Supplementary Table 1. Comprehensive description of the previous research work conducted in the field of cybersecurity

|  |  |
| --- | --- |
| **Author/ Contribution** | **Insights** |
| **Pros****Cons****Prediction Techniques** |
| **Inkster *et al.* (2021)**Studied the existing condition of cybersecurity in the digital mental health sector to jointly pinpoint risks and safeguard the vulnerabilities of users and providers and proposed the formation of a cybersecurity culture within digital mental health [4]. | **Enhanced Security**: The study emphasizes the importance of cybersecurity in protecting sensitive mental health data, which is crucial for maintaining user trust and confidentiality.**Risk Identification**: By pinpointing risks, the study helps in identifying potential vulnerabilities that could be exploited by cyber attackers.**Cybersecurity Culture**: The proposal to form a cybersecurity culture within digital mental health aims to create a proactive approach to cybersecurity, ensuring continuous improvement  | **Implementation Challenges**: Establishing a cybersecurity culture requires significant effort, resources, and time, which might be challenging for some organizations.**Technical Expertise**: The need for specialized knowledge in both mental health and cybersecurity can be a barrier, as professionals in these fields may not have overlapping expertise.**Cost**: Implementing advanced cybersecurity measures can be costly, which might be a concern for smaller organizations or those with limited budgets | **Machine Learning Models**: The study highlights the use of machine learning models to predict potential cyber threats and vulnerabilities.**Behavioral Analysis**: Analyzing user behavior to detect anomalies that could indicate a security breach.**Threat Intelligence**: Utilizing threat intelligence to stay updated on the latest cyber threats  |
| **Yeng et al. (2021)**Conducted a study to identify suitable AI techniques and data sources for effective modeling and analysis of healthcare staff’s security practices. They developed and implemented a framework using simulated data, offering a holistic method for modeling and analyzing the security practices of healthcare staff using real access logs [5]. |  **Holistic Approach**: The study provides a comprehensive framework for modeling and analyzing healthcare staff's security practices, considering various data sources and AI techniques.**Simulated Data**: The use of simulated data allows for a controlled environment to test and refine the framework before applying it to real-world scenarios.**Real Access Logs**: Incorporating real access logs ensures that the framework is grounded in actual practices | **Complexity**: The framework's comprehensive nature may make it complex to implement, requiring significant resources and expertise.**Data Privacy**: Using real access logs raises concerns about data privacy and the ethical implications of monitoring healthcare staff.**Scalability**: The framework may face challenges in scaling up to larger healthcare organizations with diverse security practices. | **K-Nearest Neighbors (KNN)**: Used for classifying security practices based on historical data.**Bayesian Network**: Employed to model the probabilistic relationships between different security practices and potential breaches.**Decision Trees (C4.5)**: Utilized for decision-making processes in identifying and mitigating security risks. |
| **Arshad *et al.* (2021)**Investigated bio-cybersecurity threats related to genomic-DNA data and software applications that utilize such data for scientific research. Using empirical methods, they analyzed and identified vulnerabilities within genomic-DNA databases and bioinformatics software, aiming to prevent cyber-attacks that could compromise the confidentiality, integrity, and availability of this critical data [6]. | **Enhanced Security**: The study emphasizes the importance of securing genomic-DNA data and bioinformatics software, which is crucial for maintaining the confidentiality, integrity, and availability of sensitive data.**Risk Identification**: By analyzing vulnerabilities, the study helps in identifying potential threats that could be exploited by cyber attackers.**Empirical Approach**: The use of empirical methods provides a robust framework for analyzing and identifying vulnerabilities within genomic-DNA databases and bioinformatics software | **Complexity**: The comprehensive nature of the study may make it complex to implement, requiring significant resources and expertise.**Data Privacy**: Handling sensitive genomic-DNA data raises concerns about data privacy and the ethical implications of monitoring and analyzing such data.**Scalability**: The framework may face challenges in scaling up to larger databases and more complex bioinformatics software | **Empirical Analysis**: The study employs empirical methods to analyze and identify vulnerabilities within genomic-DNA databases and bioinformatics software.**Threat Modeling**: Utilizing threat modeling to predict potential cyber-attacks and vulnerabilities.**Security-by-Design**: Adopting a security-by-design approach to ensure that security measures are integrated into the development and implementation of bioinformatics  |
