Digital Health Defenders: Transforming IoT Security Frameworks in Healthcare

Maola Sirzul
BCs Hons in *Computer Science (Cyber Security)*
University of Greenwich
Old Royal Naval College
United Kingdom

Abstract:

By providing remote patient monitoring as well as in health management, the Internet of Things (IoT) has the potential to completely transform the healthcare industry. Until now, the usage of IoT devices in healthcare also presents serious security threats since these devices are frequently targeted by hackers that compromise the security and privacy of patients. In order to solve these security issues, this thesis provides an advanced security architecture for IoT devices used in healthcare. The suggested framework aims to offer an extensive and reliable security solution for IoT devices in the healthcare industry.

The framework was created using a combination of case studies, literature reviews, and implementation and testing in the dataset. The evaluations of the literature presented the current state of the art in IoT security frameworks for healthcare applications and identified out key areas and knowledge gaps. The case studies were carried out to comprehend the methods already in use and the difficulties in protecting IoT devices in the healthcare industry. The suggested framework was evaluated through testing and real-world implementation.

The proposed framework includes various security measures such as secure communication protocols, strong authentication methods, and specific security controls and technologies specifically designed for IoT devices in healthcare. The secure communication protocols, such as HTTPS and TLS, provide secure communication between devices, while the strong authentication methods, such as multi-factor authentication, ensure that only authorized users can access the devices. The specific security controls and technologies are designed to protect the devices from cyber threats, such as firewalls and intrusion detection systems.

The evaluation of the proposed approach shows that it is effective at improving IoT device security in healthcare while maintaining the devices' usability for patients and healthcare professionals. The identifying was tested by being implemented in a real-world setting, and the outcomes shown that it can identify and stop cyber-attacks on IoT devices used in healthcare. The suggested framework's usability was also assessed, and the findings indicated that it had no detrimental effects on the devices' usability. Also, the analysis points up information gaps and offered suggestions for additional analysis. The requirement for efficient and secure solutions for IoT devices with limited capabilities was one of the key vulnerabilities identified. The research also indicates that more study is required to manage the security of significant, complex IoT systems in healthcare and to ensure the safety of IoT devices throughout their lifetime.

This thesis presents an advance security framework for IoT devices in healthcare that addresses the security challenges faced by these devices. The proposed framework is designed to provide a comprehensive security solution for IoT devices in healthcare. The framework was developed through a combination of literature review, case studies, implementation and testing. The evaluation of the proposed framework

shows that it is effective in improving the security of IoT devices in healthcare while maintaining the usability of the devices for healthcare professionals and patients. This research is a step towards providing a more secure and reliable infrastructure for IoT devices in healthcare, which will help to ensure the protection of patient privacy and safety.

Keywords: *IoTs Security, Cybersecurity, Medical IoT, Encryption Methods, Decryption Methods, RSA, AES, Intrusion Detection system. Intrusion Prevention System.*

1. Introduction:

Healthcare is only one of several industries that have been significantly impacted by the Internet of Thing's (IoT) quick development. IoT devices are becoming essential in healthcare settings because they enable remote monitoring, individualised treatment, and effective data management. Nowadays, telemedicine, patient care, and illness management all depend on these gadgets (Hussain *et al.*, 2022). Sensitive patient data and vital medical systems are at danger due to the rising use of IoT devices, which also exposes the healthcare industry to a variety of security risks and vulnerabilities.

This thesis aims to present an advanced security framework for IoT devices in healthcare that is intended to ensure data privacy, guarantee data integrity, and keep systems available. The framework adopts a comprehensive strategy, including user authentication, data protection, network security, and device-level security. The objective of this study is to find possible vulnerabilities in the healthcare IoT ecosystem, analyse security solutions, and create effective mitigation plans for such vulnerabilities.

Patient care, communication, and clinical processes have all been altered using IoT devices in healthcare. Despite the many advantages, the growing use of IoT devices also poses several security risks. These difficulties include data security and privacy, data integrity and reliability, security updates, authentication, and access control, as well as regulatory compliance, scalability, and interoperability (Assiri and Almagwashi, 2018). For the healthcare industry to continue to trust IoT devices, preserve sensitive patient data, and ensure the accuracy of health information, these security issues must be resolved. A safe and robust healthcare IoT ecosystem must be built by building advanced security frameworks to address these problems.

