Volume 7, Issue 1, 2023

Eigenpub Review of Science and Technology
peer-reviewed journal dedicated to showcasing cutting-edge research and innovation in the fields of science and technology.
https://studies.eigenpub.com/index.php/erst

Cybersecurity and Privacy Issues in the Internet of Medical Things (IoMT)

Ahmed Yazid

Computer science, University of Tébessa

ABSTRACT

The Internet of Medical Things (IoMT) has the potential to revolutionize the healthcare industry by providing real-time health information, remote monitoring, and improved treatment options. With this increased connectivity comes an increased risk of cybersecurity and privacy issues. This research study aimed to identify and analyze the key cybersecurity and privacy issues associated with the IoMT and provide recommendations for healthcare providers and device manufacturers to address these issues. Data breaches were identified as a significant cybersecurity risk associated with the IoMT. The IoMT collects and transmits sensitive medical data, such as patient health records and medical device data. This data is highly valuable to hackers and can be used for identity theft, insurance fraud, and other malicious activities. The study found that implementing strong authentication and access controls, using encryption to protect data in transit and at rest, regularly updating and patching devices, and training employees on cybersecurity best practices can help mitigate this risk. The research revealed vulnerable devices as a significant cybersecurity risk associated with the IoMT. Many medical devices are not designed with security in mind, which makes them vulnerable to cyberattacks. Hackers can exploit vulnerabilities in these devices to gain access to sensitive data or to take control of the device. The study found that healthcare providers and device manufacturers must prioritize cybersecurity in the design, implementation, and maintenance of IoMT systems. This includes regularly updating and patching devices and implementing security protocols to protect against known vulnerabilities. The lack of encryption was identified as another significant cybersecurity risk associated with the IoMT. Data transmitted over the IoMT may not always be encrypted, leaving it vulnerable to interception by hackers. The study found that implementing encryption technologies such as secure sockets layer (SSL) and transport layer security (TLS) can help protect data in transit. Insider threats were identified as a significant cybersecurity risk associated with the IoMT. Healthcare employees and other authorized users may accidentally or intentionally leak sensitive data, either through negligence or malicious intent. The study found that implementing role-based access control, conducting regular security awareness training, and implementing auditing and monitoring tools can help mitigate this risk. IoMT must comply with various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). The study found that compliance with these regulations can be challenging, and non-compliance can result in fines and legal penalties. Healthcare providers and device manufacturers must prioritize regulatory compliance in the design, implementation, and maintenance of IoMT systems.

Keywords: *Cybersecurity, Privacy, Internet of Medical Things, IoMT, Data breaches*

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized various industries, including healthcare. The Internet of Medical Things (IoMT) is a subset of the IoT that includes medical devices, wearable sensors, and other equipment that are connected to the internet for data collection and analysis. The IoMT has the potential to transform the healthcare industry by providing real-time health information, remote monitoring, and improved treatment options.

However, with the increased connectivity, the IoMT also poses significant cybersecurity and privacy risks.

The IoMT enables healthcare providers to collect vast amounts of data, including patient health records, medical device data, and other sensitive information. This data is highly valuable to hackers and can be used for identity theft, insurance fraud, and other malicious activities. In addition, many medical devices are not designed with security in mind, making them vulnerable to cyberattacks. As a result, cybersecurity and privacy issues have become a significant concern for the IoMT.This paper explores the key cybersecurity and privacy issues associated with the IoMT and their potential impact on the healthcare industry.

Data breaches are one of the biggest cybersecurity concerns connected to the IoMT. The IoMT collects and transmits sensitive medical data, including patient health records and medical device data. This data is highly valuable to hackers, who can use it for identity theft, insurance fraud, and other malicious activities. In addition, data breaches can have a significant impact on patients' privacy, as their sensitive medical information can be exposed to unauthorized individuals.The healthcare industry has already experienced several high-profile data breaches, which have affected millions of patients. For example, in 2015, Anthem, one of the largest health insurers in the United States, experienced a data breach that exposed the personal information of approximately 80 million individuals. Similarly, in 2017, the WannaCry ransomware attack affected several hospitals in the United Kingdom, causing significant disruption to patient care.

Many medical devices, such as pacemakers and insulin pumps, are not designed with security in mind, making them vulnerable to cyberattacks. Hackers can exploit vulnerabilities in these devices to gain access to sensitive data or to take control of the device. For example, a hacker could remotely control a pacemaker and potentially cause harm to the patient.Many medical devices have a long lifespan, which means that they may be in use for several years without being updated or replaced. This increases the risk of vulnerabilities remaining undiscovered and unpatched, making the devices even more vulnerable to cyberattacks.

Data transmitted over the IoMT may not always be encrypted, leaving it vulnerable to interception by hackers. Encryption is a critical security measure that protects sensitive data from unauthorized access. However, some IoMT devices may not use encryption or may use weak encryption, making them vulnerable to cyberattacks. Some IoMT devices may transmit data over unsecured networks, such as public Wi-Fi networks. This further increases the risk of data interception by hackers.

Healthcare employees and other authorized users may accidentally or intentionally leak sensitive data, either through negligence or malicious intent. For example, an employee may inadvertently send sensitive data to the wrong recipient or leave a device containing sensitive data in a public place. Alternatively, an employee may intentionally leak sensitive data for personal gain or to harm the organization.

The IoMT must comply with various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).

Compliance with these regulations can be challenging, as they impose strict requirements for data protection and privacy.

HIPAA is a US federal law that sets national standards for protecting the privacy and security of individuals' medical information. The law applies to covered entities, such as healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates. HIPAA requires covered entities to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of individuals' medical information.GDPR is a European Union regulation that sets strict requirements for data protection and privacy. The regulation applies to organizations that process personal data of EU citizens, regardless of the organization's location. GDPR requires organizations to obtain individuals' consent before collecting their personal data, to implement technical and organizational measures to protect personal data, and to notify individuals and authorities of data breaches.

Compliance with these regulations is essential to protect patients' privacy and to avoid legal penalties. Compliance can be challenging, particularly for smaller healthcare organizations that may lack the resources to implement robust security measures and to train their staff on data protection and privacy requirements.

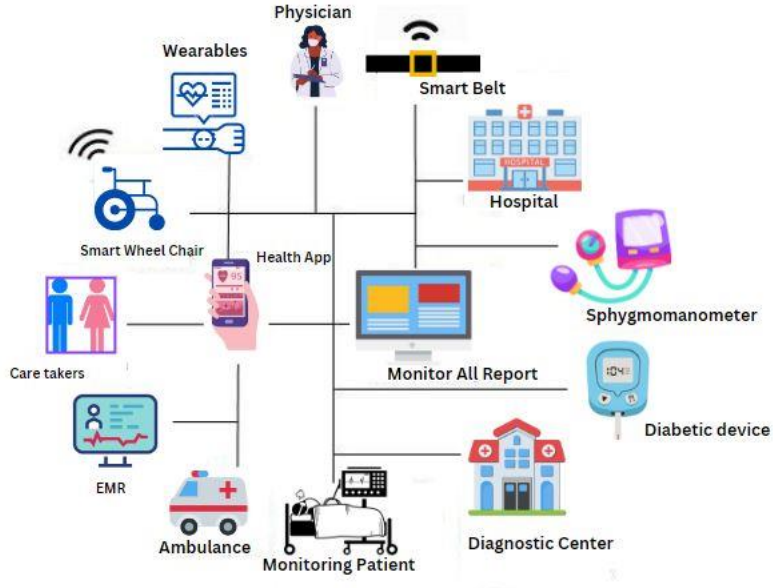

Figure 1 . Internet of Medical Things

II. Issues

Data breaches:

The Internet of Medical Things (IoMT) is an innovative technology that is transforming the healthcare industry by connecting medical devices and sensors to the internet. While the IoMT has the potential to improve patient outcomes and reduce costs, it also poses

significant security risks. One of the most significant risks associated with the IoMT is data breaches. The IoMT collects and transmits sensitive medical data, including patient health records and medical device data, which is highly valuable to hackers. With access to this information, hackers can engage in a range of malicious activities, including identity theft, insurance fraud, and other forms of cybercrime.

Data breaches in the healthcare industry have become increasingly common in recent years, with cybercriminals targeting vulnerable healthcare systems and exploiting security weaknesses. The rise of the IoMT has only heightened these risks, as more and more medical devices become connected to the internet, providing a larger attack surface for hackers to exploit. Given the sensitive nature of the data collected by the IoMT, the consequences of a data breach can be severe. Patient health records contain personal and medical information that can be used to steal identities, commit insurance fraud, and even blackmail patients. Medical device data can also be manipulated by hackers, potentially leading to serious patient harm. Thus, it is essential to address the security risks associated with the IoMT to protect patient privacy and safety.

In response to the growing threat of data breaches in the IoMT, healthcare organizations and technology providers are taking steps to improve security. These measures include implementing advanced encryption techniques, using multi-factor authentication, and conducting regular security audits to identify and address vulnerabilities. Additionally, regulatory bodies are developing guidelines and standards for the secure deployment and use of IoMT devices. However, given the complexity and diversity of IoMT systems, securing the IoMT remains a significant challenge. It requires a multi-layered approach that involves collaboration between healthcare providers, technology vendors, regulatory bodies, and cybersecurity experts. Only by working together can we ensure that the IoMT realizes its potential while minimizing the risks of data breaches and other security threats.

Vulnerable devices:

The Internet of Medical Things (IoMT) has transformed the healthcare industry by enabling real-time monitoring of patients and providing healthcare providers with unprecedented access to medical data. However, the widespread adoption of IoMT has also led to an increase in cybersecurity risks, particularly concerning vulnerable devices. Many medical devices are not designed with security in mind, which makes them vulnerable to cyberattacks.

Hackers can exploit vulnerabilities in these devices to gain access to sensitive data or to take control of the device. This can have serious consequences for patients, as cyberattacks on medical devices can lead to incorrect diagnoses, delayed treatments, or even life-threatening situations. Additionally, cyberattacks on medical devices can also disrupt hospital operations, leading to cancelled surgeries, delayed treatments, and increased costs for healthcare providers.

The vulnerability of medical devices is a significant concern for healthcare providers, as the sheer number of devices in use can make it challenging to ensure that all devices are up-to-date and secure. However, healthcare providers must take proactive steps to secure their devices, such as implementing encryption and authentication protocols, applying

software patches and updates regularly, and conducting regular vulnerability assessments. Healthcare providers must also ensure that their staff receives regular security awareness training to educate them on the importance of device security and to recognize potential cyber threats. One of the challenges in securing medical devices is that many of them have long lifecycles, which means that they may be in use for years or even decades. This can make it difficult to keep up with the latest security standards and updates, particularly as new vulnerabilities and threats emerge. Healthcare providers must work with device manufacturers to ensure that devices are designed with security in mind and that manufacturers provide regular updates and support throughout the device's lifecycle.

As the use of IoMT continues to expand, healthcare providers must be prepared for the challenges of securing an ever-growing network of connected medical devices. This includes ensuring that all devices are properly configured, that access controls are in place, and that data transmitted between devices is encrypted. Additionally, healthcare providers must develop incident response plans in case of a cyberattack and conduct regular simulations to ensure that staff members are prepared to respond quickly and effectively.The vulnerability of medical devices highlights the importance of regulatory compliance, including compliance with standards such as HIPAA and GDPR. Healthcare providers must ensure that their devices and networks meet the requirements of these standards, which include requirements for data protection and incident response planning. Compliance with these standards is not only essential for protecting patient data but also for avoiding costly legal and financial penalties in the event of a data breach.

Vulnerable devices are a significant cybersecurity risk to the IoMT. Healthcare providers must take proactive steps to secure their devices, including implementing encryption and authentication protocols, applying software patches and updates regularly, and working with device manufacturers to ensure devices are designed with security in mind. As the use of IoMT continues to expand, healthcare providers must be prepared for the challenges of securing an ever-growing network of connected medical devices and ensuring regulatory compliance.

Lack of encryption:

The Internet of Medical Things (IoMT) has the potential to revolutionize healthcare by enabling doctors to remotely monitor patients' health, streamline operations, and improve patient outcomes. The lack of encryption in IoMT devices is a significant security risk that cannot be ignored. Data transmitted over the IoMT may not always be encrypted, leaving it vulnerable to interception by hackers. This can lead to the theft of sensitive patient data, which can have serious consequences for patients and healthcare providers.

Encryption is a critical security feature that protects data from unauthorized access during transmission. Without encryption, data can be intercepted and read by anyone with access to the network. In the case of IoMT devices, this means that sensitive patient data, such as medical records, test results, and even real-time health data, can be intercepted by hackers. This data can be used for identity theft, financial fraud, or even blackmail. Furthermore, the lack of encryption can also compromise the integrity of the data, allowing hackers to modify or delete it without detection.

The consequences of the lack of encryption in IoMT devices can be severe. For example, if a hacker gains access to a patient's medical records, they can use this information to impersonate the patient, obtain prescriptions for controlled substances, or commit other forms of fraud. If a hacker intercepts real-time health data, they can manipulate this data to cause false alarms or prevent legitimate alarms from being triggered, leading to a delayed response from healthcare providers. Therefore, it is critical that manufacturers of IoMT devices prioritize encryption in their design and development processes to ensure the security and privacy of patient data.

Insider threats:

Among the most important cybersecurity risks associated with the Internet of Medical Things (IoMT) is insider threats. Healthcare employees and other authorized users may accidentally or intentionally leak sensitive data, either through negligence or malicious intent. The consequences of such incidents can be devastating, both for the patients and for the healthcare providers. Inadvertent disclosures of sensitive medical data can lead to a loss of patient trust, which can be difficult to regain. Malicious leaks, on the other hand, can result in significant legal and financial penalties, as well as damage to the reputation of the healthcare provider.

Healthcare organizations must implement robust measures to prevent insider threats and protect sensitive medical data. This includes implementing role-based access control to restrict access to sensitive data only to authorized personnel. Healthcare employees must receive regular security awareness training to educate them on the importance of protecting sensitive medical data and the potential consequences of a data breach. Additionally, healthcare providers must implement auditing and monitoring tools to detect and prevent unauthorized access to sensitive data.

Preventing insider threats is particularly challenging in healthcare organizations, as employees must balance the need to provide patients with quality care with the need to protect their privacy. This can sometimes lead to a culture where employees prioritize patient care over data security, which can result in inadvertent disclosures of sensitive data. Healthcare organizations must work to create a culture that prioritizes both patient care and data security, where employees understand the importance of protecting sensitive data and are empowered to report any suspicious activity.

Insider threats pose a significant cybersecurity risk to the IoMT. Healthcare organizations must implement robust measures to prevent insider threats and protect sensitive medical data. This includes implementing role-based access control, providing regular security awareness training, and implementing auditing and monitoring tools. Creating a culture that prioritizes both patient care and data security can help prevent inadvertent disclosures of sensitive data and reduce the risk of insider threats. The healthcare industry must work together to address this critical cybersecurity issue and protect patient privacy.

Regulatory compliance:

The Internet of Medical Things (IoMT) has the potential to transform healthcare by enabling remote patient monitoring, improving patient outcomes, and streamlining operations.The IoMT must comply with various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), to ensure the privacy and security of patient data. Compliance with these regulations can be challenging, and non-compliance can result in fines and legal penalties, which can be costly and damaging for healthcare providers.

HIPAA is a federal law that requires healthcare providers to protect the privacy and security of patients' personal health information. This includes any information that can be used to identify a patient, such as their name, address, or medical records. Failure to comply with HIPAA can result in fines of up to $50,000 per violation, with a maximum penalty of $1.5 million per year for each violation. Similarly, the GDPR is a European Union regulation that requires organizations to protect the personal data of EU citizens. Failure to comply with the GDPR can result in fines of up to 4% of the organization's global revenue or €20 million, whichever is greater.Compliance with these regulations can be challenging for healthcare providers, particularly those that are new to the IoMT. The IoMT involves the collection, storage, and transmission of large amounts of sensitive patient data, which can be difficult to manage and secure. To comply with these regulations, healthcare providers must implement a range of security measures, such as encryption, access controls, and auditing, to protect patient data from unauthorized access or disclosure. They must also ensure that their employees are trained in HIPAA and GDPR compliance and that they have policies and procedures in place to address potential breaches of patient data.

The financial and legal penalties of non-compliance, healthcare providers can also suffer reputational damage if they fail to comply with HIPAA or GDPR. Patients trust healthcare providers to protect their sensitive personal health information, and any breach of this trust can have serious consequences for the provider's reputation. Patients may be less likely to seek treatment from a provider that has suffered a data breach, which can lead to a loss of business and revenue. Therefore, it is critical that healthcare providers prioritize compliance with HIPAA and GDPR to ensure the privacy and security of patient data and maintain the trust of their patients.

Lack of user awareness:

The lack of user awareness is a significant concern in the context of the IoMT. Many patients may not be familiar with the technology or the potential risks associated with its use. This lack of awareness can lead to a range of issues, from patients inadvertently sharing sensitive information to falling victim to phishing scams or other cyber attacks.

The rapid pace of technological change can exacerbate this problem, as patients may struggle to keep up with the latest developments in IoMT technology and the associated cybersecurity risks. This can create a dangerous gap between patients' understanding of the technology and the actual risks involved. Patients may not know how to protect themselves from potential threats. This can be due to a lack of education on best practices for cybersecurity, such as using strong passwords, avoiding public Wi-Fi networks, and regularly updating software. Furthermore, patients may not know how to recognize and respond to potential threats, such as suspicious emails or messages.The consequences of

this lack of awareness can be significant. Patients may unwittingly share sensitive medical information with third parties, potentially leading to identity theft or other malicious activity. Additionally, patients may inadvertently expose themselves to cyber attacks or other security breaches, compromising the confidentiality and integrity of their personal health information.

Addressing the lack of user awareness will require a multi-pronged approach. This may include education and outreach efforts aimed at patients, healthcare providers, and other stakeholders in the healthcare industry. In addition, medical device manufacturers must take a more proactive role in designing devices that are easy to use and secure by default, rather than relying on patients to take complex and error-prone security measures.

III. CONCLUSION

The benefits of the IoMT are many and include improved patient outcomes, reduced costs, and increased access to care. With real-time health information, doctors can make more informed decisions and quickly adjust treatment plans as necessary. Remote monitoring allows patients to receive care from the comfort of their own homes, reducing the need for hospital stays and expensive medical procedures. Additionally, the IoMT can provide valuable insights into patient behavior, allowing healthcare providers to better understand and prevent diseases.Despite these benefits, it is important to recognize that the risks associated with the IoMT are significant. Medical devices are particularly vulnerable to cyberattacks, as they often lack the robust security measures that are typically used in other industries. Hackers can exploit vulnerabilities in these devices to gain access to sensitive data or to take control of the device, potentially causing harm to the patient. Additionally, the lack of encryption in data transmitted over the IoMT is a significant concern, as it can allow hackers to intercept and steal sensitive information.

Insider threats are also a significant risk associated with the IoMT. Healthcare employees and other authorized users may accidentally or intentionally leak sensitive data, either through negligence or malicious intent. This can lead to significant harm to patients and damage to the reputation of healthcare providers.Regulatory compliance is another challenge for the IoMT, as it must comply with various regulations such as HIPAA and GDPR. Compliance can be complex and difficult to achieve, particularly in the rapidly evolving landscape of healthcare technology. Non-compliance can result in significant fines and legal penalties, which can be particularly damaging to smaller healthcare providers.

To address these risks, it is essential to prioritize cybersecurity and privacy in the development and implementation of IoMT technologies. This can be achieved through increased awareness and education for healthcare providers and patients, as well as stronger security measures and regulations. Additionally, it is important to ensure that medical devices are designed with security in mind from the outset, rather than being retrofitted with security measures after the fact.

The IoMT has the potential to transform healthcare, but it is essential to address the significant cybersecurity and privacy risks associated with this technology. By prioritizing security and privacy in the development and implementation of IoMT technologies, we can

ensure that the benefits of this technology are realized while minimizing its potential risks. With strong security measures and regulations in place, the IoMT can provide valuable insights into patient behavior, improve treatment outcomes, and ultimately, save lives.

