NANOTECHNOLOGICAL TRENDS IN MEDICAL IMAGE SECURITY AND AUTHENTICATION

Abstract

Medical imaging has an important place in effective diagnosis and treatment. Picture archiving and communication system (PACS) serves as a central repository for medical images and offers easy acceptance, transfer, display, storage, and digital processing of images. PACS deals with medical information systems, and medical devices, and also engages health professionals both inside and outside the healthcare system (Cokke et al., 2003). This complexity may generate exposure chances for maliciousness and results in security requirements that are sometimes insufficient or inadequate. Sometimes, medical images are exchanged among physicians, consultants, and healthcare institutions in order to facilitate successful consultation and to provide appropriate healthcare services. It also involves the use of telemedicine that rely on biomedical sensors, Internet of Things (IOT) and Internet to provide continuous quick, efficient, healthcare services in a cost-effective manner. The privacy of healthcare information must be on top consideration for any future e-health system and can't be compromised, but due to extensive use of computers and the internet it is quite challenging (Maksimović et al., 2017).

To support the patient's care, and to protect the health information in a variety of electronic systems from cyber-attacks there is a requirement to follow the federal mandates issued by HIPAA (Health Insurance Portability and Accountability Act, It is aimed at protecting the personal data of patients from public access) and security-related guidelines such as DICOM (Digital Imaging and Communications in Medicine, defines the image format and

Authors

Simran Raj
Shobhit Institute of Engineering and Technology
(Deemed to be University)
Meerut, Uttar Pradesh, India

Vipin Dhiman
Shobhit Institute of Engineering and Technology
(Deemed to be University
Meerut, Uttar Pradesh, India

Pratishtha
Shobhit Institute of Engineering and Technology
(Deemed to be University)
Meerut, Uttar Pradesh, India

Rakhi Bhardwaj
Shobhit Institute of Engineering and Technology
(Deemed to be University)
Meerut, Uttar Pradesh, India

transfer protocol for medical images and related data) and HL7 (Health Level 7, specifies messages for transmitting patient information, orders, and reports) (Mohammed et al., 2017). As well as different security measures methods such as encryption of data, digital signature, micro-segmentation, multifactor authentication, watermarking and PMA (Privileged Access Management, safeguard individual id with special access), VNA (Vendor Neutral Archives, it store medical images in a standard format and interface for access) may be utilized to secure the medical images (Paudel,2019). This chapter specifically addresses the challenges in medical image security and methods to protect the images from cyber challenges.

Keywords: Medical imaging, PACS, Telemedicine, Cyber-challenges, Cyber-security, Security Measures and methods.

I. HEALTHCARE AND MEDICAL IMAGES SECURITY

Medical imaging has an important place in effective diagnosis and treatment. Picture archiving and communication system (PACS) serves as a central repository for medical images and offers easy acceptance, transfer, display, storage, and digital processing of images. PACS deals with medical information systems, and medical devices, and also engages health professionals both inside and outside the healthcare system. This complexity may generate exposure chances for maliciousness and results in security requirements that are sometimes insufficient or inadequate. Sometimes, medical images are exchanged among physicians, consultants, and healthcare institutions in order to facilitate successful consultation and to provide appropriate healthcare services. It also involves the use of telemedicine that rely on biomedical sensors, Internet of Things (IOT) and Internet to provide continuous quick, efficient, healthcare services in a cost-effective manner. The privacy of healthcare information must be on top consideration for any future e-health system and can't be compromised, but due to extensive use of computers and the internet it is quite challenging To support the patient's care, and to protect the health information in a variety of electronic systems from cyber-attacks there is a requirement to follow the federal mandates issued by HIPAA (Health Insurance Portability and Accountability Act, It is aimed at protecting the personal data of patients from public access) and security-related guidelines such as DICOM (Digital Imaging and Communications in Medicine, defines the image format and transfer protocol for medical images and related data) and HL7 (Health Level 7, specifies messages for transmitting patient information, orders, and reports). As well as different security measures methods such as encryption of data, digital signature, micro-segmentation, multifactor authentication, watermarking and PMA (Privileged Access Management, safeguard individual id with special access), VNA (Vendor Neutral Archives, it store medical images in a standard format and interface for access) may be utilized to secure the medical images. This chapter specifically addresses the challenges in medical image security and methods to protect the images from cyber challenges .

1. **Medical Imaging:** Medical imaging used to produce images of the whole body or a part of the body to evaluate for various clinical objectives, medical procedures and diagnosis of the disease as well as desirable to study the anatomy and the physiology of the human body. In broader form, medical imaging played central role in healthcare sector and incorporates photography, microscopy, ultrasonography, radiography, Computed Tomography (CT), Magnetic Resonance Imaging (MRI) and nuclear medicine used for research, diagnosis, therapeutic purposes that confirms, assess and document the course of many diseases and response to treatment.

   Several macroscopic and microscopic structures can be evaluated using photomacroscopy/ using camera (film camera, digital camera) and microscope. Photomacroscopy used to capture the macro or large structures whereas microscopy is the art and science of taking the photographs of the histological slides or sections taken under a microscope. There are different types of microscopes such as Light microscope (Simple, Compound, Dissecting and Stereo microscope), Comparison microscope, Inverted microscope, Surgical microscope, Digital microscope and Electron microscope (Transmission and Scanning electron microscope) to evaluate the microscopic structures.

While a noninvasive method called ultrasonography is utilised to diagnose internal organs. Without requiring an incision, it is helpful to see inside the body to see whether certain organs or tissues (such the bladder, uterus, kidney, and ovaries) are healthy or ill. There are different types of ultrasound depending on the application, including 2D, 3D, 4D ultrasound, Doppler ultrasound, Color Doppler, Power Doppler, Spectra Doppler, and Continuous Wave Doppler. Another noninvasive method is X-ray, which creates a latent image of the body's interior structures on an X-ray film using a little quantity of ionising or non-ionizing radiation (X-rays) from an X-ray machine (Projectional radiography). It generates 2D images of the organ and can be used to diagnose a number of illnesses, including cancer, breast tumours, bone fractures, and tuberculosis. While a computed tomography (CT) scan produces more detailed 3D images while using a larger dose of X-rays. In order to obtain 3D images of internal organs another technique Magnetic Resonance Imaging (MRI) is used for painless, non-invasive diagnosis. Imaging technique uses a powerful magnetic fields and radio waves to create a 3D image of internal organs of the body. Radiography uses radiation, but MRI does not. PET (Positron Emission Tomography) is another 3D functional imaging technique which demonstrates the physiological activities of tissues and organs of the body using a radiotracer. The route of administration (oral, venous or nasal) of the radiotracer depends on the tissue or organ of interest. The injected radiotracer concentrates within a tissue which has been displayed on a computer as a 3D image. The machine is similar to CT and MRI. Modern PET scan images can be combined with CT or MRI scans to create a unique view. PET scan is majorly used in the study and diagnosis of tumors and disorders associated with the brain and heart.

The above-mentioned diagnostic imaging techniques provide detailed anatomical and physiological images of the body to ease detection, diagnosis and treatment of different ailments. Health laboratory technologist and radiographers (registered Allied Health Professionals) primarily create and interpret images from microscope, ultrasound, radiograph (such as CT and PET) and MRI etcs **(Aziz et. al., 2020).** Radiologists and other physicians assist in diagnosing and treating patients based on the interpretation of the radiographer/technologist. Medical imaging has a wide range of uses in personalised medicine, including the diagnosis of cardiovascular disease, cancer, degenerative diseases, infectious diseases, paediatric illnesses, diagnostic radiopharmaceuticals, and interventional radiology **(Friedenberg et. al., 2000).**

In this pandemic of Coronavirus disease 2019 (COVID-19), a vast proportion of healthcare resources, including imaging tools, have been dedicated to the management of affected patients. The standard of care and resource allocation in health centers have changed throughout time as a result of the frequent reports of disease complications and unidentified presentations**(Mbunge et. al., 2022).** This widespread utility of imaging modalities calls for a deeper understanding of potential radiologic findings in this disease and identifying the most compatible imaging protocol with safety precautions**(Varadarajan et. al., 2021).** Although initially used for respiratory tract evaluation, imaging modalities have also been used for cardiovascular, neurologic, and gastrointestinal evaluation of patients with COVID-19**(Long et. al., 2022)**. In order to store, access, transfer and manage images and digital reports in DICOM (Digital Imaging and Communications in Medicine) format; RIS (Radiology Information System). PACS (Picture Archiving and Communication System) serves as digital medical

databases**(Oakley et. al., 2003)**. The RIS is an integral part of the Health Information System (HIS) and shares patient registration and order entry modules with other systems connected to the HIS**(Brown et. al., 2003)**. RIS also includes chronological index of patient activity, film jacket tracking system, report generating system, and an electronic physician sign-off**(Mun et. al., 1988).** The HIS/RIS events which produce information required by a PACS include the registration of new patients into the radiology department (including modification to patient demographics), the creation of new radiology orders, modifications to orders and cancellations of the orders, and the generation of radiology reports, from preliminary to approved status**(Levine et. al., 2003).**