IoT devices in healthcare can also improve the efficiency of healthcare delivery by enabling remote consultations and telemedicine. For example, during the COVID-19 pandemic, telemedicine has been extensively used to provide healthcare services remotely to minimize the risk of infection(Ding *et al.*, 2021). A smart pill bottle is one example of an IoT gadget used in healthcare, which may monitor a patient's drug intake patterns (Aldeer *et al.*, 2021). Another illustration is a wearable medical gadget that tracks a patient's heart rate, blood pressure, and other vital indicators and may be used to spot early symptoms of disease or decline(Ahmadi *et al.*, 2019).

IoT devices in healthcare can also improve the efficiency of healthcare delivery by enabling remote consultations and telemedicine. For example, during the COVID-19 pandemic, telemedicine has been extensively used to provide healthcare services remotely to minimize the risk of infection(Ding *et al.*, 2021). A smart pill bottle is one example of an IoT gadget used in healthcare, which may monitor a patient's drug intake patterns (Aldeer *et al.*, 2021). Another illustration is a wearable medical gadget that tracks a patient's heart rate, blood pressure, and other vital indicators and may be used to spot early symptoms of disease or decline(Ahmadi *et al.*, 2019).

An increasing quantity of research has been done on the application of IoT in healthcare. IoT devices can enhance patient outcomes and lower healthcare expenditures, according to certain research. The security

and privacy of IoT devices in healthcare, however, are also issues. It's critical to make sure that the data is secured against unwanted access as these devices capture and communicate sensitive medical data(Butt *et al.*, 2019).

2. Literature Review:

The Internet of Things (IoT) has the potential to revolutionize healthcare by enabling remote patient monitoring and real-time disease management. However, the use of IoT devices in healthcare also introduces significant security risks, as these devices are often vulnerable to attacks that could compromise patient privacy and safety. This literature review examines the current state of the art in IoT security frameworks for healthcare applications. IoT devices in healthcare include a wide range of devices, such as wearable fitness trackers, remote monitoring devices, and smart medical devices (Pradhan, Bhattacharyya and Pal, 2021a). These devices generate a vast amount of data, which is often transmitted wirelessly over the internet. This data can be valuable to both healthcare providers and attackers, making the security of IoT devices in healthcare a critical concern.

One key challenge in securing IoT devices in healthcare is the need to balance security with the need for device availability and ease of use. Much healthcare IoT devices, such as medical devices and telemedicine systems, are critical to patient care and must be reliable and easy to use. At the same time, these devices often handle sensitive patient data and must be protected from cyber threats.

To address this challenge, researchers have developed various approaches to improving the security of IoT devices in healthcare. These approaches include the use of secure communication protocols such as HTTPS and TLS, the implementation of strong authentication methods such as multi-factor authentication(Vegh, 2018), and the deployment of security measures such as firewalls and intrusion detection systems(Hady *et al.*, 2020).

It is important to note that the field of IoT security for healthcare is still relatively new and there are many areas where more research is needed. Some potential gaps in existing knowledge include:

Effectively securing IoT devices with limited resources: Many IoT devices, especially in healthcare, have limited processing power, memory, and other resources. This can make it difficult to implement robust security controls on these devices.

Managing the security of large, complex IoT systems: Healthcare organizations often have networks of many different IoT devices that are used for a variety of purposes. Managing the security of these systems can be challenging due to the complexity of the systems and the potential for attacks to propagate between devices.

Ensuring the security of IoT devices throughout their lifecycle: IoT devices often have a long lifecycle, and it is important to ensure that they remain secure throughout this period. This includes securing the devices during manufacturing, deployment, and maintenance.

Dealing with the unique security risks of IoT in healthcare: Healthcare organizations face several unique security challenges when it comes to IoT, such as the need to protect

sensitive patient data and the potential for devices to be used to disrupt critical medical systems.

Our review identified several key themes in the literature on IoT security for healthcare. One study shows the use of biometric authentication on wearable IoT devices in the healthcare sector (Zheng *et al.*, 2019). The study found that biometric authentication methods, such as fingerprint scanning and facial recognition, can provide a high level of security, but may not be suitable for all types of IoT devices due to the hardware and processing power required. The study also highlighted the importance of considering the usability of these methods for healthcare professionals and patients.

Another study shows the use of multi-factor authentication on medical devices in a hospital setting(Vegh, 2018). The study found that multi-factor authentication can be effective in improving the security of these devices, but also noted that it can be challenging to implement in a way that does not negatively impact the usability of the devices.

One of the major research projects has focused on the development of specific security controls and technologies for IoT devices in healthcare. For example, researchers have proposed the use of encryption, secure boot techniques, and secure firmware updates to protect against attacks on IoT devices(Abdul-Ghani and Konstantas, 2019).

Other research areas in the field of IoT security for healthcare has been the development of frameworks and guidelines for securing these devices. For example, the National Institute of Standards and Technology (NIST) has published a framework for securing the IoT that provides guidance on how to design, implement, and maintain secure IoT systems (Kandasamy *et al.*, 2020).This framework includes several recommendations for healthcare organizations, including the use of strong passwords, the implementation of secure network architecture, and the deployment of security controls at various points in the device lifecycle. A stronger quality of security assurance for healthcare IoT devices and the sensitive data they handle may be achieved by creating a comprehensive security framework that integrates numerous security elements, such as device authentication, data encryption, access control, and intrusion detection.

A further study show investigated two popular encryption techniques for protecting data in transit and at rest are AES and RSA. While RSA is an asymmetric encryption technique that employs a public key for encryption and a private key for decryption, AES is a symmetric key encryption method that uses a single key to encode and decode data(Hamza and Kumar, 2020). By encrypting patient data and communications between devices, these encryption techniques may be utilised to secure healthcare IoT devices, such as patient monitoring systems. This is capable of protecting patient data from unauthorised access and guarantee its confidentiality and integrity.

A clear research problem related to the advancement of security frameworks for IoT devices in healthcare could be: "How can strong authentication methods be effectively implemented on low-power, resource-constrained IoT devices in the healthcare industry, while maintaining a high level of usability for healthcare professionals and patients?"

There is a need for research to explore ways in which strong authentication methods can be implemented on low-power, resource-constrained IoT devices in a way that is both secure and user-friendly. This could involve the development of new authentication methods specifically designed for use on IoT devices, or the adaptation of existing methods to better suit the constraints of these devices.

Understanding how to effectively implement strong authentication on healthcare IoT devices could help to improve the overall security of these devices, reducing the risk of unauthorized access and protecting sensitive patient data. It could also help to ensure that the devices remain easy to use for the healthcare

professionals and patients who rely on them. IoT devices in the healthcare industry often have limited processing power and memory, making it challenging to implement robust security measures such as strong authentication methods. At the same time, these devices must be easy to use for healthcare professionals and patients, as they are an integral part of patient care.

One potential advantage of implementing strong authentication on these devices is that it can help to significantly improve the security of the devices, reducing the risk of unauthorized access and protecting sensitive patient data. Strong authentication methods, such as multi-factor authentication, are generally considered more secure than traditional methods such as username/password combinations and can help to protect against a wide range of cyber threats.

However, there are also several potential disadvantage to consider when implementing strong authentication on healthcare IoT devices. One major challenge is the need to balance security with usability. Many healthcare professionals and patients may not be familiar with more complex authentication methods and may find them difficult or time-consuming to use. This could lead to user frustration and potentially even impact the effectiveness of patient care.

This search may not have been comprehensive, as there may be additional sources that we did not include. Finally, our review focuses only on security frameworks, and does not address other important issues in the use of IoT in healthcare, such as data privacy and interoperability.

IoT security is a critical concern in the healthcare industry, as the use of these devices can introduce significant risks to patient privacy and safety. Our review identified several key themes in the literature on IoT security for healthcare, including the use of encryption methods like AES and RSA, machine learning algorithms for anomaly detection, and multifactor authentication. These findings highlight the need for robust security frameworks to protect IoT devices in healthcare applications.

Summary of journals on security framework for IoT device

Main Focus of journals	Description
a comprehensive resource for information on the various applications of healthcare IoT	The different uses of Internet of Things (IoT) technology in medical equipment are examined in this journal article(Pradhan, Bhattacharyya and Pal, 2021a). The authors highlight how remote monitoring, real-time data gathering, and improved patient care made possible by IoT can revolutionise healthcare. They highlight important sectors, such as wearable technology, telemedicine, and smart hospitals, where IoT has had a substantial influence. The authors also discuss the drawbacks and difficulties of IoT in healthcare, such as infrastructure needs, privacy issues, and data security issues. The journal could provide more insights into emerging trends and future developments in IoT-based healthcare applications, including innovations in sensor technology, data analytics, and artificial intelligence.

Implementing MFA and employing data analytics techniques to improve the overall security of cyber-physical systems	The essential requirement of protecting cyber-physical systems (CPS) is discussed in the journals. These systems are more susceptible to cyber-attacks because to the integration of computational and physical components. In order to maintain safe access, the study highlights the importance of implementing MFA and utilising data analytics for system monitoring and anomaly detection(Vegh, 2018). The study might benefit from case studies or actual examples of cyber-physical systems that have effectively used multi-factor authentication and data analytics.
Analyse and compare the various intrusion detection systems (IDS) created for protecting healthcare systems.	The objective of the study is to determine which IDS is most suited for healthcare contexts, considering the particular problems and needs of this industry, such as protecting private patient data and maintaining the continuity of medical care(Hady *et al.*, 2020). The study aims to offer practitioners and academics working to strengthen the security of healthcare systems against cyber-attacks useful insights through this comparison. However, the paper did not properly explain on how intrusion detection systems can adjust to new cyberthreats, particularly given that hackers are always coming up with new ways to target healthcare systems.
Analyse the potential benefits and effectiveness of distributing keys for wearable and implanted medical device security utilising electrocardiogram (ECG) data.	The research paper explores the possibility of key distribution utilising electrocardiogram (ECG) data to secure wearable and implanted medical equipment. The study considers the particular security issues that wearable and implantable devices face and offers insightful information on the benefits and drawbacks of ECG-based key distribution, as well as its real-world consequences for the security of these medical devices(Zheng *et al.*, 2019). The authors investigate the possibility of producing cryptographic keys for securing communication between medical equipment and other systems using ECG data, a distinctive biometric trait.
In-depth analysis of security and privacy challenges related to the Internet of Things (IoT)	The study examines the numerous and serious security risks and vulnerabilities that IoT systems experience, such as data loss, unauthorised access, and cyberattacks(Abdul-Ghani and Konstantas, 2019). The authors explain the dangers presented by IoT devices and emphasise the necessity for strong security measures by recognising and analysing these threats. The authors suggest and explore various solutions to reduce the detected security risks in IoT systems in response to these threats and vulnerabilities. These security measures, which include things like secure communication protocols, encryption, and access control, can improve the general security and privacy of IoT applications.

Developing effective strategies to manage IoT cyber risks by focusing on cyber risk assessment frameworks, risk vectors, and risk ranking processes.	The NIST Cybersecurity Framework and ISO/IEC 27001 are only two of the frameworks reviewed in the study that may be used to evaluate IoT cyber hazards. To provide users an in-depth understanding of IoT cyber threats, the authors focus on three major areas: frameworks for assessing cyber risk, risk vectors, and risk rating procedures(Kandasamy *et al.*, 2020). Although the study lists many risk vectors, it does not offer a thorough impact analysis of the potential repercussions of cyber hazards related to IoT equipment.
Examine the effects of utilising the TLS (Transport Layer Security) protocol to secure MQTT (Message Queue Telemetry Transport) on performance.	An overview of the MQTT protocol and its uses in IoT applications is given in the article, which is followed by a description of how MQTT messages are secured using the TLS protocol. TLS can give MQTT communications secrecy, integrity, and authentication. The performance effect investigation by the authors examines how utilising TLS to secure MQTT affects message delivery throughput, latency, CPU, and memory utilisation(Prantl *et al.*, 2021). The research can help developers make well-informed choices when it comes to using TLS to encrypt MQTT messages in Internet of Things applications. The impact on other system elements, however, such as network bandwidth utilisation or power usage, which might potentially be important aspects in IoT applications, was not included in the study.
Internet of Things (IoT) application in the medical field.	The paper offers a useful overview of IoT's application in healthcare, addressing a variety of issues and providing information on both the advantages and drawbacks of IoT-based healthcare solutions(Azzawi *et al.*, 2016b). The study conducted by the authors has the potential to help in the creation of IoT-based healthcare solutions that are more effective and efficient for both patients and healthcare professionals. The paper's consideration of potential future avenues for IoT research in healthcare identifies themes including personalised healthcare, illness prevention, and healthcare analytics as promising areas for more study.
investigating the way the Internet of Things (IoT) can help in restricting the COVID-19 epidemic.	The authors discuss about how IoT may be used for things like contact monitoring, social isolation, and remote patient monitoring to help stop the spread of the infection(Castiglione *et al.*, 2021). The use of IoT to contain the epidemic presents both possibilities and problems, including issues with data privacy and security, the requirement for interoperability, and possible advantages of IoT-based solutions.