REFERENCES

1. Nkomo, D. & Brown, R. for the Internet of Medical Things. *and Clinical Trial: Securing Patient Data* (2019).
2. Karmakar, K. K., Varadharajan, V., Tupakula, U., Nepal, S. & Thapa, C. Towards a Security Enhanced Virtualised Network Infrastructure for Internet of Medical Things (IoMT). in *2020 6th IEEE Conference on Network Softwarization (NetSoft)* 257–261 (ieeexplore.ieee.org, 2020). doi:10.1109/NetSoft48620.2020.9165387.
3. Almogren, A., Mohiuddin, I., Din, I. U., Almajed, H. & Guizani, N. FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things. *IEEE Internet of Things Journal* **8**, 4485–4497 (2021).
4. Mawgoud, A. A., Karadawy, A. I. & Tawfik, B. S. A Secure Authentication Technique in Internet of Medical Things through Machine Learning. *arXiv [cs.CR]* (2019).
5. Uyyala, P. Secure Channel Free Certificate-Based Searchable Encryption Withstanding Outside and Inside Keyword Guessing Attacks. *The International journal of analytical and experimental modal analysis* **13**, 2467–2474 (2021).
6. Basatneh, R., Najafi, B. & Armstrong, D. G. Health sensors, smart home devices, and the Internet of medical things: An opportunity for dramatic improvement in care for the lower extremity complications of diabetes. *J. Diabetes Sci. Technol.* **12**, 577–586 (2018).
7. Yaacoub, J.-P. A. *et al.* Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **105**, 581–606 (2020).
8. Kosuru, V. S. R. & Venkitaraman, A. K. CONCEPTUAL DESIGN PHASE OF FMEA PROCESS FOR AUTOMOTIVE ELECTRONIC CONTROL UNITS. *International*

Research Journal of Modernization in Engineering Technology and Science **4**, 1474–1480 (2022).

9. Alsubaei, F., Abuhussein, A. & Shiva, S. Ontology-Based Security Recommendation for the Internet of Medical Things. *IEEE Access* **7**, 48948–48960 (2019).
10. Attaran, M. The internet of things: Limitless opportunities for business and society. *Journal of Strategic Innovation and Sustainability Vol* **12**, 11 (2017).
11. Wang, X., Wang, L., Li, Y. & Gai, K. Privacy-Aware Efficient Fine-Grained Data Access Control in Internet of Medical Things Based Fog Computing. *IEEE Access* **6**, 47657–47665 (2018).
12. Uyyala, P. Delegated Authorization Framework for EHR Services using Attribute Based Encryption. *The International journal of analytical and experimental modal analysis* **13**, 2447–2451 (2021).
13. Kosuru, V. S. R. & Venkitaraman, A. K. Advancements and challenges in achieving fully autonomous self-driving vehicles. *World Journal of Advanced Research and Reviews* **18**, 161–167 (2023).
14. Jackson, G. W., Jr & Rahman, S. Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related To The Medical Internet Of Things (MIoT). *arXiv [cs.CY]* (2019).
15. Alsubaei, F., Abuhussein, A., Shandilya, V. & Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things* **8**, 100123 (2019).
16. Venkitaraman, A. K. & Kosuru, V. S. R. Hybrid deep learning mechanism for charging control and management of Electric Vehicles. *European Journal of Electrical Engineering and Computer Science* **7**, 38–46 (2023).

17. Coburn, K. R. THE INTERNET OF MEDICAL THINGS. *Scitech Lawyer* **4**, 18–20 (2016).

18. Uyyala, P. SECURE CRYPTO-BIOMETRIC SYSTEM FOR CLOUD COMPUTING. *Journal of interdisciplinary cycle research* **14**, 2344–2352 (2022).

19. Yanambaka, V. P., Mohanty, S. P., Kougianos, E. & Puthal, D. PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things. *IEEE Trans. Consum. Electron.* **65**, 388–397 (2019).

20. Venkitaraman, A. K. & Kosuru, V. S. R. A review on autonomous electric vehicle communication networks-progress, methods and challenges. *World J. Adv. Res. Rev.* **16**, 013–024 (2022).

21. Venkitaraman, A. K. & Kosuru, V. S. R. Resilence of Autosar-Complaint Spi Driver Communication as Applied to Automotive Embedded Systems. *EJECE* **7**, 44–47 (2023).

22. Nkomo, D. & Brown, R. Hybrid cybersecurity framework for the Internet of medical things (IOMT). in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* 212–212 (IEEE, 2019).

23. Kosuru, V. S. R. & Venkitaraman, A. K. Preventing the False Negatives of Vehicle Object Detection in Autonomous Driving Control Using Clear Object Filter Technique. in *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* 1–6 (ieeexplore.ieee.org, 2022). doi:10.1109/ICSTCEE56972.2022.10100170.

24. Sun, Y., Lo, F. P.-W. & Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **7**, 183339–183355 (2019).

25. Anandarajan, M. & Malik, S. Protecting the Internet of medical things: A situational crime-prevention approach. *Cogent Medicine* **5**, 1513349 (2018).

26. Ashwin, K. V., Kosuru, V. S. R., Sridhar, S. & Rajesh, P. A Passive Islanding Detection Technique Based on Susceptible Power Indices with Zero Non-Detection Zone Using a Hybrid Technique. *Int J Intell Syst Appl Eng* **11**, 635–647 (2023).

27. Putta, S. R., Abuhussein, A., Alsubaei, F., Shiva, S. & Atiewi, S. Security Benchmarks for Wearable Medical Things: Stakeholders-Centric Approach. in *Fourth International Congress on Information and Communication Technology* 405–418 (Springer Singapore, 2020). doi:10.1007/978-981-32-9343-4_32.

28. Stein, W. O. B. & Boswell, M. The Current Ethical and Regulatory Status of the Internet of Medical Thing (IoMT) and the Need of a New IoMT Law. *Journal of Healthcare Ethics & Administration* **4**, 32–38 (2018).

29. Venkitaraman, A. K. & Kosuru, V. S. R. Electric Vehicle Charging Network Optimization using Multi-Variable Linear Programming and Bayesian Principles. in *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* 1–5 (ieeexplore.ieee.org, 2022). doi:10.1109/ICSTCEE56972.2022.10099649.