2. **Picture Archiving And Communication System (Pacs):** PACS stands for Picture Archiving and Communication System. It is a technology used in the healthcare industry to manage medical images, such as X-rays, CT scans, MRIs, and ultrasounds. PACS acts as a central storage location where these images are stored digitally, making it easier for healthcare professionals to access, share, and process the images **(Cokke et al., 2003, Shini et. al., 2012).** PACS allows archiving of medical images in a digital format. Instead of storing physical film or printed images, the system stores images electronically, eliminating the need for physical storage space and making it easier to manage large volumes of images. PACS facilitates the communication and sharing of medical images between healthcare providers. It enables healthcare professionals to quickly and securely transmit images to other specialists for consultation or review, regardless of their physical location. This capability is particularly beneficial in situations where timely collaboration is crucial, such as emergency cases or consultations with remote experts. It provides a user-friendly interface for healthcare professionals to view and analyze medical images. The system offers advanced tools and functionalities for manipulating and enhancing the images, enabling clinicians to better visualize and interpret the diagnostic information. This digital viewing capability enhances efficiency and accuracy in the diagnosis and treatment planning processes. It offers a centralized storage solution for medical images, eliminating the need for physical filing and retrieval systems. Images can be securely stored and easily retrieved whenever needed, saving time and effort. PACS systems often incorporate data backup and disaster recovery mechanisms to ensure the integrity and availability of images over the long term. It can integrate with electronic health record systems, allowing medical images to be seamlessly linked to patient records. This integration enhances the accessibility and continuity of patient information, enabling healthcare providers to have a comprehensive view of a patient's medical history, including their diagnostic images. PACS simplifies the management and utilization of medical images, improving workflow efficiency, collaboration among healthcare professionals, and ultimately enhancing patient care**(Allen et. al., 2018).**

3. **Health Insurance Portability and Accountability Act:** The Health Insurance Portability and Accountability Act (HIPAA) include federal mandates and security-related guidelines that aim to protect the privacy and security of health information, including medical images. HIPAA Privacy Rule sets standards for the protection of individually identifiable health information (PHI) **(Kutkat et. al., 2003)**. It establishes the rights of patients over their health information and outlines the obligations of healthcare providers, known as covered entities, and their business associates regarding the privacy and security of PHI **(Bari et. al., 2019).** HIPAA Security Rule complements the Privacy Rule by establishing standards for the protection of electronic PHI (ePHI). It requires covered entities and their

business associates to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI**(Miaoulis et. al., 2013).**This includes assessing risks related to the TCP/IP transfer of medical images. This may involve implementing security controls, policies, and procedures to address vulnerabilities and protect against cyber attacks**(Evans et. al., 2016).** It is important for healthcare organizations to understand and comply with HIPAA and its security-related guidelines to protect medical images and other forms of health information. Compliance with HIPAA helps ensure the privacy, security, and confidentiality of patient data, including medical images, and helps mitigate the risks of cyber attacks and unauthorized access. Organizations should regularly assess and update their security measures to align with evolving threats and best practices in healthcare information security **(Watzlaf. et. al., 2017)**.

4. **HL7 (Health Level Seven):** HL7 is a set of international standards for the exchange, integration, sharing, and retrieval of electronic health information. It specifies messages and protocols for transmitting various types of healthcare data, including patient information, orders, and reports. HL7 messages are used to facilitate communication between different healthcare systems and applications, allowing for the seamless exchange of information**(Begoyan et. al., 2007).** These messages follow a specific structure and format defined by the HL7 standard. The messages contain data elements that represent different aspects of patient information, such as demographics, clinical observations, laboratory results, medical orders, and more. HL7 messages can be transmitted over various communication protocols, including TCP/IP, to enable interoperability and data exchange between different healthcare systems, such as electronic health record (EHR) systems, laboratory systems, radiology systems, and more**(Rea et. al., 2012)**. The HL7 standard provides a framework for structuring messages and defines a wide range of message types and segments to support different use cases and healthcare workflows**(Snelick et. al., 2007).** The standard also includes guidelines for data encoding, message sequencing, and handling exceptions. HL7 messages, healthcare organizations can achieve better integration and interoperability of their systems, improving the exchange of patient information, orders, and reports across different healthcare settings and applications. This helps streamline processes, reduce manual data entry, and enhance the accuracy and efficiency of healthcare information exchange**(Iroju et. al., 2013).**

5. **DICOM Standards:** ACR-NEMA, also known as DICOM (Digital Imaging and Communications in Medicine), has indeed defined various transfer syntaxes for encapsulating encoded pixel data, including compressed data formats. ACR-NEMA, which later evolved into DICOM, was an earlier version of the standard before it was extended and standardized globally**(Clunie et. al., 2000).** It defines a comprehensive framework for medical imaging and communication, including the representation, storage, transmission, and management of medical images and related data. DICOM, stands for Digital Imaging and Communications in Medicine, is the standard used for managing, storing, printing, and transferring medical imaging data. It is the prevalent standard in the healthcare industry for the communication and exchange of medical images and related information. DICOM defines a set of protocols, data formats, and network communication standards that ensure interoperability between different medical imaging devices, systems, and software. It specifies the rules for formatting and

organizing medical images and associated data, such as patient information, study details, and imaging parameters.

DICOM defines the acceptable formats for medical image interchange. It specifies the structure and encoding of images to ensure consistency and compatibility across different systems**(Clunie et. al., 2021).** This allows medical images acquired from different devices or vendors to be exchanged and interpreted accurately. DICOM provides a standard communication protocol for transmitting medical images and associated data between different systems. It ensures seamless interoperability by defining network services, such as query/retrieve, store, print, and worklist management, which enable healthcare professionals to access and share medical images efficiently**(Seeram et. al., 2019).** DICOM incorporates mechanisms for maintaining data integrity and security during image transmission and storage. It supports encryption and authentication to protect patient privacy and prevent unauthorized access to sensitive medical information**(Chenthara et. al., 2019).** DICOM includes standardized metadata attributes that capture important information about the patient, imaging procedure, and acquisition parameters. This metadata facilitates proper interpretation and analysis of medical images**(Kondylakis et. al., 2022).** Additionally, DICOM enables structured reporting, allowing for standardized and structured documentation of imaging findings and interpretations. DICOM is closely associated with PACS and EHR systems. It allows for the seamless integration of medical images and associated data into these systems, enabling efficient storage, retrieval, and access of images within the healthcare organization**(Fanni et. al., 2022)**. This integration enhances the continuity of patient care and supports comprehensive medical record-keeping. By adhering to the DICOM standard, healthcare facilities can ensure compatibility and interoperability between different imaging devices, systems, and software, leading to improved communication, streamlined workflows, and enhanced patient care **(Kalra et. al., 2006)** DICOM has indeed been widely used in the healthcare sector since its introduction in 1993, and it played a crucial role in the transition from film-based workflows to fully digital workflows in radiology and other medical imaging disciplines. One of the key strengths of DICOM is its ability to facilitate the exchange of medical images and associated information through various means, including networks and physical media**(Herrmann et. al., 2018).**This flexibility allows medical facilities to share images across different systems and locations, promoting collaboration and remote consultations among healthcare professionals**(Luff et. Al., 1998)**. DICOM recognizes the unique characteristics and requirements of different imaging modalities, such as X-ray, CT, MRI, ultrasound, and nuclear medicine. It provides a framework that accommodates the specific data formats, acquisition parameters, and image characteristics of each modality**(Thrall et. al., 2017).**This flexibility enables seamless integration of various imaging devices into a unified imaging environment, ensuring interoperability and consistent data representation**(Joshi et. al., 2011).** By establishing a common language for data items, DICOM enables healthcare providers to accurately interpret and share medical images and related information(Iroju et. al., 2013). It defines a standardized set of metadata attributes that capture essential details about the patient, imaging procedure, acquisition settings, and image characteristics. This standardization promotes consistency, improves communication, and enhances the quality and reliability of image interpretation**(Shur et. al., 2021)**. Furthermore, DICOM's support for various physical media, such as CDs and DVDs, allows for the distribution of medical images on portable

storage devices**(Maksimović et al., 2017, Mohammed et al., 2017, Paudel,2019, Constantinescu et. al., 2013).** DICOM's ability to accommodate the unique features of different imaging modalities, establish a common language for data items, and enable image exchange through networks and physical media has been instrumental in the successful transition to digital workflows in radiology and other medical imaging disciplines. It has revolutionized the way medical images are managed, shared, and interpreted, leading to significant improvements in patient care and clinical efficiency **(Ventola et. al., 2014)**.

II. IMAGE COMPRESSION

The standard encompasses a wide range of aspects related to medical imaging, including the encapsulation and handling of compressed data**(Liu et. al., 2017).** The transfer syntaxes specified by ACR-NEMA/DICOM describe the format and rules for encoding and encapsulating pixel data within the DICOM framework. These transfer syntaxes allow the representation of both uncompressed and compressed medical images, enabling interoperability and exchange of images across different systems**(Godinho et. al., 2014).** Some of the commonly used compression formats specified by ACR-NEMA/DICOM include JPEG, JPEG-LS, and JPEG-2000, among others. These formats provide options for both lossy and lossless compression, depending on the specific requirements of the medical image and the desired balance between image quality and storage efficiency**(Clunie et. at., 2016).** The transfer syntaxes specified by the standard provide a framework for interoperability and facilitate the integration of compressed image data into the broader DICOM ecosystem**(Gorman et. at., 2023).**

1. **Run Length Encoding (RLE):** RLE is a simple compression technique that replaces consecutive repeated data values with a count and a single instance of the value. While RLE can be used for general data compression, it is not typically used for medical images**(Arora et. at., 2014).**

2. **JPEG (Joint Photographic Experts Group):** JPEG is a widely used standard for lossy compression of images. It is commonly used for compressing photographic and natural images. **(Fitriya et. al., 2016).** However, in medical imaging, other formats are often preferred due to the need for lossless or near-lossless compression.

3. **JPEG-LS:** JPEG-LS is an image compression standard that provides lossless and near-lossless compression specifically designed for medical imaging. It offers better compression ratios than RLE or traditional JPEG for medical images while maintaining high image quality**(Haddad et. al., 2017).**

4. **JPEG-2000:** JPEG-2000 is an image compression standard that supports both lossless and lossy compression. It offers improved compression efficiency compared to JPEG, making it suitable for medical imaging applications where high-quality images are required with reduced storage requirements **(Skodras et. al., 2001).**

5. **JPIP (JPEG 2000 Interactive Protocol):** JPIP is a network communication protocol that enables efficient interactive access and streaming of JPEG-2000 compressed images. It

allows selective transmission of image regions or resolutions, making it suitable for remote viewing and telemedicine applications**(Memon et. al., 2017).**

6. **MPEG2 (Moving Picture Experts Group-2):** MPEG2 is a standard primarily used for compressing video content. It is commonly used in broadcasting, DVDs, and some medical imaging applications that involve video data**(Weigand et. al., 2003).**

7. **MPEG-4 AVC/H.264:** MPEG-4 AVC, also known as H.264, is a widely used video compression standard. It offers excellent video quality at lower bit rates, making it suitable for video transmission and storage in medical imaging applications such as telemedicine and surgical video recording **(Malindi et. al., 2011).**

III. COMMUNICATION FRAMEWORK

DICOM does employ the TCP/IP (Transmission Control Protocol/Internet Protocol) suite as the underlying communication protocol for interacting between systems. TCP/IP provides a reliable and widely adopted communication framework that enables secure and efficient transmission of DICOM messages over networks**(Voosberg et. al., 2008)**. DICOM utilizes the TCP/IP protocols as the underlying communication mechanism for transmitting medical images and associated data over networks. DICOM messages are typically encapsulated within TCP/IP packets, allowing them to be transmitted reliably across different network infrastructure. The use of TCP/IP in DICOM ensures the secure and efficient transfer of medical images, as TCP provides mechanisms for error detection, retransmission of lost packets, and flow control. IP handles the addressing and routing of the packets, allowing them to be transmitted across local networks and the internet**(Wang et. al., 2012).**

By leveraging TCP/IP, DICOM enables the seamless exchange of medical images and information between different healthcare systems, departments, and institutions, regardless of their physical locations. This facilitates remote consultations, telemedicine applications, and the integration of imaging data into electronic health record (EHR) systems. DICOM and TCP/IP are complementary technologies in the field of medical imaging. DICOM defines the standard for image communication and data format, while TCP/IP provides the reliable network connectivity and transmission mechanism for DICOM messages over networks**(Majumdar et. al., 2007).**

1. **Cyber attacks and Security Challenges:** The TCP/IP transfer of medical images is not immune to cyber attacks, and healthcare organizations must be aware of potential threats and take necessary measures to mitigate risks**(Chantzis et. al., 2021).**

2. **Man-in-the-Middle (MitM) Attacks:** In a MitM attack, an attacker intercepts the communication between two parties and can eavesdrop, modify, or inject malicious content into the data being transferred. This can compromise the confidentiality and integrity of medical images during transmission**(Papaioannou et. al., 2022).**

3. **Data Interception:** Attackers may attempt to intercept the transmission of medical images to gain unauthorized access to sensitive patient data. This can be achieved through techniques such as packet sniffing or unauthorized access to network infrastructure **(Yaacoub et. al., 2020).**

4. **Data Modification:** Attackers may tamper with the medical images during transmission, altering the integrity and authenticity of the data. This can lead to misdiagnosis, incorrect treatment decisions, or patient safety risks**(Eichelberg et. al., 2020).**

5. **Denial-of-Service (DoS) Attacks**: DoS attacks aim to disrupt the availability and accessibility of medical image transfer services. By overwhelming the network or server infrastructure with excessive traffic or exploiting vulnerabilities, attackers can render the system unusable for legitimate users **(Kumar et. al., 2016).**
6. **Malware Attacks:** Malware, including ransomware, can infect the network or devices involved in the TCP/IP transfer of medical images. Once infected, the malware can encrypt, modify, or steal the medical images, disrupting the operations and compromising patient data**(Alsubaei et. al., 2013).**

7. **Unauthorized Access:** Weak or compromised authentication mechanisms can lead to unauthorized access to the systems involved in medical image transfer **(Denis et. al., 2021).** Attackers can exploit vulnerabilities to gain access to sensitive medical images and patient data.

8. **Insider Threats:** Insider threats refer to malicious actions or negligence from individuals within the healthcare organization who have authorized access to the medical image transfer systems**(Yeo et. al., 2022).** These individuals can intentionally or unintentionally compromise the security and privacy of medical images. Transmission of medical signals faces problems related to data security. Dissemination of data from peer to peer or client to server via various networks faces security issues. Security is a crucial aspect of medical imaging systems, including Picture Archiving and Communication Systems (PACS), DICOM, and the underlying TCP/IP protocols. Several challenges need to be addressed to ensure the confidentiality, integrity, and availability of medical imaging data**(Sawand et. al., 2015).**

9. **Patient Data Privacy:** Medical images contain sensitive patient information, including personal health details. Protecting patient privacy is vital, and unauthorized access to patient data must be prevented. Security measures such as access controls, user authentication, and encryption techniques are essential to safeguard patient privacy**(Sun et. al., 2018).**

10. **Network Vulnerabilities:** PACS and DICOM systems often rely on TCP/IP networks for data transmission. However, these networks can be susceptible to various security threats, such as unauthorized access, network eavesdropping, data interception, and denial-of-service (DoS) attacks. Implementing network security mechanisms like firewalls, intrusion detection systems (IDS), and secure communication protocols (e.g., Secure Socket Layer/Transport Layer Security) can help mitigate these risks **(Aupet et. At., 2010).**

11. **Data Integrity:** Maintaining the integrity of medical imaging data is critical to ensure that images are not tampered with or modified in transit**(Swaraja et. al., 2020).** Data integrity measures, including digital signatures and checksums, can be employed to detect any unauthorized modifications to the images or their metadata **(Nyeem et. Al., 2013).**

12. **Secure Image Storage:** PACS systems store vast amounts of medical imaging data, making them potential targets for data breaches. Strong access controls, encryption at rest, and secure storage infrastructure are necessary to protect the data from unauthorized access or data leakage**(Mohsan et. al., 2022).**

13. **Software Vulnerabilities:** PACS, DICOM, and other medical imaging systems may be vulnerable to software flaws or vulnerabilities. Regular software updates, patches, and security testing can help address these vulnerabilities and ensure that systems remain secure against potential exploits **(Eichelberg et. al., 2021).**

14. **Interoperability Challenges:** Integrating different PACS and DICOM systems from various vendors can introduce security challenges due to variations in implementation and configuration. Properly configuring the systems, adhering to security best practices, and conducting thorough security assessments during integration can help address interoperability-related security risks**(Tong et.al., 2008).**

15. **Compliance and Regulatory Requirements:** Healthcare organizations must comply with applicable regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union. Compliance with these regulations necessitates implementing appropriate security controls and privacy measures for medical imaging systems.

Addressing these security challenges requires a holistic approach, including a combination of technical safeguards, policies and procedures, employee training, and regular security assessments. Healthcare organizations should continually evaluate and update their security measures to protect the confidentiality, integrity, and availability of medical imaging data in PACS, DICOM, and TCP/IP-based networks**(Eloff et. al., 2005).**

IV. METHODS TO MANAGE THE SECURITY CHALLENGES

Managing the security challenges associated with DICOM/PACS and TCP/IP involves implementing a range of measures to protect the confidentiality, integrity, and availability of medical imaging data.

1. **Risk Assessment:** Conduct a comprehensive risk assessment to identify potential vulnerabilities, threats, and risks within the DICOM/PACS and TCP/IP infrastructure. This assessment helps prioritize security efforts and allocate resources effectively**(Kaczmarczyk et. al., 2016).**

2. **Access Control:** Implement strong access control mechanisms to ensure that only authorized individuals or systems can access and transmit medical imaging data. This includes user authentication with secure credentials, role-based access control (RBAC), and regular access reviews**(Saidi et. al., 2022).**

3. **Encryption:** Utilize encryption techniques, such as SSL/TLS, to protect the confidentiality of medical imaging data during transmission over TCP/IP networks. Encryption ensures that the data is secure and not susceptible to eavesdropping or unauthorized interception**(Karygiannis et. al., 2002).**

4. **Network Security:** Implement network security measures such as firewalls, intrusion detection/prevention systems (IDS/IPS), and Virtual Private Networks (VPNs). These measures help safeguard against unauthorized access, network-based attacks, and ensure secure communication channels **(Weerathunga et. al., 2017).**

5. **Data Integrity Mechanisms:** Employ data integrity mechanisms such as digital signatures or checksums to detect and prevent unauthorized modifications or tampering with medical imaging data. This ensures the integrity of the data throughout the transmission process**(Qasim et. al., 2018).**

6. **Security Monitoring and Logging:** Implement robust monitoring and logging systems to detect and track suspicious activities, potential security incidents, or unauthorized access attempts. Monitoring systems should generate real-time alerts and logs for prompt investigation and response**(Priya et. al., 2023).**

7. **Security Policies and Procedures:** Develop and enforce security policies and procedures specific to DICOM/PACS and TCP/IP environments. These policies should cover areas such as user access, data handling, incident response, and disaster recovery**(Marsh et. al., 2000).**

8. **Regular Security Audits and Assessments:** Conduct periodic security audits and assessments to evaluate the effectiveness of security controls, identify vulnerabilities, and ensure compliance with security standards and regulations. This helps maintain a proactive security posture and address emerging threats**(Alhammmadi et. al., 2023).**

9. **Employee Training and Awareness:** Provide comprehensive training and awareness programs to educate employees and system users about security best practices, including safe data transmission, password hygiene, and identifying and reporting security incidents **(Fernández-Alemán et. Al., 2015).**

10. **Regulatory Compliance:** Stay updated with relevant regulatory requirements, such as HIPAA or GDPR, and ensure compliance with data privacy and security obligations. Regularly review and update security measures to align with evolving regulations**(Olukoya et. al., 2022).**

11. **Vendor Management:** If using third-party vendors for DICOM/PACS or TCP/IP components, ensure they follow robust security practices. Evaluate the security posture of vendors, review their security policies and practices, and establish contractual obligations regarding security requirements **(Grobler et. al., 2020).**

12. **Digital Signature:** Digital signatures provide a means to verify the authenticity and integrity of medical images. A digital signature is a cryptographic technique that associates the image with a digital certificate, ensuring that the image has not been tampered with and originates from a trusted source**(Kobayashi et. Al., 2009).**

13. **Micro-segmentation:** Micro-segmentation involves dividing a network into smaller, isolated segments to enhance security. By implementing micro-segmentation in the context of medical images, access to the images can be controlled and restricted to

authorized individuals or systems, reducing the risk of unauthorized access or lateral movement within the network **(Chen et. al., 2020).**

14. **Multifactor Authentication (MFA):** Multifactor authentication adds an extra layer of security by requiring users to provide multiple forms of identification before accessing medical images**(Kebande et. al., 2021).** This can include a combination of passwords, biometrics, smart cards, or other authentication factors, reducing the risk of unauthorized access.

15. **Watermarking:** Watermarking is the process of embedding invisible or visible data within the medical image to identify its origin or ownership**(Mata-Mendoza et. al., 2022).** Watermarks can be used to deter unauthorized use or distribution of medical images and trace their source if necessary.

16. **Privileged Account Management (PAM):** PAM focuses on securing and managing privileged accounts, which have extensive access rights within systems. By implementing PAM practices, healthcare organizations can control and monitor privileged accounts associated with medical image systems, reducing the risk of unauthorized access or misuse**(Tawalbeh et. al., 2022).**

17. **Vendor-Neutral Archives (VNA):** VNA refers to a technology solution that enables the storage and management of medical images from different vendors or systems in a standardized format**(Larobina et. al., 2014).** By adopting VNA, healthcare organizations can consolidate and secure medical images within a single repository, simplifying access control and enhancing security measures**(Lebre et. al., 2020).**

By implementing these methods, healthcare organizations can mitigate security challenges associated with DICOM/PACS and TCP/IP, protect sensitive medical imaging data, and maintain the trust and confidentiality of patient information**(Mata Miquel et. al., 2015).**

V. DATA ENCRYPTION AND SECURITY METHODS

Data encryption and security methods play a crucial role in protecting sensitive information from unauthorized access, interception, and tampering. Here are some commonly used data encryption and security methods**(Shiu et. al., 2011)**:

1. **Encryption Algorithms:** Encryption algorithms transform data into unreadable ciphertext using mathematical algorithms. Commonly used encryption algorithms include Advanced Encryption Standard (AES), RSA, and Triple DES. These algorithms use keys to encrypt and decrypt data, ensuring its confidentiality.

2. **Symmetric Encryption:** Symmetric encryption uses a single key for both encryption and decryption. The same key is used to encrypt the data at the sender's end and decrypt it at the recipient's end. AES is an example of a symmetric encryption algorithm widely used for secure data transmission**(Haque et. al., 2018).**

3. **Asymmetric Encryption:** Asymmetric encryption, also known as public-key encryption, uses a pair of keys - a public key for encryption and a private key for decryption. The public key is widely distributed, while the private key remains securely with the intended recipient. RSA is a popular asymmetric encryption algorithm**(Canetti et. al., 2003).**

4. **Transport Layer Security (TLS)/Secure Socket Layer (SSL):** TLS and SSL protocols provide secure communication over networks, such as the internet. They establish an encrypted connection between the client and server, ensuring the confidentiality and integrity of data transmitted over TCP/IP networks **(Husák et. al., 2015).**

5. **Hash Functions:** Hash functions convert data into fixed-length hash values or digests. These hash values are unique for each input, and even a slight change in the input data will produce a different hash value. Hash functions are used for data integrity verification and to detect any unauthorized modifications during transmission**(Ullah et. al., 2023).**

6. **Message Authentication Codes (MAC):** MACs use cryptographic hash functions along with a secret key to generate a unique code for a message or data. This code is appended to the message to verify its integrity and authenticity **(Bellare et. al., 1996).** HMAC (Hash-based Message Authentication Code) is a commonly used MAC algorithm.

7. **Digital Signatures:** Digital signatures use asymmetric encryption to provide data integrity and authentication. A digital signature is created using the sender's private key and can be verified using their public key **(Blumenthal et. al., 2007).** It ensures that the data has not been tampered with and that it originated from the expected sender.

8. **Access Control and Authentication:** Implementing strong access control mechanisms, such as username and password combinations, two-factor authentication (2FA), or biometric authentication, helps ensure that only authorized individuals can access sensitive data**(Mughal et. al., 2018).**

9. **Security Protocols:** Utilize secure communication protocols, such as Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), for transmitting data securely over networks. These protocols provide encryption and authentication mechanisms to protect data during transmission**(Barrett et. al., 2001).**

10. **Security Key Management:** Effective key management is crucial for encryption. This involves securely generating, storing, and distributing encryption keys. Key rotation, key length, and key storage practices should be followed to ensure the strength and integrity of encryption keys**(Carman et. al., 2000).**

11. **Secure Data Storage:** Protecting data at rest is equally important. Data can be encrypted using techniques like full disk encryption (FDE) or file-level encryption to secure it when stored on physical or digital storage media**(Benadjila et. al., 2022).**

12. **Regular Security Updates and Patches:** Keep systems and software up to date with the latest security updates and patches to address any known vulnerabilities and protect against potential attacks**(Lippmann et. al., 2002).**

Implementing a combination of these encryption and security methods helps safeguard data and maintain the confidentiality, integrity, and availability of sensitive information, particularly in contexts such as healthcare, finance, and other industries handling sensitive data.

VI. ENSURING INCOMING DATA CONFORMANCE WITH DICOM

(Digital Imaging and Communications in Medicine) standards is crucial for maintaining interoperability and consistency in medical imaging systems.

1. **DICOM Conformance Statements:** DICOM Conformance Statements provide detailed information about the capabilities and supported features of a DICOM-compliant system. When receiving data from external sources, such as medical imaging devices or other healthcare systems, it is important to review the DICOM Conformance Statements of those sources. These statements outline the expected format, encoding, transfer syntaxes, and supported DICOM services, helping you determine if the incoming data conforms to the expected standards**(Lim et. al., 2006).**

2. **Validation and Verification:** Implement a validation and verification process to check the conformance of incoming DICOM data. This involves using DICOM-specific software tools or libraries to validate the structure, attributes, and data encoding of the incoming DICOM objects. These tools can perform checks for mandatory fields, data types, encoding rules, and consistency with the defined DICOM standards **(Clunie et. al., 2000).**

3. **Pre-Transfer Verification:** Before accepting incoming DICOM data, perform pre-transfer verification to ensure the data adheres to the expected DICOM standards. This can include verifying the metadata, patient demographics, study information, and image-related attributes. The verification process can help identify potential issues or inconsistencies in the incoming data**(Garcia-Ceja et. al., 2018).**

4. **DICOM Data Quality Checks:** Implement data quality checks to validate the integrity and accuracy of the incoming DICOM data. This can involve checking for missing or incorrect attributes, validating the syntax and encoding of the data elements, and ensuring proper referential integrity between different DICOM objects (e.g., ensuring the association between a study, series, and images is maintained)**(Vaitkus et. al., 2021).**

5. **Interoperability Testing:** Perform interoperability testing with external systems or vendors to ensure that the incoming DICOM data conforms to the expected standards and can be seamlessly integrated into your system. This involves exchanging test datasets and verifying the compatibility and conformance of the data exchange process **(Herrmann et. al., 2018).**

6. **Compliance Monitoring:** Establish a monitoring mechanism to continuously assess and monitor the conformance of incoming DICOM data. This can involve regular audits, automated checks, and logging of DICOM data to identify any deviations from the expected standards. If non-conforming data is detected, appropriate measures can be

taken to rectify the issues or communicate with the data source for resolution**(Hills et. al., 2018).**

7. **Vendor Collaboration:** Collaborate closely with DICOM-compliant device vendors, healthcare information systems, and other stakeholders to ensure mutual understanding and compliance with DICOM standards. Engaging in discussions, participating in DICOM working groups, and staying updated with the latest DICOM releases and updates can help ensure incoming data conformance**(Bui et. al., 2010).**

VII. WATERMARKING OF MEDICAL IMAGES

Watermarking medical images involves embedding imperceptible or semi-perceptible information into the images to provide various functionalities such as copyright protection, authentication, tamper detection, and source identification. Here are some key considerations and approaches when watermarking medical images:

1. **Visible Watermarking:** Visible watermarks are overlays of visible text or logos that are added to the medical images. They are intended to be easily visible and act as a deterrent against unauthorized use or distribution of the images. Visible watermarks are useful for indicating ownership or copyright status and can discourage unauthorized copying or redistribution.

2. **Invisible Watermarking:** Invisible watermarks, also known as digital watermarks, are embedded within the image data and are not perceptible to the human eye. These watermarks are designed to be robust against various image processing operations and remain embedded even after modifications to the image. Invisible watermarks can be used for copyright protection, authentication, and tamper detection **(Swanson et. al., 1998).**

3. **Digital Signature Watermarking:** Digital signature-based watermarking utilizes cryptographic techniques to embed a unique signature into the medical image. The signature is generated using the image data and the signer's private key**(Lalem et. al., 2023).** Verifying the signature using the signer's public key ensures the integrity and authenticity of the image.

4. **Fragile Watermarking:** Fragile watermarking is a technique used to detect any unauthorized modifications or tampering of the medical images. The watermark is designed to be highly sensitive to changes, and even slight modifications in the image can render the watermark unreadable or produce a detection signal. Fragile watermarking can be used for tamper detection and forensic analysis.

5. **Region-of-Interest Watermarking:** In medical imaging, specific regions of interest (ROIs) within an image may hold critical diagnostic information. Region-of-interest watermarking focuses on embedding watermarks specifically in these ROIs to ensure their integrity and authenticity. This approach allows for more targeted and localized protection of the most crucial parts of the image **(Osborne et. al., 2004).**

6. **Robust Watermarking:** Robust watermarking techniques are designed to withstand intentional or unintentional attacks and modifications to the image. These techniques employ sophisticated algorithms that ensure the watermark remains detectable even after various image processing operations, such as compression, cropping, or filtering **(Cox et. al., 1996).**

7. **Metadata Watermarking:** In addition to embedding watermarks within the image data, metadata watermarking involves embedding watermarking information in the image metadata. This can include information such as ownership, copyright details, and authentication codes. Metadata watermarks can be used to provide supplementary information about the image and its authenticity**(Potdar et. al., 2005).**

8. **Legal Considerations:** When watermarking medical images, it is important to consider legal aspects such as copyright laws, intellectual property rights, and compliance with regulations like HIPAA or GDPR**(De Aguiar et. al., 2022).** Ensure that the watermarking process does not compromise patient privacy or violate any regulatory requirements.

It's worth noting that the implementation of watermarking techniques should consider the balance between the level of security, the impact on image quality, and the requirements of the specific medical imaging applications. Thorough testing, validation, and adherence to industry best practices are essential to ensure the effectiveness and compatibility of watermarking techniques in medical imaging workflows.

VIII. ARTIFICIAL INTELLIGENCE IN MEDICAL IMAGE SECURITY

Artificial intelligence (AI) can play a significant role in enhancing medical image security. Here are some applications of AI in medical image security:

1. **Threat Detection:** AI algorithms can be trained to analyze medical images and detect potential security threats or anomalies. For example, AI can identify regions of interest that may contain hidden data, such as embedded watermarks or unauthorized modifications. It can also detect tampering attempts or alterations in the image that could compromise its integrity.

2. **Authentication and Verification:** AI can be utilized for image authentication and verification purposes. AI models can learn patterns and features within medical images that indicate their authenticity**(Karargyris et. al., 2021).** By comparing images against known reference images or using advanced machine learning techniques, AI can determine if an image has been manipulated or if it matches the expected characteristics of a genuine image.

3. **Privacy Protection:** AI techniques like facial recognition and anonymization algorithms can be employed to protect patient privacy in medical images **(Jeong et. al., 2020).** AI can automatically detect and blur or mask personally identifiable information (PII) present in images, ensuring compliance with privacy regulations such as HIPAA. AI-powered privacy protection helps prevent unauthorized access or disclosure of sensitive patient data.

4. **Threat Prevention and Intrusion Detection:** AI-based intrusion detection systems can be employed to monitor and analyze network traffic within medical imaging systems**(Awotunde et. al., 2022).** These systems can identify potential security threats, such as unauthorized access attempts or suspicious activities, and raise alerts or take preventive actions to mitigate the risks.

5. **Secure Data Exchange:** AI can assist in secure data exchange between healthcare systems or entities. AI algorithms can be used for encryption and decryption processes, ensuring the confidentiality of medical image data during transmission and storage. AI can also aid in secure key management and access control mechanisms to protect the integrity and privacy of medical images**(Nagarajan et. al., 2021).**

6. **Adversarial Attack Detection:** Adversarial attacks are deliberate attempts to manipulate or deceive AI algorithms. In the context of medical image security, AI can be used to detect and mitigate adversarial attacks that target image classifiers or authentication systems**(Ahmad et. al., 2022).** By employing AI models trained to recognize adversarial patterns or employing defensive strategies, medical image systems can become more resilient to such attacks.

7. **Intelligent Access Control:** AI can be utilized for intelligent access control mechanisms in medical imaging systems. By analyzing user behavior patterns, AI algorithms can identify suspicious activities or unauthorized access attempts, triggering additional authentication measures or blocking access to sensitive image data **(Hu et. al., 2021).**

8. **Anomaly Detection:** AI algorithms can learn the normal behavior and patterns within medical image data. By monitoring image data in real-time, AI can detect anomalies that may indicate security breaches or unauthorized activities. Anomaly detection can help identify potential threats or deviations from expected patterns, allowing for timely intervention and mitigation.

AI can offer significant benefits in medical image security, it is crucial to ensure proper training, validation, and robustness of the AI models. Additionally, adherence to ethical guidelines and regulatory requirements is essential when deploying AI solutions in the medical field.

IX. NANOTECHNOLOGY IN MEDICAL IMAGE SECURITY

Nanotechnology has the potential to play a significant role in enhancing medical image security. While the direct application of nanotechnology in medical image security is still an emerging area, some potential ways includes Nanoparticle-Based Contrast Agents, Quantum Dots for Watermarking, Nanoscale Security Features, Nanosensors for Image Authentication, and Nanocoatings for Image Protection, Nanoparticles can serve as contrast agents in medical imaging, enhancing the visibility of specific tissues or structures. These nanoparticles can be engineered with unique properties, allowing them to be detectable by specific imaging modalities (e.g., MRI, CT, or optical imaging). By using targeted nanoparticles as contrast agents, it becomes possible to label and track medical images with unique identifiers, improving image security and reducing the likelihood of tampering or misidentification**(Rosen et. al., 2011).** Quantum dots are nanoscale semiconductor crystals

that emit light of specific colors when exposed to light of a different wavelength. They have unique optical properties that make them suitable for watermarking medical images. By incorporating quantum dots into medical images, it becomes possible to embed invisible and highly secure watermarks directly into the images. These watermarks can serve as digital signatures, making it easier to authenticate and verify the origin and integrity of the images. Nanotechnology can be used to develop nanoscale security features, such as micro-tags or nanoscale patterns, that can be embedded in medical images. These features would be challenging to replicate or counterfeit, providing an additional layer of security to medical images. Nanosensors can be designed to respond to specific physical or chemical changes, such as temperature, pressure, or exposure to certain substances **(Yeung et. al., 1998).** Integrating nanosensors into medical images could enable real-time monitoring of the image's environmental conditions and detect any alterations or unauthorized access**(Klinghammer et. al., 2020).** Nanocoatings with specific properties, such as anti-tampering or self-healing capabilities, can be applied to protect medical images from physical damage or unauthorized alterations. Nanotechnology holds great promise for medical image security, its practical implementation in the healthcare sector is still in the early stages. As with any emerging technology, there are challenges and considerations related to safety, biocompatibility, regulatory approvals, and cost-effectiveness that need to be addressed before widespread adoption in medical image security applications.

X. NANOLEVEL SECURITY FEATURES IN MEDICAL IMAGES

Nanoscale security features can be incorporated into digital medical images to enhance their security and protect against tampering or unauthorized access. Some potential nanoscale security features for digital medical images include Nanoscale Patterns, Micro-tags, Nanosensors, Cryptographic Nanomaterials, and Self-Healing Coatings.

Nanoscale patterns or structures can be embedded within the digital image at a microscopic level. These patterns can be designed using nanolithography techniques, such as electron beam lithography or nanoimprint lithography. The unique nanoscale patterns serve as a form of fingerprint or identifier, making it difficult to replicate or alter the image without detection**(Xie et. al., 2006).** Microscopic tags or markers can be added to the digital image using nanotechnology. These tags can consist of nanoscale particles, such as quantum dots or nanobarcodes, that are invisible to the naked eye. These tags can serve as unique identifiers and enable traceability of the image, making it easier to authenticate and verify its authenticity. Nanosensors can be integrated into digital medical images to detect changes in environmental conditions or to monitor for unauthorized access. These nanosensors can be designed to respond to specific stimuli, such as changes in temperature, humidity, or exposure to light. Any alteration or tampering with the image would trigger a response from the nanosensors, indicating a potential security breach**(Zafar et. al., 2021).** Cryptographic nanomaterials can be used to protect the digital image by embedding encryption keys or codes at the nanoscale level. These cryptographic nanomaterials can ensure that only authorized individuals or systems with the correct decryption keys can access or modify the image **(Du et. al., 2021).** Nanocoatings with self-healing properties can be applied to digital images to protect against physical damage or tampering attempts**(Li et. al., 2023).** These coatings can contain nanoscale capsules or polymers that can repair any damage or alterations to the image by releasing healing agents when triggered. The incorporation of nanoscale security features in digital medical images aims to enhance their integrity, traceability, and

protection against unauthorized access or tampering. These features leverage the unique properties of nanomaterials to provide additional layers of security and increase confidence in the authenticity and reliability of the images.

XI. INCORPORATING NANO LEVEL SECURITY FEATURES IN DIGITAL MEDICAL IMAGES

Incorporating nano level security features in digital medical images involves several steps and considerations.

1. **Design the Security Feature:** Determine the specific security feature or mechanism you want to incorporate into the digital medical image. This could include nanoscale patterns, micro-tags, nanosensors, cryptographic nanomaterials, or self-healing coatings.

2. **Select Nanomaterials:** Choose appropriate nanomaterials that are compatible with the desired security feature. Consider factors such as stability, biocompatibility, optical properties, and the ability to interact with the image**(Hedayatnasab et. al., 2017).**

3. **Fabrication or Modification:** Prepare or modify the nanomaterials to incorporate the desired security features. This may involve techniques such as nanolithography, surface functionalization, or encapsulation**(Zhang et. al., 2020).**

4. **Integration with the Digital Image:** Incorporate the nanomaterials into the digital image. This can be done by physically embedding the nanomaterials within the image or by using specific encoding techniques to represent the security features within the image data **(Arppe et. al., 2017).**

5. **Detection and Authentication:** Develop methods or protocols to detect and authenticate the nanolevel security features in the digital image. This may involve using specialized imaging techniques, spectroscopic analysis, or other characterization methods to identify and verify the presence of the security features **(Jones et. al., 2009).**

6. **Verification and Validation:** Establish a validation process to ensure the effectiveness and reliability of the incorporated security features**(Wishart et. al., 2020).** This may involve testing the images under different conditions, evaluating the robustness of the security features, and assessing their resistance to tampering or alteration attempts.

7. **Documentation and Standards:** Document the incorporation of nanolevel security features in digital medical images and establish standards or guidelines for their use. This includes recording the specific security mechanisms used, the validation process, and any relevant information required for future reference or compliance**(Elberskirch et. Al., 2022).**

Incorporating nano-level security in digital medical images requires expertise in both nanotechnology and medical imaging. Collaboration between researchers, nanotechnologists, and imaging specialists is crucial to ensure the successful integration of security features without compromising the quality or integrity of the medical images. Additionally, regulatory considerations and ethical aspects should be taken into account

to ensure compliance with applicable laws and patient privacy requirements **(Kelly et. al., 2013).**

XII. NANOTECHNOLOGY IN IMAGE SECURITY

Futuristic trends in image data security using nanotechnology are expected to revolutionize the field by providing advanced and robust security measures. Here are some potential trends:

1. **Nano-scale Authentication:** Nanotechnology can enable the development of nanoscale authentication methods for image data. This may involve the use of nanosensors or nanomaterials that can uniquely identify and authenticate the image data, ensuring its integrity and preventing unauthorized access**(Nikhat et. al., 2020).**

2. **Self-healing Nanomaterials:** Self-healing nanomaterials can automatically repair any damage or tampering attempts in image data. These materials can detect and respond to alterations, restoring the image data to its original state **(Tan et. al., 2021).** This technology can provide an additional layer of security, ensuring the integrity of image data even in the face of cyber attacks.

3. **Nanoscale Cryptographic Keys:** Nanotechnology can facilitate the generation and distribution of nanoscale cryptographic keys. These keys can be extremely small and offer enhanced security due to their unique properties at the nanoscale. Nanoscale cryptographic keys can provide stronger encryption and protection against brute-force attacks **(Sicari et. al., 2021).**

4. **Quantum Computing-resistant Encryption:** Quantum computing has the potential to break traditional encryption algorithms. Nanotechnology can contribute to the development of quantum-resistant encryption techniques that can withstand attacks from quantum computers. Nanostructured materials can be used to create new encryption algorithms that are resistant to quantum-based attacks**(Cambou et. al., 2020).**

5. **Nano-based Intrusion Detection Systems**: Nanosensors embedded within image data or imaging systems can act as advanced intrusion detection systems. These nanosensors can detect and alert for any unauthorized access, modification, or tampering attempts in real-time, providing immediate response and protection against cyber attacks **(Roobini et. al., 2022).**

6. **Biometric-based Nanosensors:** Nanotechnology can enable the development of biometric-based nanosensors for image data security**(Perdomo et. al., 2021).** These sensors can utilize unique biological characteristics, such as fingerprints or DNA, to authenticate users and ensure secure access to image data. Biometric-based nanosensors offer enhanced security and eliminate the need for traditional passwords or access credentials.

7. **Nanobots for Threat Mitigation:** Nanobots, tiny robots operating at the nanoscale, can be employed for threat mitigation in image data security. These nanobots can actively

patrol and monitor image data, identifying and neutralizing potential threats or vulnerabilities in real-time**(Hooker et. al., 2016).**

8. **Nanoparticle-based Secure Storage:** Nanoparticles can be engineered to provide secure storage for image data. These nanoparticles can store and protect image data within their structure, making it difficult for unauthorized individuals or cyber attackers to access or retrieve the data without proper authentication.

Futuristic trends are still in the realm of ongoing research and development. The practical implementation and commercial availability of such nanotechnology-based solutions for image data security may take time. However, as nanotechnology continues to advance, these trends hold great potential to shape the future of image data security, providing robust protection against cyber threats**(Goh et. al., 2016).**

REFERENCES

[1] Cooke Jr, R. E., Gaeta, M. G., Kaufman, D. M., & Henrici, J. G. (2003). U.S. Patent No. 6,574,629. Washington, DC: U.S. Patent and Trademark Office.
[2] Maksimović, M., & Vujović, V. (2017). Internet of things based e-health systems: ideas, expectations and concerns. Handbook of large-scale distributed computing in smart healthcare, 241-280.
[3] Mohammed, D. (2017). US healthcare industry: Cybersecurity regulatory and compliance issues. Journal of Research in Business, Economics and Management, 9(5), 1771-1776.
[4] Paudel, S. (2019). Data Breach a Cyber Security Issue in Cloud.
[5] Aziz, Azaam, et al. "Medical imaging of microrobots: Toward in vivo applications." ACS nano 14.9 (2020): 10865-10893.
[6] Friedenberg, Richard M. "The role of the supertechnologist." Radiology 215.3 (2000): 630-633.
[7] Mbunge, Elliot, et al. "Virtual healthcare services and digital health technologies deployed during coronavirus disease 2019 (COVID-19) pandemic in South Africa: a systematic review." Global health journal 6.2 (2022): 102-113.
[8] Varadarajan, Vinithra, et al. "Role of imaging in diagnosis and management of COVID-19: a multiorgan multimodality imaging review." Frontiers in Medicine 8 (2021): 765975
[9] Long, Brit, et al. "Clinical update on COVID-19 for the emergency clinician: Presentation and evaluation." The American journal of emergency medicine 54 (2022): 46-57.
[10] Oakley, Jason, ed. Digital imaging: a primer for radiographers, radiologists and health care professionals. Cambridge University Press, 2003.
[11] Brown, Steven H., et al. "VistA—US department of veterans affairs national-scale HIS." International journal of medical informatics 69.2-3 (2003): 135-156.
[12] Mun, Seong K., et al. "Baseline study of radiology services for the purpose of PACS evaluation." Medical Imaging II. Vol. 914. SPIE, 1988.
[13] Levine, Betty A., et al. "Assessment of the Integration of a HIS/RIS with a PACS." Journal of Digital Imaging 16 (2003): 133-140.
[14] Shini, S. G., Tony Thomas, and K. Chithraranjan. "Cloud based medical image exchange-security challenges." Procedia Engineering 38 (2012): 3454-3461.
[15] Allen Jr, Bibb, et al. "A road map for translational research on artificial intelligence in medical imaging: from the 2018 National Institutes of Health/RSNA/ACR/The Academy Workshop." Journal of the American College of Radiology 16.9 (2019): 1179-1189.
[16] Kutkat, Lora, et al. "The HIPAA Privacy Rule: Reviewing the post-compliance impact on public health practice and research." Journal of Law, Medicine & Ethics 31.S4 (2003): 70-72.
[17] Bari, Lisa, and Daniel P. O'Neill. "Rethinking patient data privacy in the era of digital health." Health Affairs Forefront (2019).
[18] Miaoulis, William M. "Hipaa security overview-retired." Journal of AHIMA (2013).
[19] Evans, Mark, et al. "Human behaviour as an aspect of cybersecurity assurance." Security and Communication Networks 9.17 (2016): 4667-4679.

[20] Watzlaf, Valerie JM, et al. "A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers." International Journal of Telerehabilitation 9.2 (2017): 39.
[21] Begoyan, A. "An overview of interoperability standards for electronic health records." USA: society for design and process science (2007).
[22] Rea, Susan, et al. "Building a robust, scalable and standards-driven infrastructure for secondary use of EHR data: the SHARPn project." Journal of biomedical informatics 45.4 (2012): 763-771.
[23] Snelick, Robert, et al. "Towards interoperable healthcare information systems: The HL7 conformance profile approach." Enterprise Interoperability II: New Challenges and Approaches. Springer London, 2007.
[24] Iroju, Olaronke, et al. "Interoperability in healthcare: benefits, challenges and resolutions." International Journal of Innovation and Applied Studies 3.1 (2013): 262-270.
[25] Clunie, David A. DICOM structured reporting. PixelMed publishing, 2000.
[26] Clunie, David A. "DICOM format and protocol standardization—a core requirement for digital pathology success." Toxicologic Pathology 49.4 (2021): 738-749.
[27] Seeram, Euclid, and Euclid Seeram. "Picture Archiving and Communication Systems." Digital Radiography: Physical Principles and Quality Control (2019): 139-164.
[28] Chenthara, Shekha, et al. "Security and privacy-preserving challenges of e-health solutions in cloud computing." IEEE access 7 (2019): 74361-74382.
[29] Kondylakis, Haridimos, et al. "Position of the AI for Health Imaging (AI4HI) network on metadata models for imaging biobanks." European Radiology Experimental 6.1 (2022): 1-15.
[30] Fanni, Salvatore Claudio, et al. "Structured reporting and artificial intelligence." Structured Reporting in Radiology. Cham: Springer International Publishing, 2022. 169-183.
[31] Kalra, Dipak, and David Ingram. "Electronic health records." Information technology solutions for healthcare. London: Springer London, 2006. 135-181.
[32] Herrmann, Markus D., et al. "Implementing the DICOM standard for digital pathology." Journal of pathology informatics 9.1 (2018): 37.
[33] Thrall, Donald E. Textbook of Veterinary Diagnostic Radiology-E-Book. Elsevier Health Sciences, 2017.
[34] Joshi, Alark, et al. "Unified framework for development, deployment and robust testing of neuroimaging algorithms." Neuroinformatics 9 (2011): 69-84.
[35] Iroju, Olaronke, et al. "Interoperability in healthcare: benefits, challenges and resolutions." International Journal of Innovation and Applied Studies 3.1 (2013): 262-270.
[36] Shur, Joshua D., et al. "Radiomics in oncology: a practical guide." Radiographics 41.6 (2021): 1717-1732.
[37] Constantinescu, Liviu, et al. "A patient-centric distribution architecture for medical image sharing." Health information science and systems 1 (2013): 1-14.
[38] Ventola, C. Lee. "Mobile devices and apps for health care professionals: uses and benefits." Pharmacy and Therapeutics 39.5 (2014): 356.
[39] Liu, Feng, et al. "The current role of image compression standards in medical imaging." Information 8.4 (2017): 131.
[40] Godinho, Tiago Marques, et al. "A Routing Mechanism for Cloud Outsourcing<? brk?> of Medical Imaging Repositories." IEEE journal of biomedical and health informatics 20.1 (2014): 367-375.
[41] Clunie, David A., et al. "Technical challenges of enterprise imaging: HIMSS-SIIM collaborative white paper." Journal of digital imaging 29 (2016): 583-614.
[42] Gorman, Chris, et al. "Interoperable slide microscopy viewer and annotation tool for imaging data science and computational pathology." Nature Communications 14.1 (2023): 1572.
[43] Arora, Kitty, and Manshi Shukla. "A comprehensive review of image compression techniques." International Journal of Computer Science and Information Technologies 5.2 (2014): 1169-1172.
[44] Fitriya, L. Anjar, Tito Waluyo Purboyo, and Anggunmeka Luhur Prasasti. "A review of data compression techniques." International Journal of Applied Engineering Research 12.19 (2017): 8956-8963.
[45] Haddad, Sahar, et al. "Joint watermarking and lossless JPEG-LS compression for medical image security." Proceedings of the International Conference on Watermarking and Image Processing. 2017.
[46] Skodras, Athanassios, Charilaos Christopoulos, and Touradj Ebrahimi. "The JPEG 2000 still image compression standard." IEEE Signal processing magazine 18.5 (2001): 36-58.
[47] Memon, Qurban A. "Authentication and error resilience in images transmitted through open environment." Medical Imaging: Concepts, Methodologies, Tools, and Applications. IGI Global, 2017. 1651-1676.

[48] Wiegand, Thomas, et al. "Overview of the H. 264/AVC video coding standard." IEEE Transactions on circuits and systems for video technology 13.7 (2003): 560-576.
[49] Malindi, Phumzile. "QoS in telemedicine." Telemedicine Techniques and Applications (2011): 119-138.
[50] Vossberg, Michal, Thomas Tolxdorff, and Dagmar Krefting. "DICOM image communication in globus-based medical grids." IEEE Transactions on Information Technology in Biomedicine 12.2 (2008): 145-153.
[51] Wang, Tusheng, et al. "A comparison of image communication protocols in e-science platform for biomedical imaging research and applications." Medical Imaging 2012: Advanced PACS-based Imaging Informatics and Therapeutic Applications. Vol. 8319. SPIE, 2012.
[52] Majumdar, A. K. "Advances in telemedicine and its usage in India." 15th International Conference on Advanced Computing and Communications (ADCOM 2007). IEEE, 2007.
[53] Chantzis, Fotios, et al. Practical IoT hacking: the definitive guide to attacking the internet of things. No Starch Press, 2021.
[54] Papaioannou, Maria, et al. "A survey on security threats and countermeasures in internet of medical things (IoMT)." Transactions on Emerging Telecommunications Technologies 33.6 (2022): e4049.
[55] Yaacoub, Jean-Paul A., et al. "Securing internet of medical things systems: Limitations, issues and recommendations." Future Generation Computer Systems 105 (2020): 581-606.
[56] Eichelberg, Marco, Klaus Kleber, and Marc Kämmerer. "Cybersecurity challenges for PACS and medical imaging." Academic Radiology 27.8 (2020): 1126-1139.
[57] Kumar, Gulshan. "Denial of service attacks–an updated perspective." Systems science & control engineering 4.1 (2016): 285-294.
[58] Alsubaei, Faisal, Abdullah Abuhussein, and Sajjan Shiva. "Security and privacy in the internet of medical things: taxonomy and risk assessment." 2017 IEEE 42nd conference on local computer networks workshops (LCN workshops). IEEE, 2017.
[59] Denis, R., and P. Madhubala. "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems." Multimedia Tools and Applications 80 (2021): 21165-21202.
[60] Yeo, Liu Hua, and James Banfield. "Human factors in electronic health records cybersecurity breach: an exploratory analysis." Perspectives in Health Information Management 19.Spring (2022).
[61] Sawand, Ajmal, et al. "Toward energy-efficient and trustworthy eHealth monitoring system." China Communications 12.1 (2015): 46-65.
[62] Sun, Wencheng, et al. "Security and privacy in the medical internet of things: a review." Security and Communication Networks 2018 (2018): 1-9.
[63] Aupet, J -B., et al. "Security in medical telediagnosis." Multimedia Services in Intelligent Environments: Integrated Systems (2010): 201-226.
[64] Swaraja, K., K. Meenakshi, and Padmavathi Kora. "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine." Biomedical Signal Processing and Control 55 (2020): 101665.
[65] Nyeem, Hussain, Wageeh Boles, and Colin Boyd. "A review of medical image watermarking requirements for teleradiology." Journal of digital imaging 26 (2013): 326-343.
[66] Mohsan, Syed Agha Hassnain, et al. "Decentralized Patient-Centric Report and Medical Image Management System Based on Blockchain Technology and the Inter-Planetary File System." International Journal of Environmental Research and Public Health 19.22 (2022): 14641.
[67] Eichelberg, Marco, Klaus Kleber, and Marc Kämmerer. "Cybersecurity protection for PACS and medical imaging: deployment considerations and practical problems." Academic Radiology 28.12 (2021): 1761-1774.
[68] Tong, Carrison KS, and Eric TT Wong, eds. Governance of Picture Archiving and Communications Systems: Data Security and Quality Management of Filmless Radiology: Data Security and Quality Management of Filmless Radiology. IGI Global, 2008.
[69] Eloff, J. H. P., and M. M. Eloff. "Information security architecture." Computer Fraud & Security 2005.11 (2005): 10-16.
[70] Kaczmarczyk, Lisa C. Computers and society: computing for good. CRC Press, 2016.
[71] Saidi, Hafida, et al. "DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data." IEEE Access 10 (2022): 101011-101028.
[72] Karygiannis, Tom, and Les Owens. Wireless Network Security:. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002.

[73] Weerathunga, Pubudu Eroshan, and Anca Cioraca. "Securing IEDs against cyber threats in critical substation automation and industrial control systems." 2017 70th Annual Conference for Protective Relay Engineers (CPRE). IEEE, 2017.
[74] Qasim, Asaad F., Farid Meziane, and Rob Aspin. "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review." Computer Science Review 27 (2018): 45-60.
[75] Priya, VS Devi, and S. Sibi Chakkaravarthy. "Containerized cloud-based honeypot deception for tracking attackers." Scientific Reports 13.1 (2023): 1437.
[76] Marsh, Andy. "Virtual Medical Worlds: The foundation for a Telemedical Information Society." Advanced Infrastructures for Future Healthcare (2000): 87-127.
[77] Alhammmadi, Mohamed Jasem. "Continuous Internal Penetration Testing (CIPT)." (2023).
[78] Fernández-Alemán, José Luis, et al. "Analysis of health professional security behaviors in a real clinical setting: An empirical study." International journal of medical informatics 84.6 (2015): 454-467.
[79] Olukoya, Oluwafemi. "Assessing frameworks for eliciting privacy & security requirements from laws and regulations." Computers & Security 117 (2022): 102697.
[80] Grobler, A. D. A model for the teaching of imaging informatics, a platform in biomedical informatics, in a future integrated National Health Insurance system in South Africa. Diss. University of the Free State, 2020.
[81] Kobayashi, Luiz Octavio Massato, Sergio Shiguemi Furuie, and Paulo Sergio Licciardi Messeder Barreto. "Providing integrity and authenticity in DICOM images: a novel approach." IEEE transactions on information technology in Biomedicine 13.4 (2009): 582-589.
[82] Chen, Baozhan, et al. "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture." IEEE Internet of Things Journal 8.13 (2020): 10248-10263.
[83] Kebande, Victor R., et al. "A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles." Sensors 21.18 (2021): 6018.
[84] Mata-Mendoza, David, et al. "Secured telemedicine of medical imaging based on dual robust watermarking." The Visual Computer 38.6 (2022): 2073-2090.
[85] Tawalbeh, Lo'ai, et al. "Edge enabled IoT system model for secure healthcare." Measurement 191 (2022): 110792.
[86] Larobina, Michele, and Loredana Murino. "Medical image file formats." Journal of digital imaging 27 (2014): 200-206.
[87] Lebre, Rui, Luís Bastião Silva, and Carlos Costa. "A cloud-ready architecture for shared medical imaging repository." Journal of Digital Imaging 33 (2020): 1487-1498.
[88] Mata Miquel, Christian. "Web-based application for medical imaging management." (2015).
[89] Shiu, Yi-Sheng, et al. "Physical layer security in wireless networks: A tutorial." IEEE wireless Communications 18.2 (2011): 66-74.
[90] Haque, Md Enamul, et al. "Performance analysis of cryptographic algorithms for selecting better utilization on resource constraint devices." 2018 21st International Conference of Computer and Information Technology (ICCIT). IEEE, 2018.
[91] Canetti, Ran, Shai Halevi, and Jonathan Katz. "A forward-secure public-key encryption scheme." Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22. Springer Berlin Heidelberg, 2003.
[92] Husák, Martin, et al. "Network-based HTTPS client identification using SSL/TLS fingerprinting." 2015 10th international conference on availability, reliability and security. IEEE, 2015.
[93] Ullah, Fasee, and Chi-Man Pun. "Deep self-learning based dynamic secret key generation for novel secure and efficient hashing algorithm." Information Sciences 629 (2023): 488-501.
[94] Bellare, Mihir, Ran Canetti, and Hugo Krawczyk. "Keying hash functions for message authentication." Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16. Springer Berlin Heidelberg, 1996.
[95] Blumenthal, Matt. "Encryption: Strengths and weaknesses of public-key cryptography." CSRS 2007 1 (2007).
[96] Mughal, Arif Ali. "The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection." International Journal of Intelligent Automation and Computing 1.1 (2018): 1-20.
[97] Barrett, Daniel J., and Richard E. Silverman. SSH, the Secure Shell: the definitive guide. " O'Reilly Media, Inc.", 2001.

[98] Carman, David W., Peter S. Kruus, and Brian J. Matt. "Constraints and approaches for distributed sensor network security (final)." DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs) 1.1 (2000): 1-39.
[99] Benadjila, Ryad, Louiza Khati, and Damien Vergnaud. "Secure storage—Confidentiality and authentication." Computer Science Review 44 (2022): 100465.
[100] Lippmann, Richard, Seth Webster, and Douglas Stetson. "The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection." Recent Advances in Intrusion Detection: 5th International Symposium, RAID 2002 Zurich, Switzerland, October 16–18, 2002 Proceedings 5. Springer Berlin Heidelberg, 2002.
[101] Lim, Jinho, and Rashad Zein. "The digital imaging and communications in medicine (DICOM): description, structure and applications." Rapid prototyping: theory and practice (2006): 63-86.
[102] Clunie, David A. DICOM structured reporting. PixelMed publishing, 2000.
[103] Garcia-Ceja, Enrique, et al. "Mental health monitoring with multimodal sensing and machine learning: A survey." Pervasive and Mobile Computing 51 (2018): 1-26.
[104] Vaitkus, Antanas, Andrius Merkys, and Saulius Gražulis. "Validation of the crystallography open database using the crystallographic information framework." Journal of applied crystallography 54.2 (2021): 661-672.
[105] Herrmann, Markus D., et al. "Implementing the DICOM standard for digital pathology." Journal of pathology informatics 9.1 (2018): 37.
[106] Hills, Rodger. "Cladding audits: The problem of combustible cladding and the wider problem of NCBPs and non-compliant building work." Journal of building survey, appraisal & valuation 6.4 (2018): 312-321.
[107] Bui, Alex AT, and Craig Morioka. "Information systems & architectures." Medical Imaging Informatics (2010): 93-137.
[108] Swanson, Mitchell D., Mei Kobayashi, and Ahmed H. Tewfik. "Multimedia data-embedding and watermarking technologies." Proceedings of the IEEE 86.6 (1998): 1064-1087.
[109] Lalem, Farid, et al. "A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques." Applied Sciences 13.8 (2023): 5172.
[110] Osborne, Dominic, et al. "Multiple embedding using robust watermarks for wireless medical images." Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia. 2004.
[111] Cox, Ingemar J., et al. "A secure, robust watermark for multimedia." Information Hiding: First International Workshop Cambridge, UK, May 30–June 1, 1996 Proceedings 1. Springer Berlin Heidelberg, 1996.
[112] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.. IEEE, 2005.
[113] De Aguiar, Erikson J., et al. "A blockchain-based protocol for tracking user access to shared medical imaging." Future Generation Computer Systems 134 (2022): 348-360.
[114] Karargyris, Alexandros, et al. "Creation and validation of a chest X-ray dataset with eye-tracking and report dictation for AI development." Scientific data 8.1 (2021): 92.
[115] Jeong, Yeon Uk, et al. "De-identification of facial features in magnetic resonance images: software development using deep learning technology." Journal of medical Internet research 22.12 (2020): e22739.
[116] Awotunde, Joseph Bamidele, and Sanjay Misra. "Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks." Illumination of artificial intelligence in cybersecurity and forensics. Cham: Springer International Publishing, 2022. 21-44.
[117] Nagarajan, Senthil Murugan, et al. "Secure data transmission in internet of medical things using RES-256 algorithm." IEEE Transactions on Industrial Informatics 18.12 (2021): 8876-8884.
[118] Ahmad, Kashif, et al. "Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges." Computer Science Review 43 (2022): 100452.
[119] Hu, Yupeng, et al. "Artificial intelligence security: Threats and countermeasures." ACM Computing Surveys (CSUR) 55.1 (2021): 1-36.
[120] Rosen, Joshua E., et al. "Nanotechnology and diagnostic imaging: new advances in contrast agent technology." J Nanomed Nanotechnol 2.5 (2011): 115-126.
[121] Yeung, Minerva M., and Frederick C. Mintzer. "Invisible watermarking for image verification." Journal of Electronic imaging 7.3 (1998): 578-591.
[122] Klinghammer, Stephanie, et al. "Nanosensor-based real-time monitoring of stress biomarkers in human saliva using a portable measurement system." ACS sensors 5.12 (2020): 4081-4091.

[123] Xie, Xian Ning, et al. "Nanoscale materials patterning and engineering by atomic force microscopy nanolithography." Materials Science and Engineering: R: Reports 54.1-2 (2006): 1-48.
[124] Zafar, Sidra, et al. "A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things." IEEE Acces
[125] Du, Nan, Heidemarie Schmidt, and Ilia Polian. "Low-power emerging memristive designs towards secure hardware systems for applications in internet of things." Nano Materials Science 3.2 (2021): 186-204.s 9 (2021): 93529-93566.
[126] Li, Zijie, and Zhiguang Guo. "Self-healing system of superhydrophobic surfaces inspired from and beyond nature." Nanoscale 15.4 (2023): 1493-1512.
[127] Hedayatnasab, Ziba, Faisal Abnisa, and Wan Mohd Ashri Wan Daud. "Review on magnetic nanoparticles for magnetic nanofluid hyperthermia application." Materials & Design 123 (2017): 174-196.
[128] Zhang, Xin, et al. "Direct Photolithographic Deposition of Color- Coded Anti- Counterfeit Patterns with Titania Encapsulated Upconverting Nanoparticles." Advanced Optical Materials 8.20 (2020): 2000664.
[129] Arppe, Riikka, and Thomas Just Sørensen. "Physical unclonable functions generated through chemical methods for anti-counterfeiting." Nature Reviews Chemistry 1.4 (2017): 0031.
[130] Jones, Clinton F., and David W. Grainger. "In vitro assessments of nanomaterial toxicity." Advanced drug delivery reviews 61.6 (2009): 438-456.
[131] Wishart, Jeffrey, et al. "Literature review of verification and validation activities of automated driving systems." SAE Int. J. Connect. Autom. Veh 3 (2020): 267-323.
[132] Elberskirch, Linda, et al. "Digital research data: from analysis of existing standards to a scientific foundation for a modular metadata schema in nanosafety." Particle and fibre toxicology 19 (2022): 1-19.
[133] Kelly, John E., and Steve Hamm. Smart machines: IBM's Watson and the era of cognitive computing. Columbia University Press, 2013.
[134] Nikhat, Akhtar, and Perwej Yusuf. "The internet of nano things (IoNT) existing state and future Prospects." GSC Advanced Research and Reviews 5.2 (2020): 131-150.
[135] Tan, Yu Jun, et al. "Progress and Roadmap for Intelligent Self- Healing Materials in Autonomous Robotics." Advanced Materials 33.19 (2021): 2002800.
[136] Sicari, Sabrina, et al. "Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the Internet of Nano-Things." Computer Networks 162 (2019): 106856.
[137] Cambou, Bertrand, et al. "Blockchain technology with ternary cryptography." Northern Arizona University Flagstaff United States, Tech. Rep (2020).
[138] Roobini, S., et al. "Cyber-Security Threats to IoMT-Enabled Healthcare Systems." Cognitive Computing for Internet of Medical Things. Chapman and Hall/CRC, 2022. 105-130.
[139] Perdomo, Sammy A., Juan M. Marmolejo-Tejada, and Andres Jaramillo-Botero. "Bio-nanosensors: Fundamentals and recent applications." Journal of The Electrochemical Society 168.10 (2021): 107506.
[140] Hooker, Richard D. Charting a course: Strategic choices for a new administration. Government Printing Office, 2016.
[141] Goh, P. S., et al. "Recent trends in membranes and membrane processes for desalination." Desalination 391 (2016): 43-60.