Investigate ways eHealth might involve remote monitoring and medical device control.	The study offers an insightful examination of the possible uses of remote monitoring and medical device control in eHealth. The authors' analysis of the difficulties and possibilities presented by using these technologies, along with their case studies of eHealth-based solutions put into practise in different nations, can aid in the development of more effective and efficient eHealth-based solutions to enhance patient outcomes and lower healthcare costs(Moustafa *et al.*, 2016). The research is a timely addition to the area of eHealth, which has become even more important in light of the continuing COVID-19 epidemic, and it highlights the potential advantages of remote monitoring and medical device control in enhancing healthcare delivery.
An in-depth examination of the three most widely used encryption protocols: DES, AES, and RSA.	The distinctions between symmetric and asymmetric encryption techniques are included in the authors' comprehensive introduction of cryptography and encryption.(Hamza and Kumar, 2020) Additionally, authors examine the present status of research and development in the area of encryption standards, as well as new algorithms and protocols that could provide better security and functionality (Konstantas, 2019).

3. IoT device in healthcare:

The Internet of Things (IoT) has completely transformed the healthcare industry by enabling the collection, analysis, and sharing of real-time data amongst numerous devices, sensors, and systems(Azzawi *et al.*, 2016a). Patient care, diagnosis, therapy, and overall healthcare administration have all significantly improved because to this networked ecosystem of medical software and hardware.

The following are some significant areas where IoT has impacted healthcare:

1. Remote Patient Monitoring: The Internet of Things (IoT) has completely transformed the healthcare industry by enabling the collection, analysis, and sharing of real-time data amongst numerous devices, sensors, and systems. Patient care, diagnosis, therapy, and overall healthcare administration have all significantly improved because to this networked ecosystem of medical software and hardware(Akkaş, SOKULLU and Ertürk Çetin, 2020).

   By allowing a linked ecosystem of medical devices and apps that enhance patient care, diagnosis, treatment, and overall healthcare management, the Internet of Things (IoT) has had a significant impact on healthcare. Remote patient monitoring (RPM), telemedicine and wearable technology, and mobile health (mHealth), smart hospitals, and medical device management are important areas where IoT has had an impact. Using connected medical devices that continually gather and send patient data, remote patient monitoring in particular enables healthcare personnel to check on patients' health state from a distance(Akkaş, SOKULLU and Ertürk Çetin, 2020). To enable the secure and efficient application of IoT in healthcare settings, issues with data security, privacy, and device interoperability must be resolved.

2. Telemedicine and Telehealth: IoT is used in telemedicine to provide remote consultations, diagnosis, and treatment. This includes video conferencing, remote patient monitoring, and mobile

health apps that let healthcare practitioners give medical services without requiring face-to-face encounters, hence enhancing accessibility to healthcare services, and lowering healthcare expenditures.

Without the need for in-person visits, telemedicine and telehealth make use of IoT technology to deliver remote healthcare services including consultations, diagnosis, and treatment(Castiglione *et al.*, 2021). These services improve access to healthcare, particularly for people who live in distant locations or have mobility problems. Video conferencing, integration of remote patient monitoring, and mobile health applications are important telemedicine and telehealth components. Advantages include enhanced patient happiness, reduced costs, and improved access to healthcare services(Castiglione *et al.*, 2021). To enable the secure and successful use of telemedicine and telehealth in healthcare settings, issues relating to data security, privacy, and regulatory compliance must be resolved.

3. Medical Device Management: Infusion pumps and ventilators are two examples of IoT-enabled medical equipment that may be remotely regulated and maintained. By lowering the chance of device faults and assisting healthcare professionals in ensuring that medical equipment is operating properly, this improves patient care and safety(Castiglione *et al.*, 2021).

   Medical device management in healthcare settings entails being watchful, managing, and maintaining medical equipment. Remote monitoring, predictive maintenance, device configuration and control, asset management and tracking, data security and compliance, and interoperability are all made possible by IoT-enabled medical equipment(Hussain *et al.*, 2022). Improved patient care, operational efficiency, and safety are all results of these skills. To guarantee the secure and efficient use of IoT-enabled medical devices in healthcare settings, however, regulatory compliance issues, data security concerns, privacy concerns, interoperability concerns, and other issues must be addressed.

4. Smart Hospitals: Hospital infrastructures are using IoT devices and sensors to automate procedures, improve patient care, and maximise resource use. Examples include smart beds that can modify patients' postures automatically, patient-specific temperature and lighting settings, and real-time monitoring of medical workers and equipment to increase efficiency.

   IoT technology, automation, and data analytics are used by smart hospitals to optimise medical care, improve productivity, and improve the patient experience. Automated patient care, real-time location systems, environmental controls, integration of remote monitoring and telehealth, data analytics and decision support, improved security, and safety(Yu, Lu and Zhu, 2012). These attributes improve patient care, boost operational effectiveness, improve the patient experience, and reduce costs. To enable the secure and efficient use of IoT technologies in smart hospitals, concerns about data security, privacy, interoperability, and regulatory compliance must be resolved.

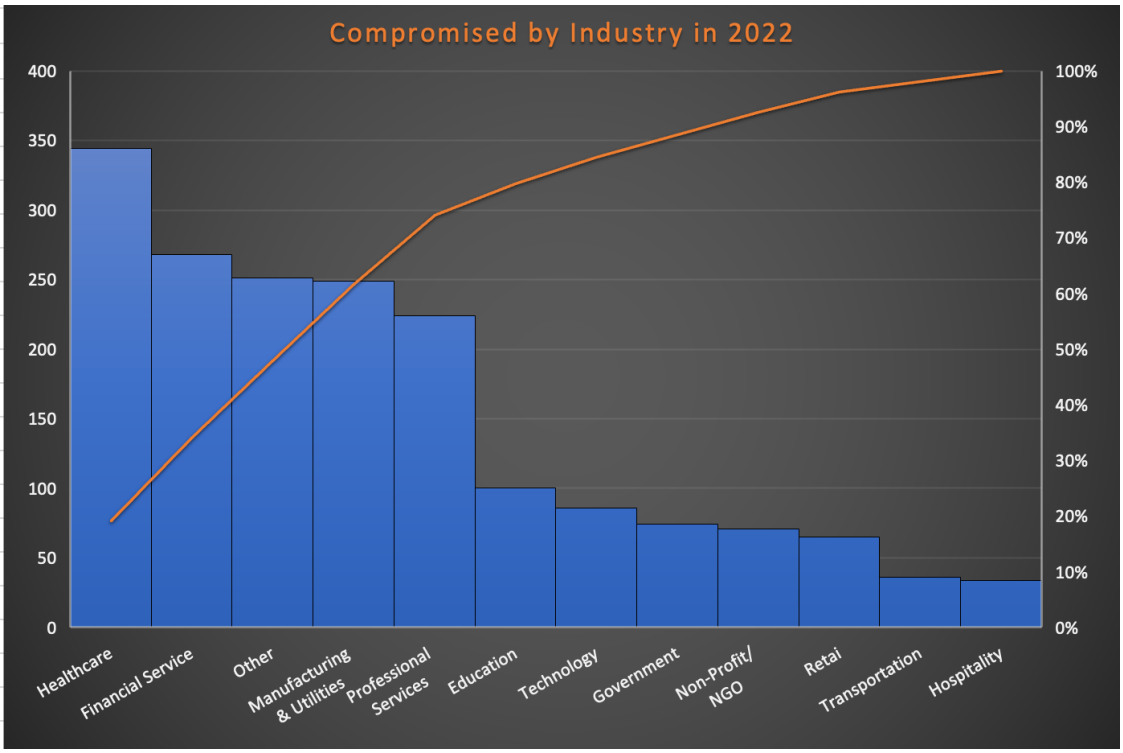


Figure 1:Representation of Data breaches by Industry

The chart above, which is obtained from the website of identity theft research centre, gives an overview of hack incidences in several businesses('ITRC_2022-Data-Breach-Report_Final-1', no date). It shows the overall number of victims for each industry as well as the total number of affected businesses. Education, financial services, government, healthcare, hospitality, manufacturing & utilities, non-profit/non-governmental organisations, professional services, retail, technology, and transportation are among the mentioned sectors. For sectors that don't fall into the given categories, there is also a category called "Other". The overall number of affected businesses and victims across all industries is shown in the table's conclusion. A brief examination of the chart shows that, with 248,564,988 victims, the IT sector has been the most severely harmed. With 980 021 casualties, the Non-Profit/NGO sector had the fewest victims overall. The number of impacted businesses is biggest in the hospitality sector (344), while it is lowest in the education sector (100).With a total of 1,802 impacted firms and 422,143,321 victims, the table demonstrates the huge impact of cyberattacks across many different sectors.

4. C.I.A triad:

A well-known information security model used to direct the implementation of security policies and procedures is the C.I.A. triad, often known as the Confidentiality, Integrity, and Availability triad. The trinity provides a solid basis for protecting the security of sensitive data, systems, and assets across a variety of organisations, including corporations, governmental bodies, and healthcare providers.

- **Confidentiality:** To prevent unwanted access, disclosure, or abuse of sensitive patient data, confidentiality in healthcare IoT devices is crucial. Confidentiality must be maintained not only to comply with data protection laws but also to maintain patient confidence and secure personal database information(Yu, Lu and Zhu, 2012). The collection, transmission, and storage of a large

volume of sensitive patient data by healthcare IoT devices makes it imperative to use the proper security measures.

The following are essential steps to keep healthcare IoT devices confidential:

1. **Data Encryption:** The IoT device for healthcare can utilise data encryption both in transit and at rest while storing data on the device or database. Strong encryption techniques, such as AES or RSA, can be used during the transmission process to secure sensitive patient data from unauthorised access or interception(Bokefode *et al.*, 2016).
2. **Strong Authentication:** Strong authentication techniques, such certificate-based authentication or multi-factor authentication (MFA), can assist in confirming the identities of individuals and devices seeking to access sensitive data(Vegh, 2018). This guarantees that the healthcare IoT ecosystem may only be accessed by approved users and devices.
3. **Secure Communication Protocols:** Data sent between IoT devices, gateways, and cloud services may be protected by using secure communication protocols like HTTPS and TLS (Yu, 2019). These protocols encrypt data as it is being transmitted to prevent snooping or spying.
4. **Access Control**: Only authorised users will be able to access sensitive patient data by using position or attribute-based access control techniques. Organisations can reduce the risk of data breaches and unauthorised access by restricting access to the information required for certain job positions(Aleisa, Abuhussein and Sheldon, 2020).
5. **Security Awareness and Training:** Regular security awareness training can assist healthcare workers in identifying and efficiently addressing possible risks to data confidentiality(Serror *et al.*, 2021). This entails being aware of social engineering threats, securely handling sensitive data, and adhering to recommended procedures for managing devices and passwords.
6. **Regular Security Updates:** Regular software and operating system upgrades for IoT devices used in the healthcare industry can improve in mitigating any software bugs(Serror *et al.*, 2021). Patches for known security breaches as well as improvements to data confidentiality may be included in these upgrades.

- **Integrity:** For the data that these IoT devices gather and analyse to be accurate, reliable, and consistent, they must have integrity. The accuracy of diagnoses, the efficacy of treatments, and the general safety of patients all depend on maintaining data integrity(Hady *et al.*, 2020). It's crucial to implement the right security measures to protect data integrity in IoT healthcare equipment.

