sector, this research emphasizes the need for security standards that protect sensitive patient information, while in mobility, it underscores the importance of regulations to secure autonomous vehicles, connected infrastructure, and smart cities. Moving forward, this study advocates for collaborative efforts to refine cybersecurity measures in tandem with the evolution of AI technologies. By addressing these challenges, AI can continue to transform industries responsibly, enriching society and unlocking its potential as a revolutionary tool for progress.

REFERENCES

- Alchi, A. N., & Dodiya, K. R. (2023). Demystifying ransomware: classification, mechanism and anatomy. In *Perspectives on Ethical Hacking and Penetration Testing* (pp. 171–192). IGI Global.
- Ali, G., & Mijwil, M. M. (2024). Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles. *Mesopotamian Journal of CyberSecurity*, 4(2), 20–62.
- Arefin, M. T., Ali, M. H., & Haque, A. K. M. F. (2017). Wireless body area network: An overview and various applications. *Journal of Computer and Communications*, 5(07), 53.
- Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O’Leary, C., & Eshaya-Chauvin, B. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20, 1–10.
- Banos, O., Villalonga, C., Damas, M., Gloesekoetter, P., Pomares, H., & Rojas, I. (2014). Physiodroid: Combining wearable health sensors and mobile devices for a ubiquitous, continuous, and personal monitoring. *The Scientific World Journal*, 2014(1), 490824.

- Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. *Computer Networks*, 239, 110138.
- Chen, J.-J., Husnain, A., & Cheng, W.-W. (2023). Exploring the Trade-Off Between Performance and Cost in Facial Recognition: Deep Learning Versus Traditional Computer Vision. *Proceedings of SAI Intelligent Systems Conference*, 400–412.
- Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems*, 43, 1–12.
- Chirra, D. R. (2022). Collaborative AI and Blockchain Models for Enhancing Data Privacy in IoMT Networks. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 13(1), 482–504.
- Damaraju, A. (2022). Social Media Cybersecurity: Protecting Personal and Business Information. *International Journal of Advanced Engineering Technologies and Innovations*, 1(2), 50–69.
- Desai, A., & Desai, M. (2023). A review of the state of cybersecurity in the healthcare industry and propose security controls. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, 2023, 82–84.
- Flynn, C. D., Chang, D., Mahmud, A., Yousefi, H., Das, J., Riordan, K. T., Sargent, E. H., & Kelley, S. O. (2023). Biomolecular sensors for advanced physiological monitoring. *Nature Reviews Bioengineering*, 1(8), 560–575.
- Gadde, H. (2022). AI in Dynamic Data Sharding for Optimized Performance in Large Databases. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 13(1), 413–440.
- Goriparthi, R. G. (2023). Federated Learning Models for Privacy-Preserving AI in Distributed Healthcare Systems. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 14(1), 650–673.
- Goriparthi, Rithin Gopal. (2023). Leveraging AI for Energy Efficiency in Cloud and Edge Computing Infrastructures. *International Journal of Advanced Engineering Technologies and Innovations*, 1(01), 494–517.
- Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*.
- Husnain, A., Alomari, G., & Saeed, A. (n.d.). *AI-Driven Integrated Hardware and Software Solution for EEG-Based Detection of Depression and Anxiety*.
- Husnain, A., & Saeed, A. (2024). AI-enhanced depression detection and therapy: Analyzing the VPSYC system. *IRE Journals*, 8(2), 162–168.
- Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1, 100016.
- Kalid, N., Zaidan, A. A., Zaidan, B. B., Salman, O. H., Hashim, M., & Muzammil, H. (2018). Based real time remote health monitoring systems: A review on patients prioritization and related "big data" using body sensors information and communication technology. *Journal of Medical Systems*, 42, 1–30.
- Khan, A. H., Zainab, H., Khan, R., & Hussain, H. K. (2024). Deep Learning in the Diagnosis and Management of Arrhythmias. *Journal of Social Research*, 4(1), 50–66.
- Khan, M., Shiwlani, A., Qayyum, M. U., Sherani, A. M. K., & Hussain, H. K. (2024). Revolutionizing