| **Roosan *et al.* (2022)** Proposed a conceptual framework based on blockchain and AI by conducting a scoping review of successful blockchain integrations in health systems to enhance access to healthcare data in the community pharmacy setting through the adoption of blockchain technology and AI. They used the Pharmacists’ Patient Care Process to pinpoint crucial areas for blockchain integration that can assist community pharmacists in accessing patient’s electronic health records and incorporating patient-specific information into clinical decision-making [7]. | **Enhanced Data Access**: The framework improves access to healthcare data for community pharmacists, enabling them to make more informed clinical decisions.**Data Security**: Blockchain technology ensures secure sharing of healthcare data, protecting patient privacy and data integrity.**Integration with AI**: The use of AI enhances the ability to analyze and utilize healthcare data effectively, improving patient outcomes | **Implementation Complexity**: Integrating blockchain and AI into existing healthcare systems can be complex and resource-intensive.**Technical Expertise**: Requires specialized knowledge in both blockchain and AI, which may not be readily available in all healthcare settings.**Cost**: The initial setup and maintenance of blockchain and AI systems can be expensive | **Scoping Review**: The study conducted a scoping review to identify successful blockchain integrations in health systems.**Pharmacists’ Patient Care Process (PPCP)**: Used to pinpoint crucial areas for blockchain integration that can assist community pharmacists in accessing and utilizing patient-specific information.**AI Algorithms**: Employed to analyze healthcare data and support clinical decision-making |
| **Almaiah *et al.* (2022)**Introduced a two-layer blockchain-based deep-learning framework in which a blockchain scheme was proposed where each participant was registered, verified, and subsequently validated using an enhanced Proof of Work based on smart contracts to achieve security and privacy. using a Variational auto-encoder technique, A deep-learning scheme was also designed for privacy and a Bidirectional long short-term memory or intrusion detection [8]. | **Enhanced Security and Privacy**: The two-layer blockchain-based framework ensures robust security and privacy by registering, verifying, and validating each participant using an enhanced Proof of Work based on smart contracts.**Privacy Preservation**: The use of a Variational Auto-Encoder (VAE) technique enhances privacy by ensuring that sensitive data is protected.**Intrusion Detection**: The Bidirectional Long Short-Term Memory (BiLSTM) model is effective for intrusion detection, providing an additional layer of security | **Complex Implementation**: The framework's complexity may pose challenges in implementation, requiring significant resources and expertise.**Scalability Issues**: The scalability of the framework may be limited, especially in larger networks with numerous participants.**Cost**: Implementing and maintaining the blockchain-based framework can be costly, which might be a concern for smaller organizations. | **Variational Auto-Encoder (VAE)**: Used for privacy preservation by encoding and decoding data in a way that ensures sensitive information is protected.**Bidirectional Long Short-Term Memory (BiLSTM)**: Employed for intrusion detection, analyzing data sequences to identify potential security threats.**Enhanced Proof of Work (PoW)**: Utilized for registering, verifying, and validating participants, ensuring the integrity and security of the blockchain network |