30. Uyyala, P. Credit Card Transactions Data Adversarial Augmentation in the Frequency Domain. *The International journal of analytical and experimental modal analysis* **13**, 2712–2718 (2021).

31. Kavasseri Venkitaraman, A. & Satya Rahul Kosuru, V. Trends and challenges in electric vehicle motor drivelines - A review. *Int. J. Elect. Computer Syst. Eng.* **14**, 485–495 (2023).

32. Alsubaei, F., Abuhussein, A. & Shiva, S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)* 112–120 (ieeexplore.ieee.org, 2017). doi:10.1109/LCN.Workshops.2017.72.

33. Uyyala, P. DETECTION OF CYBER ATTACK IN NETWORK USING MACHINE LEARNING TECHNIQUES. *Journal of interdisciplinary cycle research* **14**, 1903–1913 (2022).

34. Williams, P. A. H. & McCauley, V. Always connected: The security challenges of the healthcare Internet of Things. in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* 30–35 (ieeexplore.ieee.org, 2016). doi:10.1109/WF-IoT.2016.7845455.

35. Kosuru, V. S. R. & Venkitaraman, A. K. Developing a deep Q-learning and neural network framework for trajectory planning. *European Journal of Engineering and Technology Research* **7**, 148–157 (2022).

36. Alamdari, M. G. & Nasab, M. A. INTERNET OF THINGS AND SUSTAINABLE DEVELOPMENT OF HEALTH. *Fundam. Appl. Toxicol.* **8**, 2732–2740 (2016).

37. Uyyala, P. DETECTING AND CHARACTERIZING EXTREMIST REVIEWER GROUPS IN ONLINE PRODUCT REVIEWS. *Journal of interdisciplinary cycle research* **14**, 1689–1699 (2022).

38. Maksimović, M. & Vujović, V. Internet of Things Based E-health Systems: Ideas, Expectations and Concerns. in *Handbook of Large-Scale Distributed Computing in Smart Healthcare* (eds. Khan, S. U., Zomaya, A. Y. & Abbas, A.) 241–280 (Springer International Publishing, 2017). doi:10.1007/978-3-319-58280-1_10.

39. Jahankhani, H. & Ibarra, J. Digital forensic investigation for the Internet of Medical Things (IoMT). *Forensic Leg. Investig. Sci* **5**, 029 (2019).

40. Uyyala, P. AUTOMATIC DETECTION OF GENETIC DISEASES IN PEDIATRIC AGE USING PUPILLOMETRY. *Journal of interdisciplinary cycle research* **14**, 1748–1760 (2022).

41. Hatzivasilis, G. *et al.* Review of Security and Privacy for the Internet of Medical Things (IoMT). in *2019 15th International Conference on Distributed Computing in*

Sensor Systems (DCOSS) 457–464 (ieeexplore.ieee.org, 2019). doi:10.1109/DCOSS.2019.00091.

42. Rahul, V. S. Kosuru; Venkitaraman, AK Integrated framework to identify fault in human-machine interaction systems. *Int. Res. J. Mod. Eng. Technol. Sci* (2022).
43. Aftab, M. U. *et al.* Negative Authorization by Implementing Negative Attributes in Attribute-Based Access Control Model for Internet of Medical Things. in *2019 15th International Conference on Semantics, Knowledge and Grids (SKG)* 167–174 (ieeexplore.ieee.org, 2019). doi:10.1109/SKG49510.2019.00036.
44. Uyyala, P. COLLUSION DEFENDER PRESERVING SUBSCRIBERS PRIVACY IN PUBLISH AND SUBSCRIBE SYSTEMS. *The International journal of analytical and experimental modal analysis* **13**, 2639–2645 (2021).
45. Treacy, C., Loane, J. & McCaffery, F. A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. in *Systems, Software and Services Process Improvement* 107–119 (Springer International Publishing, 2020). doi:10.1007/978-3-030-56441-4_8.
46. Uyyala, P. Efficient and Deployable Click Fraud Detection for Mobile Applications. *The International journal of analytical and experimental modal analysis* **13**, 2360–2372 (2021).
47. Uyyala, P. PREDICTING RAINFALL USING MACHINE LEARNING TECHNIQUES. *J. Interdiscipl. Cycle Res.* **14**, 1284–1292 (2022).
48. Fiaidhi, J. & Mohammed, S. Security and Vulnerability of Extreme Automation Systems: The IoMT and IoA Case Studies. *IT Prof.* **21**, 48–55 (2019).
49. Banerjee, M., Lee, J. & Choo, K.-K. R. A blockchain future for internet of things security: a position paper. *Digital Communications and Networks* **4**, 149–160 (2018).

50. Kosuru, V. S. R. *et al.* Automatic Identification of Vehicles in Traffic using Smart Cameras. in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* 1009–1014 (ieeexplore.ieee.org, 2022). doi:10.1109/IC3I56241.2022.10072979.

51. Uyyala, P. Privacy-aware Personal Data Storage (P-PDS): Learning how toProtect User Privacy from External Applications. *The International journal of analytical and experimental modal analysis* **13**, 3257–3273 (2021).

52. Gardašević, G., Katzis, K., Bajić, D. & Berbakov, L. Emerging Wireless Sensor Networks and Internet of Things Technologies—Foundations of Smart Healthcare. *Sensors* **20**, 3619 (2020).

53. Bates, J. A. Cyber Threats that Lurk in the Internet of Medical Things (IoMt). (search.proquest.com, 2020).

54. Kosuru, V. S. R. & Kavasseri Venkitaraman, A. A Smart Battery Management System for Electric Vehicles Using Deep Learning-Based Sensor Fault Detection. *World Electric Vehicle Journal* **14**, 101 (2023).

55. Kosuru, V. S. R. & Venkitaraman, A. K. Evaluation of Safety Cases in The Domain of Automotive Engineering. *International Journal of Innovative Science and Research Technology* **7**, 493–497 (2022).

56. Uyyala, P. SIGN LANGUAGE RECOGNITION USING CONVOLUTIONAL NEURAL NETWORKS. *Journal of interdisciplinary cycle research* **14**, 1198–1207 (2022).

57. Nkomo, D. & Brown, R. Hybrid Cyber Security Framework for the Internet of Medical Things. in *Blockchain and Clinical Trial: Securing Patient Data* (eds. Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G. & Al-Khateeb, H.) 211–229 (Springer International Publishing, 2019). doi:10.1007/978-3-030-11289-9_9.

58. Tariq, M. I., Mian, N. A., Sohail, A., Alyas, T. & Ahmad, R. Evaluation of the challenges in the Internet of medical things with multicriteria decision making (AHP and TOPSIS) to overcome its obstruction under fuzzy environment. *Mobile Information Systems* **2020**, 1–19 (2020).

59. Rajput, A. & Brahimi, T. Chapter 15 - Characterizing internet of medical things/personal area networks landscape. in *Innovation in Health Informatics* (eds. Lytras, M. D. & Sarirete, A.) 353–371 (Academic Press, 2020). doi:10.1016/B978-0-12-819043-2.00015-0.

60. McFarland, R. J. & Olatunbosun, S. B. An Exploratory Study on the use of Internet_of_Medical_Things (IoMT) In the Healthcare Industry and their Associated Cybersecurity Risks. in (search.proquest.com, 2019).

61. Kim, E.-C., Kim, E.-Y., Lee, H.-C. & Yoo, B.-J. The Details and Outlook of Three Data Acts Amendment in South Korea: With a Focus on the Changes of Domestic Financial and Data Industry. *Informatization Policy* **28**, 49–72 (2021).

62. Daniels, J. *et al.* The Internet of Things, Artificial Intelligence, Blockchain, and Professionalism. *IT Prof.* **20**, 15–19 (2018).

63. Choi, B., Lee, Y., Kyung, Y. & Kim, E. ALBERT with Knowledge Graph Encoder Utilizing Semantic Similarity for Commonsense Question Answering. *arXiv [cs.CL]* (2022).

64. Karakolias, S. & Kastanioti, C. Application of an organizational assessment tool of primary health care. *Arch Hell Med* **35**, 497–505 (2018).

65. Kim, E. *et al.* SHOMY: Detection of Small Hazardous Objects using the You Only Look Once Algorithm. *KSII Transactions on Internet & Information Systems* **16**, (2022).

66. Marafino, B. J. *et al.* Validation of Prediction Models for Critical Care Outcomes Using Natural Language Processing of Electronic Health Record Data. *JAMA Netw Open* **1**, e185097 (2018).

67. Cook, B. L. *et al.* Novel Use of Natural Language Processing (NLP) to Predict Suicidal Ideation and Psychiatric Symptoms in a Text-Based Mental Health Intervention in Madrid. *Comput. Math. Methods Med.* **2016**, 8708434 (2016).

68. Kim, E., Kim, M. & Kyung, Y. A Case Study of Digital Transformation: Focusing on the Financial Sector in South Korea and Overseas. *Asia Pacific Journal of Information Systems* **32**, 537–563 (2022).

69. Conway, M., Hu, M. & Chapman, W. W. Recent Advances in Using Natural Language Processing to Address Public Health Research Questions Using Social Media and ConsumerGenerated Data. *Yearb. Med. Inform.* **28**, 208–217 (2019).

70. Kim, E., Kim, J., Park, J., Ko, H. & Kyung, Y. TinyML-Based Classification in an ECG Monitoring Embedded System. *CMC-COMPUTERS MATERIALS & CONTINUA* **75**, 1751–1764 (2023).

71. Low, D. M. *et al.* Natural Language Processing Reveals Vulnerable Mental Health Support Groups and Heightened Health Anxiety on Reddit During COVID-19: Observational Study. *J. Med. Internet Res.* **22**, e22635 (2020).

72. Ayanouz, S., Abdelhakim, B. A. & Benhmed, M. A Smart Chatbot Architecture based NLP and Machine Learning for Health Care Assistance. in *Proceedings of the 3rd International Conference on Networking, Information Systems & Security* 1–6 (Association for Computing Machinery, 2020). doi:10.1145/3386723.3387897.

73. Kim, E. *et al.* Machine Learning-based Prediction of Relative Regional Air Volume Change from Healthy Human Lung CTs. *KSII Transactions on Internet & Information Systems* **17**, (2023).

74. Gopalan, S. S., Raza, A. & Almobaideen, W. IoT Security in Healthcare using AI: A Survey. in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)* 1–6 (ieeexplore.ieee.org, 2021). doi:10.1109/ICCSPA49915.2021.9385711.