- Healthcare with AI: Innovative Strategies in Cancer Medicine. *International Journal of Multidisciplinary Sciences and Arts*, 3(1), 316–324.
- Khan, Y., Ostfeld, A. E., Lochner, C. M., Pierre, A., & Arias, A. C. (2016). Monitoring of vital signs with flexible and wearable medical devices. *Advanced Materials*, 28(22), 4373–4395.
- Lee, I. (2022). Analysis of insider threats in the healthcare industry: A text mining approach. *Information*, 13(9), 404.
- Mazhar, F., Khan, M. G., & Sällberg, B. (2017). Precise indoor positioning using UWB: A review of methods, algorithms and implementations. *Wireless Personal Communications*, 97(3), 4467–4491.
- Merlo, V., Pio, G., Giusto, F., & Bilancia, M. (2023). On the exploitation of the blockchain technology in the healthcare sector: A systematic review. *Expert Systems with Applications*, 213, 118897.
- Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the top five evolving threats in cybersecurity: an in-depth overview. *Mesopotamian Journal of Cybersecurity*, 2023, 57–63.
- Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, 3(12), e224873–e224873.
- Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, 9(4), 571–588.
- Qayyum, M. U., Sherani, A. M. K., Khan, M., & Hussain, H. K. (2023). Revolutionizing Healthcare: The Transformative Impact of Artificial Intelligence in Medicine. *BIN: Bulletin Of Informatics*, 1(2), 71–83.
- Qayyum, M. U., Sherani, A. M. K., Khan, M., Shiwani, A., & Hussain, H. K. (2024). Using AI in Healthcare to Manage Vaccines Effectively. *JURIHUM: Jurnal Inovasi Dan Humaniora*, 1(6), 841–854.
- Rawat, R., Mahor, V., Garg, B., Chouhan, M., Pachlasiya, K., & Telang, S. (2022). Modeling of cyber threat analysis and vulnerability in IoT-based healthcare systems during COVID. In *Lessons from COVID-19* (pp. 405–425). Elsevier.
- Reddy, V. M., & Nalla, L. N. (n.d.). *Implementing Graph Databases to Improve Recommendation Systems in E-commerce*.
- Saeed, A., Husnain, A., Zahoor, A., & Gondal, R. M. (2024). A comparative study of cat swarm algorithm for graph coloring problem: Convergence analysis and performance evaluation. *International Journal of Innovative Research in Computer Science and Technology (IJIRCST)*, 12(4), 1–9.
- Saini, G., Budhwar, V., & Choudhary, M. (2022). Review on people's trust on home use medical devices during COVID-19 pandemic in India. *Health and Technology*, 12(2), 527–546.
- Shihab, S., & AlTawy, R. (2023). Lightweight authentication scheme for healthcare with robustness to desynchronization attacks. *IEEE Internet of Things Journal*, 10(20), 18140–18153.
- Shukur, B. S., Yaacob, N. M., & Doheir, M. (2023). Diabetes at a Glance: Assessing AI Strategies for Early Diabetes Detection and Intervention. *Mesopotamian Journal of Artificial*

Intelligence in Healthcare, 2023, 85–89.

Syed, F. M., & ES, F. K. (2023). The Impact of AI on IAM Audits in Healthcare. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14*(1), 397–420.

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology, 10*(3), 100549.

Tröster, G. (2005). The agenda of wearable healthcare. *Yearbook of Medical Informatics, 14*(01), 125–138.

Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion. *Electronics, 12*(20), 4299.

Vijayakumar, G. N. S., Sharma, V., Pradeep, S., Pratheeba, C., Balakrishnan, T. S., & Jat, R. (2024). Machine Learning Techniques for Predictive Maintenance in Industrial IoT Systems. *2024 International Conference on Science Technology Engineering and Management (ICSTEM)*, 1–5.

Wright, A., Aaron, S., & Bates, D. W. (2016). The big phish: cyberattacks against US healthcare systems. *Journal of General Internal Medicine, 31*, 1115–1118.

Yang, M., Wang, L., Lu, H., & Dong, Q. (2023). Advances in MXene-based electrochemical (bio) sensors for neurotransmitter detection. *Micromachines, 14*(5), 1088.

Yang, Y., Lin, Y., Li, Z., Zhao, L., Yao, M., Lai, Y., & Li, P. (2023). GooseBt: A programmable malware detection framework based on process, file, registry, and COM monitoring. *Computer Communications, 204*, 24–32.

Zhang, W., Chen, Z., Chen, D., Li, J., & Pan, Y. (2023). DID-IDS: A Novel Diffusion-based Imbalanced Data Intrusion Detection System. *2023 IEEE 11th International Conference on Information, Communication and Networks (ICICN)*, 364–369.

Copyright holder:

Ahmad Bacha, Murad Khan, Abdul Mannan Khan Sherani, Heta Hemang Shah, Noman Abid, Nahid Neoaz, Mohammad Hasan Amin (2025)

First publication right:

Asian Journal of Engineering, Social and Health (AJESH)

This article is licensed under:

