We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

Smart Health and Cybersecurity in the Era of Artificial Intelligence

A.K.M. Jahangir Alam Majumder and Charles B. Veilleux

Abstract

The need for a transformation in providing healthcare has been recognized by organizations and captured in reports. Research into Smart Health using Artificial Intelligence (AI) could help identify the mental health of individuals by analyzing physiological data. The complexity of emotions can make it challenging for an individual to recognize they are coping with mental illness. AI could be used as an objective method in recognizing mental health crisis. This is where smart emotion could help as a Human-in-the-loop system that can reduce the time it takes for an individual to get treatment by identifying mental illness. Early treatment of mental health crises can lead to an overall reduction in damage caused by it. Further, COVID-19 has overwhelmed many healthcare systems, leading malicious actors to target them, highlighting many Cybersecurity issues. AI could aid in addressing Cybersecurity concerns to create a robust and secure Human-in-the-Loop system for mental health problems.

Keywords: COVID-19, Cybersecurity, Smart Health, Human-in-the-loop, IoT, CPS, AI

1. Introduction

Given the frequency and the intensity of healthcare-related incidents, Artificial intelligence (AI) applications and cybersecurity threats in healthcare are all the rage now [1]. Cybersecurity is the process of protecting computer systems, networks, and programs from any unauthorized access. Cyberattacks have become more sophisticated using AI to get past cyber defenses. The AI is also being used to constantly manage and secure the increasing number of healthcare Internet of Things (IoT) sensor nodes and Cyber Physical Systems (CPS) devices as they connect and disconnect from hospital networks [2]. The CPS is intelligent system consisting of cyber and physical components which is controlled and monitored by AI algorithm. With the development of smart multisensory systems, sensorial media, smart things, and cloud technologies, "Smart healthcare" is getting notable attention from academia, government, industry, caregivers, and healthcare communities [3–9]. In the recent smart health technological revolution, IoT technology playing an important role in healthcare for it's ability to predict, prevent, and intelligently control the the emerging infectious diseas like, Coronavirus (Covid-19). Also, IoT has introduced the vision of a smarter world into a reality with large datasets and services [10–13]. The AI-driven IoT has become more popular in smart healthcare system by utilizing machine learning algorithms and by providing a better understanding of healthcare information to support improved personalized healthcare during the epidemic of Covid-19 [14–16]. Also, it can support powerful

processing and storage capacity of enormous datasets from IoT sensors and actuators as well as to provide automated decision making in real-time. A very little attention is given to developing a secure affordable healthcare system while the study of AI and cybersecurity for smart healthcare have been making great innovations in the age of Covid-19. The AI-driven IoT (AIIoT) for smart healthcare has the potential to revolutionize many aspects of our healthcare industry. AI-based analytics for secure smart health infrastructure is shown in **Figure 1**.

The importance of secure transformation in medical, public health, and healthcare delivery approaches have been recognized by numerous organizations [17]. The Networking and Information Technology Research and Development (NITRD) program recently has published the Federal Health Information Technology Research and Development Strategic Framework. This framework has explained the importance of the integration between the computing, engineering, mathematics and statistics, behavioral and social science, and public health research communities to explore the essential innovation to improve the services in the healthcare system [18]. Recent significant advances in machine learning (ML), artificial intelligence (AI), deep learning, high-performance cloud computing, and the availability of new datasets make such integration achievable.

Transformative approach can help to develop computational approaches for the analysis of multilevel and multiscale personal and clinical health data to maximize the accuracy of data implications. The transformative data science, mainly focuses on science and engineering innovations by interdisciplinary teams and utilize the advance sensing methods to intuitively and intelligently collect, connect, analyze and interpret data from individuals, device, and systems. Also, this integrated and intelligent data collection will help to optimize the healthcare services. The challenges include a number of issues from data collection, synchronization, fusion, and visualization of multisensory systems, electronic health records (EHRs), and medical and consumer devices. Underlying these challenges are many fundamentals issues, such as interoperability, integration, and reuse of heterogeneous data, feature selection, optimization, uncertainty quantification, robustness, model validation and evaluation, data privacy, and most importantly physical and cybersecurity. A robust research study might help to address how predictive, rigorous models with uncertainty can be build from sensory or EHR data for validation and testing and to improve the reproducibility of model building and simulations [18].

The World Health Organization (WHO) defines Smarthealthcare as "Information and Communication Technology applications in the healthcare, including disease

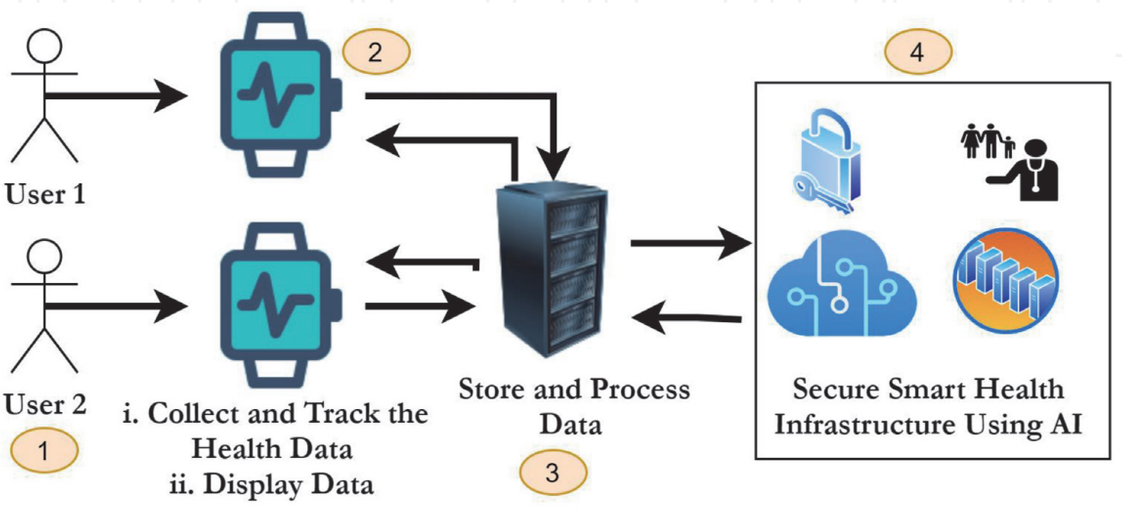

Figure 1.
AI-based Analytics for Secure Smart Health Infrastructure.

control and monitoring, education, and research". Additionally, scientists state that "Smart Healthcare" is the integration of health informatics, public health, and business applications through the internet and related AI and data mining techniques. The above mentioned techniques can provide more security and high accuracy in personalized healthcare and health informatics. Though the deep learning concept becomes popular, the scientists have rarely used this technique to predict outcomes from multisensory health data. They prefer to make the healthcare prediction using algorithm based on statistical methods and regression analysis [19–21]. In this chapter, the authors discussed the importance and challenges of using AI for cybersecurity vulnerabilities that have compromised the confidentiality, integrity, and availability of data for the affected healthcare systems in the age of Covid-19.

2. Cybersecurity for smart health

2.1 Healthcare Cybersecurity In The Age of COVID-19

Healthcare is one of the most vulnerable industries when it comes to cybersecurity. The healthcare system around the globe has become more susceptible to cyber attacks in the age of COVID-19. Many cyber-security organizations are reporting a rapid increase in cyber attacks since the start of the COVID-19 pandemic. The healthcare system, including nursing home, has always been one of the key target of cyberattacks. Recent string of attacks in several major hospitals and healthcare systems, have exposed the security vulnerabilities of most trusted healthcare institutions. The healthcare industries are at forefront of global efforts to fight the virus (COVID-19) during the pandemic. As such, this critical sector should be secure by cybercriminals, but that is not what has happened. The COVID-19 era is characterized by a steep rise in cyber attacks, from different perpetrators and for different motivations, and the healthcare sector has not been secure [22]. The smart health pipeline for data processing and security analytics using AI is shown in **Figure 2**.

Security and privacy in the healthcare industry are very crucial as they involve a patient's/user's personal information and private medical records. During the last few decades, the healthcare provider has increased the use of advanced technologies, like Artificial Intelligence (AI), machine learning techniques to secure patients' health profiles, storing data in the cloud, advanced medical devices, etc. These technological advancements have reduced the work of healthcare providers and have led to a paperless environment. But in return, the risk of cyber-attacks has increased. In most of the cases, there are no appropriate security systems installed to protect the hospital database, and the healthcare provider are often unaware of the cybersecurity threats lie in the shadows. Information Technology (IT) in

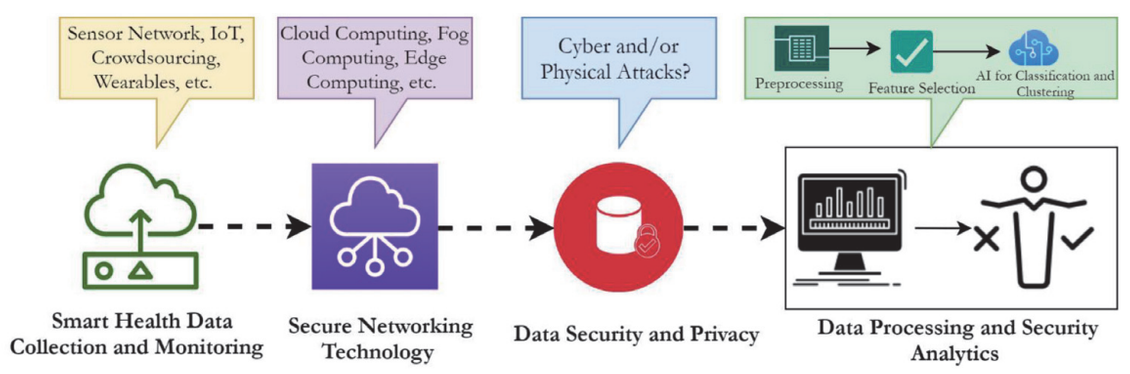

Figure 2.
Smart Health Pipeline.

healthcare systems is vulnerable to the point that it can take even several weeks before a cyberattack is acknowledged. The healthcare providers continue working with a hacked system without having any knowledge of the attacks. This could result in spending billions of dollars and affect millions of patients each year [23].

In the last few years, the healthcare industry has been exposed to several cyberattacks. The most significant cyberattacks among them are:

2.1.1 Cyberattack on UVM Health Network

The University of Vermont (UVM) Healthcare system was shut down after identifying a cyberattack on Oct. 28, 2020. The hospital was losing about $1.5 million per day, including lost revenue from postponed services and expenses needed to recover from the attack. The healthcare system was shut down for about 40 days including electronic health records (HER). More than 5000 computers were infected as they all were connected to the same network. In November, about three hundred employees were not able to work during this outage. UVM Medical Center President and COO Stephen Leffler, MD, said the health system expects the entire incident will cost more than $63 million by the time it resolves [24].

2.1.2 Ryuk and NHSD ransomware attack

On Oct. 26, 2020, an adversary attack (Ryuk ransomware) affected the network systems of six hospital systems from New York to California over 24 hours. A few hospitals self-reported IT outages due to ransomware during that time. The attackers have demanded more than $1 million from unknown hospitals. According to the New York Times, the hackers are known to set the ransom at 10% of the organization's annual income. The federal government wants the hospital systems and healthcare providers to boost protection networks, ensure all the software updates are made, back up data, monitor access to their systems closely. Ryuk has been deployed as a payload from banking. Ryuk was first introduced in August 2018 as a derivative of Hermes 2.1 ransomware. One of the key reasons the attackers target healthcare organizations to get the monetary benefits in terms of ransom. In May 2017, National Health Services (NHS) in the UK were one of the victims of the ransomware attack. Almost 200,000 computers at 16 healthcare facilities affected by the WannaCry attack at that time. Thousands of patients were suffered from the outcomes of the attack as it stop down the many vital medical equipments [25].

2.1.3 Nebraska medicine in Omaha attack

In September 2020, Nebraska Medicine first reported the outage, and the health system anticipates its computer network will remain down. The adversary incident affected the Nebraska Medicine IT system and required many patient's appointments to be postponed or rescheduled. The attack also affected the EHRs and computer systems for several other Regional Health Services because Nebraska Medicine powers their EHRs. Also, from Feb. to May 2020, there are more than 46 hospitals and health systems that had patient information exposed in a security hole at Blackbaud, a company that stores donor information for organizations, including health systems [26].

2.1.4 DDoS attack at Boston's Children Hospital

Distributed Denial of Service (DDoS) occurs when the network is overloaded and it starts denial of availability to its recipients. There are a few times the DDoS

attack happens unintentionally. But most of the time the cybercriminals created DDoS attack to get access the critical data, including the financial information of an organization. The healthcare system is one of the main targets for the hackers. In 2014, one of the most remarkable DDoS attacks targeted Boston's Children Hospital. The hospital system was attacked by DDoS when dealing with the case of parental withdrawal of a 14-year-old girl. The hospital had an about $300,000 loss to overcome the damage caused by the DDoS cyberattack [27].

2.1.5 Data breach at Montpellier University Hospital

Data breaches at the healthcare system have been rampant for the last decades as data breach is also a common types of cyberattacks. Almost all Attackers use phishing emails and manipulative web links to trick the user. The attacker will get access to the account as well as the network system when the user click on the suspicious web link receive in their email. On March 2019, the healthcare provider at the Montpellier University Medical Center found out that an outsider can access one of the employee email accounts. The employee of this medical center unintentionally clicked on a malicious link in the phishing email. As a result attacker got accessed in his/her account and as well as to the hospital network. Around 600 computers were affected due to this data breach [28]. The healthcare provider discovered that the affected account had sensitive patient information, including name, social security number, date of birth, insurance details, etc.

2.1.6 Internal threats

Besides external cybersecurity threats, healthcare providers sometimes have to face internal threats as well. These internal threats to the organizations are either due to human error or as a result of a breach of an employment contract. According to several case studies, there are three types of internal attacks: the carelessness/negligence of employee or contractor, the criminal or malicious insider, and the credential thief (imposter risk) [28].

2.2 Medjacking

Medjacking is the practice of attacking and manipulating a medical device and instrument with the intent to harm a patient. The malfunctioning of any medical instruments at hospital and/or clinic is very distressing and might have severe fatal consequences. The faulty diagnostic results from any medical instruments could lead to the wrong prescription. If any medical devices are not operating properly, it might cause harm to patients that lead to death, rather than help. Medjacking is often targeted, especially to harm influential personalities, and to damage the reputation of the healthcare organization. Artificial Intelligence (AI) can support and help to improve the security aspect of manipulating medical devices and instruments [28].

3. Artificial intelligence

3.1 How artificial intelligence helps in healthcare security and cybersecurity

Artificial intelligence (AI) can provide a device or software program the ability to interpret complex data, including images, video text, and speech, or other sounds and to work on that interpretation to achieve the goal. Since AI-driven computers are programmed to make decisions with little human intervention, some wonder if

machines will soon make the difficult decisions we now entrust to our doctors. It is important to separate fact from science fiction, because AI is already here and it is fundamentally changing medicine, according to David B. Agus, MD, a professor of medicine and engineering at the University of Southern California Keck School of Medicine and Viterbi School of Engineering.

AI has been employed in applications in various domains of healthcare including cancer research, cardiology, diabetes, mental health, identification of Alzheimer's disease, stroke-related studies, identification of cardiovascular disease, etc. Rather than robotics, AI in healthcare mainly refers to doctors and hospitals accessing vast data sets of potentially life-saving information. The recent advancement of computing power can analyze the different features from the multisensory data for predictive analytics to identify the potential health outcomes through the machine learning techniques. The artificial intelligence and machine learning techniques use statistical methods to analyze incoming sensory and network data to identify patterns and security threat and make a decision with a minimum human interaction.

3.2 AI in mobile heath (m-Health)

Mobile health (m-Health) is the employment of smartphones and mobile devices with their communication to assist healthcare. M-Health comprises a combination of mobile devices, medical sensors, and smartphones. There is plenty of research that has shown that the application of AI in healthcare systems can significantly improve the security of patient health analysis. Like, the author in [29] proposed an AI-based smartphone application for predicting heart failures and alert the users. Currently, the researchers and healthcare providers are use and apply the simple methods for generating alerts in case of emergency. But, there are a high number of false alerts generated in the present methodology. The authors of this work used predictive models to avoid the impact of these false alerts. The proposed predictive models built based on the 44 months clinical data collected from 242 patients' smartphone who had experienced a heart failure at least once. In this work, the best predictive model developed using an application of a Naïve Bayes Classifier based on integration of observing data and a set of questions from the various alerts. The author claimed that their proposed model can lower the yearly rate of false alerts for a heart patient from 28.64 to 7.8 gradually.

Another m-Health based approach for speech recognition of users who are affected with dysarthria proposed in [30]. In this work, the author showed that their approach can assist in the process of voice message generation. The Hidden Markov Model approach was employed to measure the overall proximity of a word used in a speech model and is personalized for a particular user. The Hidden Markov Models are used to build AI to estimate the unknown parameters in a mobile target moving in a define environment. The speech recognition accuracy of their methodology is only 67% based on the real life study of nine test subjects. The authors of this work showed that the difficulties in the process of communication with users decreased significantly by using their proposed technology compared to the already available methods in the market. The drawback of this approach is the lower accuracy in speech recognition hardware and need usual aid for the voice-output communication.

3.3 Internet of Things (IoT) and Cyber-Physical System (CPS) in the era of AI

Healthcare systems in hospitals/clinics are one of the key targets of attackers for carrying out Internet-of-Things (IoT) and Cyber-physical System (CPS)-focused cyberattacks. The most critical endpoints from the hospital security viewpoint are

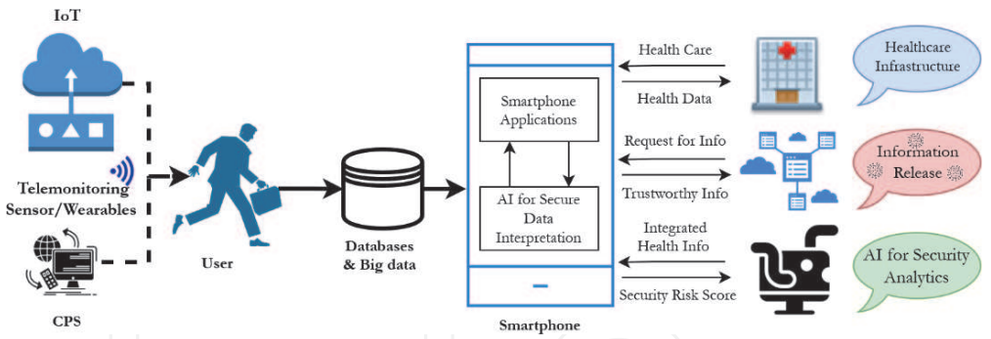

Figure 3.
AI for Smart m-Health (the workflow with IoT and CPS communicate with a smartphone via Wi-Fi or Bluetooth).

patient health monitoring, ventilation, anesthesia, infusion pumps, etc. There is increasing use of IoT in healthcare settings, including mobile devices, wearables, robots, drones, and contactless devices. IoT is enabling the control of coronavirus.

Early detection of Covid-19, isolation of infected people, and tracing possible contacts are critical to stopping the spread of the virus. IoT and CPS protocols, GPS, and Wi-Fi are providing solutions to the challenges that distance and accessibility would have posed. Using the IoT to fight virus outbreaks has been effective during Covid-19. Interconnected tech devices, such as smart thermometers to test a patient's temperature, are used to build up detailed datasets for more accurate analysis and diagnosis. Quarantine compliance is also greatly assisted by the use of IoT. By using a patient's existing smartphone or wearable devices, it is easier to ensure compliance with quarantine rules and establish patterns via track-and-trace methods.

A Cyber-Physical System (CPS) is a collection of sensors/devices interacting with each other and communicating with the physical world. Many CPS application is based on the medical devices used in smart healthcare technology. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and useability that will expand the horizon of critical application in the healthcare system with cybersecurity. The ideas in CPS-based research are being challenged by the new research concepts emerging from AI and machine learning. The integration of AI with CPS especially with real-time secure health care operation creates new research opportunities with major societal implications. The application of AI and smart m-Health with the workflow including IoT and CPS communicate with a smartphone via Bluetooth or Wi-Fi is shown in **Figure 3**.

4. Cybersecurity

4.1 Cybersecurity for AI

Artificial Intelligence (AI) and machine learning are playing an important role in cybersecurity. AI-based cybersecurity systems can provide a clear knowledge of global and healthcare industry security threats to help make critically important decisions in a critical situation. AI techniques are expected to enhance cybersecurity by assisting human system managers with automated monitoring, analysis, and responses to adversarial attacks.

The research outcomes from the integrated AI and cybersecurity can lead to an extensive change in the understanding of the basis of cybersecurity. Also, this integrated results can help to motivate and educate healthcare providers about

cybersecurity in the age of AI in an innovative way. Fundamental research in AI together with cybersecurity research might expand existing AI opportunities and resources in cybersecurity analytics and workforce development. AI relies on innovations like Machine Learning, Deep Learning, Natural Language Processing, and so forth to make it hard for malicious actors to access servers and other important data. AI has crossed many milestones and now it is turning towards cybersecurity. According to MIT, AI can detect about 85% of cyberattacks and help to secure IoT and CPS systems including the healthcare industry from cyberattacks. The prototype AI-based cybersecurity system is shown in **Figure 4**.

AI, Machine Learning (ML), and Deep Learning (DL) are overlapping and someone can easily get confused with these terminologies. The AI technique can help computers to mimic human behavior. The machine learning is a subset of AI, which give computers to automatically learn models and representation of the data sets. The deep learning is a subset of machine learning that help computers to solve multi-layer neural network complex problems. Use AI and leveraging machine learning and deep learning techniques are the smart choice to extract and analyze the sensory data from a smart IoT system. The researchers in [31] evaluate the performance of eleven famous ML and DL algorithms using six IoT related data sets. The authors of this paper showed that considering their performance evaluation matrics, including precision, recall, f1-score, accuracy, execution time, area under receiver operating characteristic curve (ROC-AUC) score, and confusion matrix, Random Forest performed better than other ML models. Also, they showed that ANN and CNN have interesting results comparing with other deep learning models.

4.2 How AI is helpful in cybersecurity

AI is changing the game for cybersecurity, analyzing massive data sets to improve response times and augment under-resourced security operations. AI and machine learning are playing a key role in cybersecurity to identify potential threats. AI can use to remove noise as well as unwanted data from any signals or data sets. Also, currently most of the security experts utilize AI to understand the cyber environment.

4.2.1 Network security

For network security in the healthcare system, AI can confidently navigate HIPAA privacy law and prevent patient data from wearable devices or public system from ending up in the hands of unauthorized personnel. The three important ways to use AI for network security are to use machine learning to detect

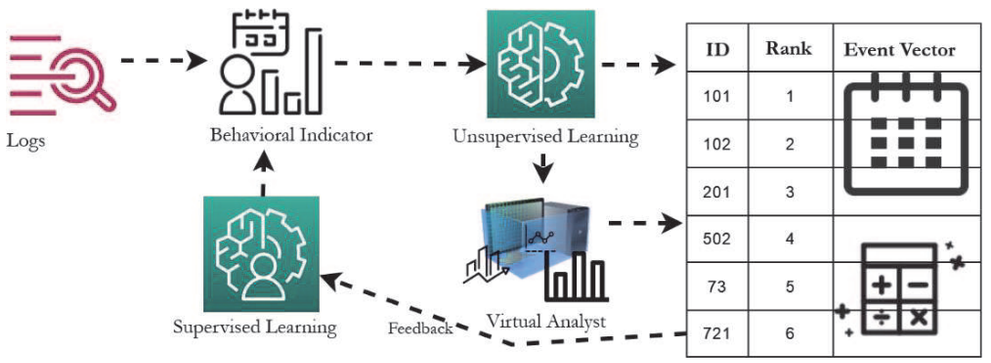

Figure 4.
AI-based Cybersecurity System.

AI-based cyberthreats, use AI to enhance human judgment, and use AI as a tool to save security policy and network architecture. AI can detect new threats based on the identification and analysis of threats before they exploit vulnerabilities in the network. Also, a human can become complacent and reliant on AI and machine learning to handle the cybersecurity of their network.

4.2.2 Faster response times

A key benefit of AI in cybersecurity is AI can immediately identify any anomalous behavior and suspected problems and prevent the healthcare systems from a potential cyber threat. The ability to detect a threat and respond to it quickly can improve the security system of any organization that costs resources and reputation. Three important strategies to improve detection and response before threats damage a critical healthcare system are managed security service, getting ahead with AI, and centralizing the response. Managed security service providers offer outsourced monitoring of security devices and systems. The cyberattack and ransomware attacks lead the healthcare industry to use AI to better and faster detect threats by recognizing patterns and anomalies. Centralization is very important as most of the healthcare industry faces a lack of centralization when dealing with a cyberattack. Human digital security specialists will even now make the approaches the needs of the episodes to be taken care of. However, it can be additionally helped by AI frameworks that consequently recommend plans for improving reactions.

4.2.3 Phishing detection and prevention

Phishing attacks are one of the most common security challenges for an individual and a company in keeping their information secure, where malicious actors attempt to convey their payload utilizing a phishing assault. AI and machine learning may assume a noteworthy job in forestalling and deflecting phishing assaults. Computer-based intelligence machine learning can recognize and follow over 10,000 dynamic phishing sources. Additionally, AI-machine learning works at filtering phishing dangers from everywhere throughout the world. Phishing attacks can have several different goals, including malware delivery, stealing money, and credential theft. Most phishing scams are designed to steal personal information. There is no limitation in its comprehension of phishing efforts to a particular geological territory. Computer-based intelligence has made it conceivable to separate between a phony site and a real one rapidly.

4.2.4 Secure authentication

Security provisioning or authentication has become a key issue in wireless networks due to their vital roles in supporting numerous services. The Physically recognizable proof in which AI used to explore the various security elements to distinguish a user could be the primary way to security verification. A smartphone can utilize the scanner for unique fingerprint and facial expression to permit for a secure login of a user. The smartphone application examines the fingerprint and facial expression to identify if the login is true. Also, AI technique can investigate the different features to verify the user authentication and allow the user to access information from any device.

4.2.5 Behavioral analytics

One of the important uses of AI in cybersecurity originates from its ability to analyze behavior. This means the machine learning calculations can learn and make

an example of your conduct by breaking down how you utilize your gadget and online stages. The use of AI in healthcare like DNA/genome research is truly captivating to read. People are involved in the behavior part of cybersecurity. Also, machine behavior plays a significant role in cyber events. AI is changing our lifestyle, including the way we live, work, and play. With more and more healthcare data being collected from multisensory system and medical instruments and being processed, predict and behavioral analytics allow to generate insight and take a necessary action.

In conclusion, AI techniques have experienced quick change and progress from being inconsequential specialized. This will help cybersecurity specialists in managing moves identified with the discovery and avoidance of cyberattacks. AI can help to detect cybersecurity dangers and advise the specialists to take proper actions. The job of AI is expanding different parts of data innovation like AI in Cybersecurity, Software Testing, and Data Security.

5. Challenges in intelligent cybersecurity

Cybersecurity is the main concern of the nation's overall cyber-physical security and economic interests. The security analysts in every organization are facing many challenges related to cybersecurity including securing federal and state confidential data. One needs to distinguish between the immediate goals and long-term goals when coming up with the long-term analysis, development, and application of AI in cybersecurity. There are a variety of ways AI can be directly applied in cybersecurity. Currently, there are immediate cybersecurity issues that need a lot of intelligent solutions. In the future, users will see the promising views of the application of fully new principles of data handling. A key application space of AI is the data management for cyber threats. AI-based systems are already getting used in several applications, like the security measures hidden within the software. However, AI will get a wider application as massive databases for healthcare systems are developed. Many technologies are usually mentioned as most of the healthcare databases are incorporating AI for cybersecurity. However, there are many different technologies that, if they reach a high level of sophistication, would bring about the creation of smarter-than-human intelligence.

6. How to improve cybersecurity for AI

The development of AI and machine learning technologies will impact cybersecurity in several ways. Cyber attackers can attack any network systems from anywhere in the world, at any time. It is noticed that cybersecurity applications have received massive technological advancement over the last few years. There are many ways to improve cybersecurity for AI, like improving cyber threat detection with machine learning, AI and machine learning plays an important role in mitigating phishing attacks, automated network security, robust behavioral analytics, etc. AI and machine learning make smarter cybersecurity possible and these emerging technologies have vast potential applications in healthcare, finance, retail, etc. There are several similar issues to deal with the question of how AI systems are secure when they are used to augment the security of the collected healthcare data and computer networks. The application of AI security solutions to respond to quickly evolving threats makes the need to secure AI itself even more pressing. It is all the more important that those algorithms be protected from interference, compromise, or misuse if we rely on machine learning algorithms to detect and protect

from cyberattacks. Increasing dependence on AI for critical functions and services will not only create greater incentives for attackers to target those algorithms, but also the potential for each successful attack to have more severe consequences.

The improvement of cybersecurity and safety for AI is one of the key challenges. The US Government has already indicated their interest in cybersecurity targeting certain types of technology, including the IoT, CPS, and voting systems. Recently, AI has become more popular and widely used technology in many different sectors including the healthcare industry. The policymakers find it increasingly necessary to consider the intersection of cybersecurity with AI. Recently, several researchers working on to reduce the possibility for adversaries to access confidential AI training data or models in healthcare systems during the era of Covid-19.

As mentioned above, one of the key security threats to AI systems is the possibility for adversaries to compromise the integrity of their decision-making processes. The way to achieve this when adversaries take the direct control of an AI system so that they can decide the outputs the system generates and the decisions it makes. An attacker might try to influence those decisions directly by delivering malicious inputs or training data to an AI model.

7. Mathematical modeling for healthcare and cybersecurity

Mathematics is one of the key components for cybersecurity data analysis. Mathematics has a direct impact on the advancement of the science of cybersecurity. Considering the complexity and dynamics of cyberspace it is essential to have a formal scientific basis for the field of cybersecurity. Mathematics plays a critical role in the construction of the science of cybersecurity.

There have been many research studies for modeling of dynamics and spread of COVID-19. Most of them are based on the Susceptible (S_i)-Exposed (E_i)-Infected (I_i)-Removed (R_i) and susceptible-infected-recovered (SIR) model as shown in **Figure 5**. Susceptible individuals might acquire the infection at a given rate when they are in contact with an infectious individual and enter the exposed disease state before they become infectious and later either recover or die.

For a given age group i, epidemic transitions can be described as,

$$S_{i,t+1} = S_{i,t} - \beta\, S_{i,t} \sum_{j=1}^{n} C_{i,j} I_{j,t}^{c} - \alpha\, \beta_{i,t} \sum_{j=1}^{n} C_{i,j} I_{j,t}^{sc} \tag{1}$$

$$E_{i,t+1} = (1-k)E_{i,t} + \beta\, S_{i,t} \sum_{j=1}^{n} C_{i,j} I_{j,t}^{c} + \alpha\beta\, S_{i,t} \sum_{j=1}^{n} C_{i,j} I_{j,t}^{sc} \tag{2}$$

$$I_{j,t+1} = \rho_i k\, E_{i,t} + (1-\gamma) I_{j,t}^{c} \tag{3}$$

$$I_{j,t+1} = (1-\rho_i) k\, E_{i,t} + (1-\gamma) I_{j,t}^{c} \tag{4}$$

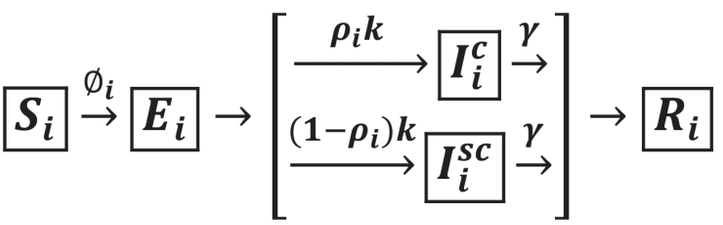

Figure 5
SEIR model for Dynamics and Spread Prediction of Covid-19 [32].

$$R_{i,t+1} = R_{i,t} + \gamma I^{c}_{j,t+1} + \gamma I^{sc}_{j,t+1} \tag{5}$$

Where,

β = Transmission rate.

$C_{i,j}$ = Contact of age group j made by age group i.

$k = 1 - e^{-}\left(\frac{1}{d_L}\right)$ = the daily probability of an exposed individual becoming infectious.

$\gamma = 1 - e^{-}\left(\frac{1}{d_I}\right)$ = the daily probability that an infected individual recovers when the average duration of infection is dI.

d_L = average incubation period.

d_I = average duration of infection.

α = infection acquired from subclinical individual.

ρ_i = the probability that an individual is symptomatic or clinical.

$1 - \rho_i$ = probability of an infected case being asymptomatic or subclinical.

I^c = an infected individual can be clinical.

I^{sc} = an infected individual can be subclinical.

$\varnothing_{i,t} = \beta \sum_j C_{i,j} I^{c}_{j,t} + \alpha\beta \sum_j C_{i,j} I^{sc}_{j,t}$ =The force of infection.

Primarily, these models were used in the past for the research of epidemic spreading with various forms of networks of transmission. The principle of AI techniques, like, Neural Networks (NN) are based on the collection of artificial neurons, without any prior knowledge, this AI technique automatically generates identification characteristics for cybersecurity.

8. Carbon footprint (gCO_2eq) and Artificial Intelligence

AI is an important factor in our daily life and an important factor in the science of the healthcare system. Deep learning (a process by which computer models are trained to identify the patterns from a data set) training requires computationally intensive computers and a large amount of power and associated carbon emission. In a report published by researchers from the University of Massachusetts Amherst estimating the amount of power required for training certain type of Artificial Neural Network (ANN) architecture emits roughly 626, 000 pounds of carbon dioxide [33]. This will get more severe during the model development phase. The proposed deep neural networks are deployed on diverse hardware platforms with different computational properties.

Researchers from MIT-IBM Watson AI Lab introduced a novel AI system "Once-for-all network" with improved computational efficiency and with a smaller carbon footprint. In their approach, the system, train a large neural network comprising of many different sizes subnetworks and a large number of IoT devices connected to the network. All the subnetworks used in the system can be tailored to diverse hardware platforms without retrain them. In their work, the authors estimate that the computer-vision model process will require $\frac{1}{1300}$ the carbon emission compared to the existing neural architecture search approaches. Also, the approach reduces the interference time with a minimum of 1.5–2.6 times [33].

Another approach for tracking and predicting the energy and carbon footprint of training deep learning models is explained in [34]. The tool "Carbontracker" is used to report energy and carbon footpring alongside of performance metrics of model development and training. In this work, to predict the accuracy on reducing the carbon footprint, the authors experimentaly evaluate the tool on different convolutional neural network (CNN) architectures and healthcare data sets.

9. Future directions

Technology is changing continuously, and it is important to stay on the cutting edge. In the future, incorporating hybrid software would be a good idea to secure the health data. Cybersecurity experts should intelligently manage the system since AI and machine learning are still susceptible to attacks. It is recommended that in the future data governance and compliance strategies should be a top priority with more security and privacy legislation on the horizon. Many cybersecurity applications can be made easier and more efficiently with machine learning algorithms. In the future, this technology will lighten the weight of a heavy cybersecurity workload and will reduce human error.

That same reduction in human error is also applicable to health diagnoses. Medical errors, some of which are incorrect diagnoses, may result in approximately 251,000 deaths every year according to [35]. Additionally, many more die every year because they do not get treatment quickly enough. Healthcare systems that incorporate AI into the diagnosis process, as well as the smart health sector, could see a drop in these deaths due to the AI more accurately diagnosing a patient, as well as identifying the problem sooner.

10. Conclusion

Artificial Intelligence is fast, growing field with broad applications. Recent cybersecurity events that targeted healthcare systems have highlighted cybersecurity vulnerabilities that have compromised the confidentiality, integrity, and availability of data for the affected institutions. Further, these events have shown that even with care, it only takes one slip up to cost a business or organization millions of dollars and several years to resolve the issue. Additionally, the COVID-19 pandemic has shown the need for improvements in the healthcare sector that can make diagnoses more accurate and more efficient. One proposed approach is to integrate AI into both cybersecurity and healthcare. AI is already used in the medical field to diagnose many types of cancer, as well as many other illnesses. Further integration of AI into the smart health field can lead to quicker treatment, as well as make the diagnosis process more efficient. AI is also already finding use in the cybersecurity field to detect threats or to help aid experts in identifying and dealing with threats. Continued integration of AI in the cybersecurity field will lead to more refined, and robust systems that are capable of dealing with ever-changing cyber threats.

Acknowledgements

We would like to thank the Office of Sponsored Awards and Research Support at USC Upstate for the partial funding of this project under the grant no. UP000-981350-A001-101. We would also like to thank the anonymous reviewers for reviewing earlier drafts of this chapter.

Conflict of interest

The authors declare no conflict of interest regarding this chapter.

IntechOpen

IntechOpen

Author details

A.K.M. Jahangir Alam Majumder* and Charles B. Veilleux
Division of Mathematics and Computer Science, University of South Carolina Upstate, Spartanburg, SC, USA

*Address all correspondence to: majumder@mailbox.sc.edu

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Healthcare Cybersecurity- the impact of AI, IoT-related threats and recommended approaches" by Richard Staynings, Chief Seurity Strategist, Cylera. September 18, 2019. https://www.healthcareitnews.com/news/asia-pacific/healthcare-cybersecurity-impact-ai-iot-related-threats-and-recommended-approaches.

[2] McGee, Timothy Matthew, "Evaluating The Cyber Security In The Internet Of Things: Smart Home Vulnerabilities" (2016). West Point ETD. 6. https://digitalcommons.usmalibrary.org/faculty_etd/6

[3] Jacob Rodrigues M, Postolache O, Cercas F. Physiological and Behavioral Monitoring Systems for Smart Healthcare Environments: A Review. Sensors (Basel). 2020 April 12; 20(8): 2186. Doi:10.3390/s20082186. PMID: 32290639; PMCID: PMC7218909.

[4] Gope P., and Hwang T., "BSN-Care: A Secure IoTBased Modern Healthcare System Using Body Sensor Network," IEEE Sensors Journal, vol. 16, no. 5, pp. 1368–1376, 2016.

[5] Zhu N., Diethe T., Camplani M., Tao L., Burrows A., Twomey N., Kaleshi D., Mirmehdi M., Flach P., and Craddock I., "Bridging e-Health and the Internet of Things: The SPHERE Project," IEEE Intelligent Systems, vol. 30, no. 4, pp. 39–46, 2015

[6] Majumder A. J., Dedmondt J. W., Jones S. and Asif A. A., "A Smart Cyber-Human System to Support Mental Well-Being through Social Engagement," *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC),* Madrid, Spain, 2020, pp. 1050-1058, doi: 10.1109/COMPSAC48688.2020.0-134.

[7] Chang S. H., Chiang R. D., Wu S. J., and Chang W. T., "A Context-Aware, Interactive M-Health System for Diabetics," IT Professional, vol. 18, no. 3, pp. 14–22, 2016.

[8] Pasluosta C. F., Gassner H., Winkler J., Klucken J., and Eskofier B. M., "An emerging era in the management of Parkinson's disease: Wearable technologies and the internet of things," IEEE Journal of Biomedical and Health Informatics, vol. 19, no. 6, pp. 1873–1881, 2015.

[9] Arcadius T. C., Gao B., Tian G., and Yan Y., "Structural Health Monitoring Framework Based on Internet of Things: A Survey," IEEE Internet of Things Journal, vol. PP, no. 99, p. 1, 2017.

[10] Ahad A, Tahir M, Aman Sheikh M, Ahmed KI, Mughees A, Numani A. Technologies Trend towards 5G Network for Smart Health-Care Using IoT: A Review. Sensors (Basel). 2020;20 (14):4047. Published 2020 Jul 21. doi: 10.3390/s20144047

[11] 2019 Global Health Care Outlook Shaping the Future—Deloitte. [(accessed on 10 June 2020)]; Available online: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-hc-outlook-2019.pdf.

[12] Liu X., Jia M., Zhang X., Lu W. A novel multichannel Internet of things based on dynamic spectrum sharing in 5G communication. *IEEE Internet Things J.* 2018;**6**:5962–5970. doi: 10.1109/JIOT.2018.2847731.

[13] Li D. 5G and intelligence medicine—How the next generation of wireless technology will reconstruct healthcare? *Precis. Clin. Med.* 2019;**2**:205–208. doi: 10.1093/pcmedi/pbz020.

[14] Chen J, See KC "Artificial Intelligence for COVID-19: Rapid Review" J Med Internet Res 2020;22 (10):e21476

[15] Yassine HM, Shah Z. How could artificial intelligence aid in the fight against coronavirus? Expert Rev Anti Infect Ther 2020 Jun 29;18(6):493-497.

[16] Mashamba-Thompson TP, Crayton ED. Blockchain and Artificial Intelligence Technology for Novel Coronavirus Disease-19 Self-Testing. Diagnostics (Basel) 2020 Apr 01;10(4): 198.

[17] Institute of Medicine (US) Committee on Assuring the Health of the Public in the 21st Century. The Future of the Public's Health in the 21st Century. Washington (DC): National Academies Press (US); 2002. 5, The Health Care Delivery System. Available from: https://www.ncbi.nlm.nih.gov/books/NBK221227/

[18] National Science Foundation (NSF)- "Smart Health and Biomedical Research in the Era of AI and Advanced Data Science", https://www.nsf.gov/pubs/2021/nsf21530/nsf21530.htm

[19] Lin SH, Chen MY. [Artificial Intelligence in Smart Health: Investigation of Theory and Practice]. Hu Li Za Zhi. 2019 Apr;66(2):7-13. Chinese. doi: 10.6224/JN.201904_66(2).02. PMID: 30924509.

[20] Gopal G, Suter-Crazzolara C, Toldo L, Eberhardt W. Digital transformation in healthcare - architectures of present and future information technologies. Clin Chem Lab Med. 2019 Feb 25;57(3):328-335. doi: 10.1515/cclm-2018-0658. PMID: 30530878.

[21] Kamel Boulos MN, Peng G, VoPham T. An overview of GeoAI applications in health and healthcare. Int J Health Geogr. 2019 May 2;18(1):7. doi: 10.1186/s12942-019-0171-2. PMID: 31043176; PMCID: PMC6495523.

[22] Jeffery S., "Healthcare Cybersecurity in the Age of Covid-19: A Once-in-a-Lifetime Level of Distraction." Disaster Recovery Journal, November 2020.

[23] Zeina R., Marco A., Abdel-Badeeh S., "Machine Learning Approaches in Smart Health" 8th International Congress of Information and Communication Technology, ICICT 2019. Procedia Computer Science 154 (2019) 361–368.

[24] The University of Vermont (UVM) Health Network Cyberattack. https://www.uvmhealth.org/uvm-health-network-cyber-attack

[25] "Six hospital ransomware attacks in 24 hours prompts US advisory: 8 things to know" Laura Dyrda (Twitter) - Thursday, October 29th, 2020

[26] Nebraska Medicine reverts to paper records during computer network outage: 4 details. Laura Dyrda (Twitter) - Tuesday, September 22nd, 2020

[27] DDoS Case Study: Boston's Children's Hospital DDoS attack Mitigation. https://www.radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/ Cybersecurity & Healthcare During COVID-19

[28] Cybersecurity and Healthcare During Covid-19 by Susan Alexandra on April 2020.

[29] Larburu, N., Artetxe, A., Escolar, V., Lozano, A., and Kerexeta, J. "Artificial intelligence to prevent mobile heart failure patients decompensation in real time: monitoringbased predictive model," Mobile Information Systems, vol. 2018, Article ID 1546210, 11 pages, 2018.

[30] Hawley, M. S., Cunningham, S. P., Green, P. D. et al., "A voiceinput voice-output communication aid for people with severe speech impairment," IEEE Transactions on Neural Systems and

Rehabilitation Engineering, vol. 21, no. 1, pp. 23–31, 2013.

[31] Vakili, M., Ghamsari, M., & Rezaei, M. (2020). Performance Analysis and Comparison of Machine and Deep Learning Algorithms for IoT Data Classification. arXiv preprint arXiv: 2001.09636.

[32] Kiesha P., Yang L., Timothy W. R., Adam J. K., Rosalind M. E., Nicholas D., "The effect of control strategies to reduce social mixing on outcomes of the COVID-19 epidemic in Wuhan, China: a modelling study," Centre for the Mathematical Modelling of Infectious Diseases COVID-19 Working Group. March 25, 2020.

[33] https://news.mit.edu/2020/artificial-intelligence-ai-carbon-footprint-0423.

[34] Lasse F., Benjamin K., Raghavendra S., "Carbontracker: Tracking and Predicting the Carbon Footprint of Training Deep Learning Models" ICML Workshop on "Challenges in Deploying and monitoring Machine Learning Systems", 2020.

[35] Anderson JG, Abrahamson K. Your Health Care May Kill You: Medical Errors. Stud Health Technol Inform. 2017;234:13-17. PMID: 28186008.