| **Nayak *et al.* (2022)**Introduced a new IoMT framework combining Bayesian optimization and an extreme learning machine that showed promising results and improved decision-making accuracy compared to other contemporary methods [9]. |  **Improved Decision-Making Accuracy**: The combination of Bayesian optimization and extreme learning machine (ELM) showed promising results in enhancing decision-making accuracy.**Enhanced Performance**: The proposed IoMT framework demonstrated better performance compared to other contemporary methods.**Efficient Cyber-Attack Detection**: The framework effectively detected cyber-attacks, ensuring the security of IoMT devices . | **Complex Implementation**: The integration of Bayesian optimization and ELM can be complex and may require significant resources and expertise.**Scalability Issues**: The framework may face challenges in scaling up to larger networks with numerous IoMT devices.**Cost**: Implementing and maintaining the framework can be costly, which might be a concern for smaller healthcare organizations | **Bayesian Optimization**: Used to optimize the parameters of the extreme learning machine, enhancing its performance and accuracy.**Extreme Learning Machine (ELM)**: Employed for cyber-attack detection, analyzing data to identify potential security threats |
| **Salim *et al.*(2022)**Used a decentralized Federated Learning-based Convolutional Neural Network model to train data locally within the hospital and store the results in a private Interplanetary File System and the evaluation results showed that in terms of accuracy, sensitivity, and specificity, the decentralized CNN model performs almost the same as the traditional centralized model [10]. | **Data Privacy**: The decentralized Federated Learning-based Convolutional Neural Network (CNN) model ensures that data is trained locally within the hospital, enhancing data privacy and security.**Performance**: The evaluation results showed that the decentralized CNN model performs almost the same as the traditional centralized model in terms of accuracy, sensitivity, and specificity.**Data Storage**: Storing the results in a private Interplanetary File System (IPFS) ensures secure and efficient data storage. | **Implementation Complexity**: Implementing a decentralized Federated Learning-based CNN model can be complex and resource-intensive.**Technical Expertise**: Requires specialized knowledge in both federated learning and CNNs, which may not be readily available in all healthcare settings.**Scalability**: The framework may face challenges in scaling up to larger networks with numerous participants. | **Federated Learning**: Used to train data locally within the hospital, ensuring data privacy and security.**Convolutional Neural Network (CNN)**: Employed for training and analyzing the data.**Interplanetary File System (IPFS)**: Utilized for secure and efficient data storage. |
| **Ramasamy *et al.* (2022)**Developed an AI-powered Internet of Things Cyber-Physical System (IoT-CPS) intended for physicians to diagnose various medical conditions in patients to detect diseases such as diabetes, heart disease, and gait abnormalities [11]. | **Enhanced Diagnostic Accuracy**: The AI-powered IoT-CPS improves the accuracy of diagnosing various medical conditions, such as diabetes, heart disease, and gait abnormalities2.**Real-Time Monitoring**: The system allows for real-time monitoring of patients' health data, enabling timely interventions and better management of chronic conditions.**Integration of Wearable Sensors**: To ensures continuous data collection, providing a comprehensive view of patient's health | **Implementation Complexity**: Integrating AI and IoT-CPS into existing healthcare systems can be complex and resource-intensive.**Data Privacy Concerns**: Handling sensitive health data raises concerns about data privacy and security.**Technical Expertise**: Requires specialized knowledge in AI, IoT, and healthcare, which may not be readily available in all healthcare settings. | **AI Algorithms**: The study employs AI algorithms to analyze health data and diagnose medical conditions.**Wearable Sensors**: Utilized for continuous data collection and monitoring of patients' health.**Cyber-Physical Systems (CPS)**: Integrates physical and computational components to enhance the accuracy and efficiency of medical diagnoses |
| **Wahab *et al.* (2022)**Proposed an AI-powered, SDN-enabled Intrusion Detection System for e-health and IoMT environments. Combined LSTM and GRU models, evaluated using the CIC DDoS 2019 dataset, achieved high-performance metrics such as 99.01% accuracy and 99.12% F1 score [12]. | **High Performance**: The AI-powered, SDN-enabled Intrusion Detection System (IDS) achieved impressive performance metrics.**Effective Detection**: The combination of Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) models enhances the system's ability to detect cyber threats in e-health and IoMT environments.