75. Chen, M. & Decary, M. Artificial intelligence in healthcare: An essential guide for health leaders. *Healthc. Manage. Forum* **33**, 10–18 (2020).

76. Kim, E. & Kyung, Y. Factors Affecting the Adoption Intention of New Electronic Authentication Services: A Convergent Model Approach of VAM, PMT, and TPB. *IEEE Access* **11**, 13859–13876 (2023).

77. Baba, A. & Bunji, K. Prediction of mental health problem using annual student health survey: A machine learning approach (preprint). *JMIR Ment. Health* (2022) doi:10.2196/42420.

78. Vozikis, A., Panagiotou, A. & Karakolias, S. A Tool for Litigation Risk Analysis for Medical Liability Cases. *HAPScPBS* **2**, 268–277 (2021).

79. Karakolias, S. & Polyzos, N. Application and assessment of a financial distress projection model in private general clinics. *Archives of Hellenic Medicine/Arheia Ellenikes Iatrikes* **32**, (2015).

80. Dredze, M. How Social Media Will Change Public Health. *IEEE Intell. Syst.* **27**, 81–84 (2012).

81. Qureshi, B. Towards a Digital Ecosystem for Predictive Healthcare Analytics. in *Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems* 34–41 (Association for Computing Machinery, 2014). doi:10.1145/2668260.2668286.

82. Karakolias, S. E. & Polyzos, N. M. The newly established unified healthcare fund (EOPYY): current situation and proposed structural changes, towards an upgraded model of primary health care, in Greece. *Health* **2014**, (2014).

83. Polyzos, N., Karakolias, S., Mavridoglou, G., Gkorezis, P. & Zilidis, C. Current and future insight into human resources for health in Greece. *Open J. Soc. Sci.* **03**, 5–14 (2015).

84. Yu, K.-H., Beam, A. L. & Kohane, I. S. Artificial intelligence in healthcare. *Nat Biomed Eng* **2**, 719–731 (2018).

85. Polyzos, N. *et al.* Greek National E-Prescribing System: Preliminary Results of a Tool for Rationalizing Pharmaceutical Use and Cost. *Glob. J. Health Sci.* **8**, 55711 (2016).

86. Jiang, F. *et al.* Artificial intelligence in healthcare: past, present and future. *Stroke Vasc Neurol* **2**, 230–243 (2017).

87. Polyzos, N. *et al.* The introduction of Greek Central Health Fund: Has the reform met its goal in the sector of Primary Health Care or is there a new model needed? *BMC Health Serv. Res.* **14**, 583 (2014).

88. Karakolias, S., Kastanioti, C., Theodorou, M. & Polyzos, N. Primary care doctors' assessment of and preferences on their remuneration. *Inquiry* **54**, 46958017692274 (2017).

89. Singh, K., Misra, M. & Yadav, J. Artificial Intelligence and Machine Learning as a Tool for Combating COVID-19: A Case Study on Health-Tech Start-ups. in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* 1–5 (ieeexplore.ieee.org, 2021). doi:10.1109/ICCCNT51525.2021.9579950.

90. Pramanik, P. K. D., Pareek, G. & Nayyar, A. Chapter 14 - Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards. in *Telemedicine Technologies*

(eds. D. Jude, H. & Balas, V. E.) 201–225 (Academic Press, 2019). doi:10.1016/B978-0-12-816948-3.00014-3.

91. Vaishya, R., Javaid, M., Khan, I. H. & Haleem, A. Artificial Intelligence (AI) applications for COVID-19 pandemic. *Diabetes Metab. Syndr.* **14**, 337–339 (2020).
92. Shaw, J., Rudzicz, F., Jamieson, T. & Goldfarb, A. Artificial Intelligence and the Implementation Challenge. *J. Med. Internet Res.* **21**, e13659 (2019).
93. Carson, N. J. *et al.* Identification of suicidal behavior among psychiatrically hospitalized adolescents using natural language processing and machine learning of electronic health records. *PLoS One* **14**, e0211116 (2019).
94. Barrera Ferro, D., Brailsford, S., Bravo, C. & Smith, H. Improving healthcare access management by predicting patient no-show behaviour. *Decis. Support Syst.* **138**, 113398 (2020).
95. D'Alfonso, S. AI in mental health. *Curr Opin Psychol* **36**, 112–117 (2020).
96. Yang, Z. *et al.* Modified SEIR and AI prediction of the epidemics trend of COVID-19 in China under public health interventions. *J. Thorac. Dis.* **12**, 165–174 (2020).
97. Ghazal, T. M. RETRACTED ARTICLE: Internet of things with artificial intelligence for health care security. *Arab. J. Sci. Eng.* **48**, 5689–5689 (2023).
98. Hamet, P. & Tremblay, J. Artificial intelligence in medicine. *Metabolism* (2017).
99. Yeng, P. K., Nweke, L. O., Woldaregay, A. Z., Yang, B. & Snekkenes, E. A. Data-Driven and Artificial Intelligence (AI) Approach for Modelling and Analyzing Healthcare Security Practice: A Systematic Review. in *Intelligent Systems and Applications* 1–18 (Springer International Publishing, 2021). doi:10.1007/978-3-030-55180-3_1.
100. Davenport, T. & Kalakota, R. The potential for artificial intelligence in healthcare. *Future Healthc J* **6**, 94–98 (2019).

101. Topol, E. J. High-performance medicine: the convergence of human and artificial intelligence. *Nat. Med.* (2019).