**Scalability**: The use of Software-Defined Networking (SDN) allows for flexible and scalable network management, making it suitable for dynamic IoMT environments | **Complex Implementation**: Integrating AI and SDN into existing healthcare systems can be complex and resource-intensive.**Technical Expertise**: Requires specialized knowledge in AI, SDN, and cybersecurity, which may not be readily available in all healthcare settings.**Data Privacy Concerns**: Handling sensitive health data raises concerns about data privacy and security | **Long Short-Term Memory (LSTM)**: Used for analyzing sequential data and detecting anomalies in network traffic.**Gated Recurrent Unit (GRU)**: Employed alongside LSTM to enhance the model's performance in detecting cyber threats.**CIC DDoS 2019 Dataset**: Utilized for evaluating the performance of the proposed IDS, ensuring its effectiveness in real-world scenarios |
| **Ali *et al.* (2022)**Emphasized the significance of Federated Learning within IoMT networks to uphold privacy. Introduced advanced Federated Learning structures incorporating Deep Reinforcement Learning, Digital Twin, and GANs to identify privacy vulnerabilities [13]. | **Privacy Preservation**: Federated Learning (FL) ensures that data remains local, enhancing privacy by not sharing raw data with central servers.**Advanced Techniques**: Incorporating Deep Reinforcement Learning (DRL), Digital Twin, and Generative Adversarial Networks (GANs) helps in identifying and mitigating privacy vulnerabilities.**Scalability**: FL can be scaled across multiple IoMT devices, making it suitable for large-scale healthcare applications. | **Complex Implementation**: Integrating FL with DRL, Digital Twin, and GANs can be complex and resource-intensive.**Technical Expertise**: Requires specialized knowledge in FL, DRL, Digital Twin, and GANs, which may not be readily available in all healthcare settings.**Data Synchronization**: Ensuring consistent and synchronized data across multiple devices can be challenging. | **Deep Reinforcement Learning (DRL)**: Used to optimize the decision-making process in identifying privacy vulnerabilities.**Digital Twin**: Creates a virtual replica of the IoMT network to simulate and analyze potential privacy threats.**Generative Adversarial Networks (GANs)**: Employed to detect and mitigate privacy vulnerabilities by generating synthetic data for training |
| **Radanliev et al. (2022)** Investigated cybersecurity risks in the context of AI and technological singularity. Developed a framework to mitigate AI-related risks, emphasizing the importance of AI in defense and preventing autonomous AI device actions [15]. | **Risk Mitigation:** The framework developed in the study aims to mitigate AI-related risks, ensuring that AI systems are secure and reliable.**Proactive Defense:** Emphasizes the importance of AI in defense, highlighting its potential to prevent autonomous AI deviceactions that could pose threats.**Comprehensive Analysis:** The study provides a thorough analysis of cybersecurity risks in the context of AI and technological singularity, offering valuable insights for future research and development. | **Complexity:** Implementing the proposed framework can be complex and resource-intensive, requiring significant expertise in AI and cybersecurity.**Unpredictability:** The study acknowledges the inherent unpredictability of AI systems, which can make it challenging to fully anticipate and mitigate all potential risks.**Ethical Concerns:** The use of AI in defense raises ethical concerns, particularly regarding the potential for autonomous AI devices to act independently. | **Risk Forecasting**: The study employs risk forecasting to predict emerging cyber-risks from the integration of AI in cybersecurity2.**Super-Forecasting**: Utilizes super-forecasting techniques to create synergies between existing literature, data sources**Algorithm Development**: Focuses on developing algorithms that enable systems to continue operating even when parts of the system have been compromised |
| **Biasin *et al.* (2022)**Examined the interaction between new reforms and existing laws from a cybersecurity perspective. Found that simultaneous implementation of similar measures could lead to fragmentation and inconsistent protection levels in healthcare [16]. | **Enhanced Cybersecurity:** The study highlights the importance of new reforms in strengthening cybersecurity measures in healthcare, ensuring better protection of sensitive data.**Regulatory Improvements:** The interaction between new reforms and existing laws can lead to more comprehensive and updated cybersecurity regulations | **Fragmentation**: The simultaneous implementation of similar measures could lead to regulatory fragmentation, causing inconsistencies in protection levels across different regions and healthcare systems.**Inconsistent Protection**: The study found that overlapping cybersecurity requirements might result in uneven levels of protection, potentially leaving some areas more vulnerable than others. | **Regulatory Analysis**: The study employs regulatory analysis to examine the interaction between new reforms and existing laws, identifying potential areas of overlap and fragmentation.**Policy Recommendations**: Based on the findings, the study provides policy recommendations to mitigate the risks of fragmentation and ensure consistent protection levels. |
| **Horowitz et al. (2023)** Studied the influence of human inclinations on the adoption of AI-powered autonomous technologies. Found that individuals with AI knowledge were more inclined to endorse autonomous applications across various fields compared to those with limited understanding [17]. | **Innovative Approaches**: The study emphasizes the potential of evolutionary medicine to transform biomedicine and public health by sparking innovation.**Cross-Disciplinary Insights**: The research highlights the importance of integrating insights from various disciplines to address complex health issues.**Therapeutic Advancements**: The study suggests novel therapeutic approaches that target the development of treatment resistance in cancers and antimicrobial resistance | **Implementation Challenges**: Integrating evolutionary medicine into existing healthcare systems can be complex and resource-intensive.**Acceptance**: The study acknowledges that some medical professionals may be resistant to adopting new approaches based on evolutionary medicine.**Ethical Concerns**: The use of evolutionary principles in medicine may raise ethical concerns, particularly regarding the manipulation of biological systems | **Adaptive Therapy**: The study suggests using adaptive therapy to manage treatment resistance in cancers.**Extinction Therapy**: Proposed as a method to target and eliminate resistant cancer cells.**Innovations in Chemistry**: The study highlights the importance of developing new chemical compounds to combat antimicrobial resistance. |
| **Kelly *et al.* (2023)**Proposed cybersecurity principles for medical imaging, detailing strategies for detection and prevention, and the role of technology in enhancing security. Offered suggestions for radiologists to understand threats linked with radiology AI [18]. | **Enhanced Security**: The study emphasizes the importance of cybersecurity principles in medical imaging, ensuring better protection of sensitive data.**Proactive Measures**: The proposed strategies for detection and prevention help in identifying and mitigating potential threats before they can cause harm.**Educational Value**: The study offers valuable suggestions for radiologists to understand and address threats linked with radiology AI, promoting a better understanding of cybersecurity in the medical field | **Implementation Challenges**: Integrating the proposed cybersecurity principles into existing medical imaging systems can be complex and resource-intensive.**Technical Expertise**: Requires specialized knowledge in both cybersecurity and medical imaging, which may not be readily available in all healthcare settings.**Cost**: Implementing advanced cybersecurity measures can be costly, which might be a concern for smaller healthcare organizations | **AI Algorithms**: The study highlights the use of AI algorithms to detect and prevent cybersecurity threats in medical imaging.**Data Encryption**: Emphasizes the importance of data encryption to protect sensitive medical information during transmission and storage.**Regular Audits**: Recommends conducting regular cybersecurity audits to identify and address vulnerabilities in medical imaging systems |
| **Oniani *et al.* (2023)**Investigated ethical principles for generative AI in healthcare from a military perspective. Presented a framework for implementing ethical principles such as Governability, Reliability, Equity, Accountability, Traceability, Privacy, Lawfulness, Empathy, and Autonomy [19]. | **Comprehensive Ethical Framework**: The study proposes a detailed framework for implementing ethical principles in generative AI, ensuring that AI systems are governed by principles such as Governability, Reliability, Equity, Accountability, Traceability, Privacy, Lawfulness, Empathy, and Autonomy.**Cross-Disciplinary Insights**: By drawing parallels between military and healthcare applications, the study provides valuable insights that can be applied across different fields.**Proactive Approach**: The framework aims to proactively address ethical dilemmas and challenges posed by the integration of generative AI into healthcare | **Implementation Complexity**: Implementing the proposed ethical framework can be complex and resource-intensive, requiring significant expertise and coordination.**Potential Resistance**: There may be resistance to adopting new ethical principles, especially if they require significant changes to existing practices.**Ethical Concerns**: The study acknowledges that ethical concerns, such as transparency and bias, remain challenging to fully address | **Reliability**: Implementing measures to ensure that AI systems are reliable and perform as expected.**Equity**: Addressing biases in AI models to ensure fair and equitable outcomes.**Accountability**: Establishing mechanisms for holding AI systems and their developers accountable for their actions.**Privacy**: Protecting the privacy of individuals whose data is used by AI systems.**Autonomy**: Balancing the autonomy of AI systems with the need for human oversight. |
| **Riggs *et al*. (2023)**Compiled significant cyber data to examine types of cyber-attacks, their impacts, vulnerabilities, and the victims and perpetrators. Catalogued cybersecurity standards and tools to tackle these issues [20]. | C**omprehensive Analysis**: The study provides a thorough examination of various types of cyber-attacks, their impacts, vulnerabilities, and the victims and perpetrators.**Catalogued Standards and Tools**: By cataloging cybersecurity standards and tools, the study offers valuable resources for addressing cybersecurity issues.**Future Predictions**: The study includes predictions about the number of major cyber-attacks on critical infrastructure, helping organizations prepare for future threats | **Implementation Complexity**: Implementing the recommended cybersecurity standards and tools can be complex and resource-intensive.**Data Overload**: The extensive amount of data compiled in the study may be overwhelming for some organizations to process and utilize effectively.**Scalability Issues**: The study's recommendations may face challenges in scaling up to larger organizations with diverse cybersecurity needs | **Risk Forecasting**: The study employs risk forecasting to predict the number of major cyber-attacks on critical infrastructure in the future.**Data Analysis**: Utilizes extensive data analysis to examine the types of cyber-attacks, their impacts, vulnerabilities, and the victims and perpetrators.**Cybersecurity Standards and Tools**: Catalogues various cybersecurity standards and tools to address identified vulnerabilities and mitigate future risks |
| **Barbaria *et al.*(2023)**To safeguard the integrity of sensitive healthcare data in AI-driven medical research, Proposed a blockchain-based architectural framework and Conducted a comprehensive analysis of public administration purchase records for potentially vulnerable medical devices [21]. | **Data Integrity**: The blockchain-based architectural framework ensures the integrity of sensitive healthcare data, making it tamper-proof and secure.**Enhanced Security**: By using blockchain technology, the framework provides robust security measures to protect healthcare data from unauthorized access and cyber-attacks.**Transparency**: Blockchain's decentralized nature ensures transparency in data transactions, making it easier to track and verify data changes. | **Implementation Complexity**: Implementing a blockchain-based framework can be complex and resource-intensive, requiring significant expertise and coordination.**Scalability Issues**: The framework may face challenges in scaling up to larger networks with numerous participants. **Cost**: The initial setup and maintenance of blockchain technology can be costly, which might be a concern for smaller healthcare organizations. | **Blockchain Analysis**: The study employs blockchain technology to ensure data integrity and security.**Public Administration Purchase Records Analysis**: Conducted a comprehensive analysis of public administration purchase records to identify potentially vulnerable medical devices.**Smart Contracts**: Utilized smart contracts to automate compliance and enhance security measures. |
| **Selvarajan *et al*. (2023)**Introduced a technique for secure data exchange within healthcare systems using blockchain technology. Shaped a distinctive key pair for secure storage of patient data in hash value blocks [22]. | **Enhanced Security**: The technique ensures secure data exchange within healthcare systems by using blockchain technology, which provides robust security measures.**Data Integrity**: The use of distinctive key pairs for secure storage of patient data in hash value blocks ensures data integrity and prevents tampering.**Privacy Protection**: Blockchain technology enhances privacy protection by ensuring that patient data is securely stored and accessed only by authorized personnel. | **Implementation Complexity**: Implementing blockchain technology in healthcare systems can be complex and resource-intensive, requiring significant expertise and coordination.**Scalability Issues**: The framework may face challenges in scaling up to larger healthcare networks with numerous participants.**Cost**: The initial setup and maintenance of blockchain technology can be costly, which might be a concern for smaller healthcare organizations. | **Blockchain Technology**: Used to ensure secure data exchange and storage within healthcare systems.**Distinctive Key Pair**: Shaped a distinctive key pair for secure storage of patient data in hash value blocks, ensuring data integrity and privacy. |
| **Cartwright *et al.* (2023)**Described on the daily use of IoMT devices in anesthesia and ICU, highlighting the potential entry points for cyber threats and the risks to patient safety and PHI. Also Emphasized the need for secure IoT devices in healthcare [23]. | **Enhanced Patient Care**: The daily use of IoMT devices in anesthesia and ICU improves patient monitoring and care by providing real-time data and advanced functionalities.**Increased Efficiency**: IoMT devices streamline various medical processes, making healthcare delivery more efficient and effective.**Data-Driven Decisions**: The integration of IoMT devices allows for data-driven decision-making, enhancing the accuracy and quality of medical interventions. | **Cybersecurity Risks**: The study highlights the potential entry points for cyber threats, posing significant risks to patient safety and Protected Health Information (PHI).**Underfunding**: There is a chronic underfunding of cybersecurity in healthcare, leaving the sector exposed to cyberattacks.**Complexity**: The increasing wireless connectivity of IoMT devices adds complexity to the healthcare network, making it more challenging to secure | **Risk Assessment**: The study emphasizes the importance of conducting regular risk assessments to identify and mitigate potential cyber threats.**Security Audits**: Recommends conducting regular security audits to ensure that IoMT devices and healthcare networks are secure.**Encryption**: Emphasizes the need for data encryption to protect sensitive information during transmission and storage |
| **Silvestri *et al.* (2023)**Applied Machine Learning models like BERT and XGBoost to analyze threats and vulnerabilities in healthcare. Extracted information from natural language documents to assess the severity of threats and provide effective risk management [24]. | **Advanced Threat Analysis:** The application of Machine Learning models like BERT and XGBoost enhances the ability to analyze threats and vulnerabilities in healthcare, providing a more comprehensive understanding of potential risks.**Effective Risk Management:** By extracting information from natural language documents, the study offers effective risk management strategies, ensuring that healthcare organizations can better protect sensitive data.**Improved Accuracy:** The use of advanced ML models improves the accuracy of threat detection and vulnerability assessment, leading to more reliable security measures. | **Implementation Complexity**: Integrating advanced ML models into existing healthcare systems can be complex and resource-intensive, requiring significant expertise and coordination.**Data Privacy Concerns**: Handling sensitive healthcare data raises concerns about data privacy and the ethical implications of using ML models.**Scalability Issues**: The framework may face challenges in scaling up to larger healthcare networks with diverse data sources and security needs. | **BERT (Bidirectional Encoder Representations from Transformers)**: Used for natural language processing to extract and analyze information from documents, assessing the severity of threats.**XGBoost (Extreme Gradient Boosting)**: Employed for predictive modeling to identify and prioritize vulnerabilities, enhancing risk management strategies. |
| **Rubinic *et al.* (2023)**Investigated the misuse of large language models (LLMs) in clinical pharmacology for creating bioweapons. Proposed mitigation strategies including explainable AI, ethical guidelines, and policy deviations to address ethical issues [25]. | **Enhanced Awareness**: The study brings attention to the potential misuse of large language models (LLMs) in clinical pharmacology, particularly in the creation of bioweapons.**Mitigation Strategies**: The proposed mitigation strategies, including explainable AI, ethical guidelines, and policy deviations, provide a comprehensive approach to addressing ethical issues and preventing misuse. **Ethical Framework**: The study emphasizes the importance of establishing an ethical framework to guide the development and use of AI in clinical pharmacology | **Implementation Challenges**: Implementing the proposed mitigation strategies can be complex and resource-intensive, requiring significant expertise and coordination.**Regulatory Gaps**: The study highlights existing regulatory gaps that need to be addressed to effectively manage the risks associated with AI and LLMs.**Ethical Concerns**: Despite the proposed strategies, ethical concerns related to the dual-use nature of AI and LLMs remain challenging to fully address | **Explainable AI**: Used to enhance transparency and accountability in AI systems, making it easier to understand and mitigate potential risks.**Ethical Guidelines**: Establishing ethical guidelines to ensure responsible development and use of AI in clinical pharmacology. |
| **Messinis *et al.* (2024)** Studied contemporary cybersecurity technologies using AI methods. Emphasized that machine learning and deep learning enhance the performance, speed, reliability, and effectiveness of cybersecurity measures, especially in IoMT [26]. | **Enhanced Performance:** The study highlights that machine learning (ML) and deep learning (DL) significantly enhance the performance of cybersecurity measures, making them more effective in detecting and mitigating threats.**Speed and Reliability:** ML and DL methods improve the speed and reliability of cybersecurity systems, allowing for faster detection and response to cyber threats.**Effectiveness in IoMT:** The study emphasizes the effectiveness of these AI methods in the Internet of Medical Things (IoMT), ensuring better protection of sensitive healthcare data. | **Implementation Complexity**: Integrating ML and DL into existing cybersecurity frameworks can be complex and resource-intensive, requiring significant expertise and coordination.**Data Privacy Concerns**: Handling sensitive data with AI methods raises concerns about data privacy and the ethical implications of using ML and DL models.**Scalability Issues**: The framework may face challenges in scaling up to larger networks with diverse data sources and security needs. | **Deep Learning Algorithms**: The study examines state-of-the-art DL algorithms such as Long Short-Term Memory (LSTM), Deep Belief Networks (DBN), and Convolutional Neural Networks (CNN) for anomaly detection and threat prediction.**Machine Learning Methods**: ML methods like CatBoost, LightGBM, and XGBoost are used for classifying attacks and forecasting vulnerabilities.**Anomaly Detection**: The study utilizes AI techniques to identify anomalies in IoMT security datasets, enhancing the ability to detect and respond to cyber threats. |
| **Zhan *et al.* (2024)**Identified obstacles to adopting digital information systems in healthcare. highlighted that outward attacks and technological factors were the main challenges, while employee-related factors had a lesser impact on the adoption process [27]. | **Comprehensive Analysis**: The study provides a thorough examination of the obstacles to adopting digital information systems in healthcare, offering valuable insights for future implementations.**Focus on Major Challenges**: By highlighting outward attacks and technological factors as the main challenges, the study helps prioritize areas that need the most attention and resources.**Guidance for Improvement**: The findings can guide healthcare organizations in developing strategies to overcome the identified obstacles, enhancing the adoption process. | **Complexity of Implementation**: Addressing the identified challenges, especially outward attacks and technological factors, can be complex and resource-intensive.**Potential Overlook of Minor Factors**: While the study focuses on major challenges, it may overlook minor factors that could also impact the adoption process.**Scalability Issues**: Implementing solutions to address the identified challenges may face scalability issues, particularly in larger healthcare organizations. | **Risk Assessment**: The study employs risk assessment techniques to identify and evaluate the obstacles to adopting digital information systems.**Data Analysis**: Utilizes data analysis to examine the impact of outward attacks and technological factors on the adoption process.**Predictive Modeling**: Employs predictive modeling to forecast potential challenges and develop strategies to mitigate them. |