The following are important steps to preserve integrity in IoT healthcare devices:

1. **Intrusion Detection System (IDS):** Protecting the integrity of data collected and processed by IoT devices calls for the implementation of IDS solutions, which can monitor and report unwanted modifications to data or systems(Hady *et al.*, 2020). Moreover, these systems can defend against potential data corruption and assist in preventing invasions.
2. **Digital Signatures:** Data integrity may be checked while being sent between devices, gateways, and cloud services using cryptographic hashing techniques (like SHA-256 or MD5) and digital signatures(*Security of Cyber-Physical Systems*, 2020). This improves in the detection of data tampering.
3. **Device and Data Access Monitoring**: It is possible to detect unwanted or suspect activities that might compromise the integrity of data by monitoring access to healthcare IoT devices and data. Installing a central monitoring solution that records and analyses user and device

behaviour can offer insightful information and assist in detecting possible dangers(*Security of Cyber-Physical Systems*, 2020).

4. **Network Security and Segmentation**: The danger of unauthorised data access or manipulation can be reduced by increasing network security and isolating IoT devices on different networks or VLANs. Also, this containment method contributes to preventing the spread of malware and other dangers that can compromise network and data security.

- **Availability**: Healthcare IoT device availability assures that these systems, devices, and data are accessible by authorised users when required. To deliver timely patient care, facilitate successful emergency response, and guarantee the ongoing availability of crucial healthcare services, availability must be maintained. It's essential for the effective operation of healthcare IoT devices to put in place the right safeguards to secure their accessibility.

  The following are important steps to sustain availability in IoT healthcare devices:

1. **Network Security and Monitoring:** IoT devices and data are protected from possible attacks that might affect availability by enhancing network security by installing firewalls, intrusion detection systems, and other security measures in operation(Xiao *et al.*, 2018). In addition, smart network monitoring can identify problems and fix them before they affect service.
2. **Quality of Service (QoS):** Valuable IoT device traffic may be prioritised on networks using QoS methods, ensuring that crucial services and data remain accessible even during periods of severe network load(White, Nallur and Clarke, 2017). The performance of IoT devices can be maintained and bandwidth allotment can be managed using QoS, assuring availability.
3. **Redundancy and Fault Tolerance:** The impact of hardware or software failures on the availability of IoT devices and data may be reduced by using redundancy and fault tolerance solutions, such as redundant hardware components or backup systems(Nasiri *et al.*, 2019). As a result, even in the event of a component failure, crucial services are maintained.
4. **Scalability and Capacity Planning:** As the healthcare organisation expands, maintaining availability may be made easier by ensuring that IoT devices and systems are scalable to handle rising user counts, device counts, or data volumes(Breivold and Sandstrom, 2015). In order to prevent potential service interruptions, effective capacity planning helps estimate future demands and distribute resources appropriately.

5. Implementation and Evaluation

5.1 Implementation of Advanced Security Framework

5.1.1 Selection of Healthcare IoT Devices and Test Environment

A vital step in the evaluation process is selecting the healthcare IoT devices and the testing environment for the advanced security framework. To gain thorough insights into the efficiency of the security framework in various scenarios, it is crucial to select devices that represent a variety of use cases and functionalities.

IoT healthcare device examples include:

- **Wearable health monitors:** By allowing individuals to assume charge of their health and giving healthcare providers useful information for tracking and managing a range of medical diseases, wearable health monitors play a crucial role in the modern healthcare scene. People can track and assess their health metrics in real-time tribute to devices like fitness trackers, smartwatches, heart rate monitors, blood pressure monitors, continuous glucose monitors, and sleep monitors(Karunarathne, Saxena and Khan, 2021). This enables the early detection of potential problems and encourages a proactive approach to health management.

  Also, it is critical to address the security and privacy issues surrounding the sensitive data these devices capture as wearable health monitor use keeps growing. To preserve user privacy and guarantee the secure and efficient use of these reducing health monitoring systems, it is crucial to implement strong security measures, data encryption, and stringent access controls(Karunarathne, Saxena and Khan, 2021). We can maximise the potential of wearable health monitors to improve health outcomes, promote an atmosphere of wellness, and advance preventative treatment by prioritising security and privacy in their development and implementation.

- **Heart rate** monitors are important devices for monitoring heart health, improving exercises, and assessing levels of general fitness. Users may select the best solution for their requirements and preferences from a variety of monitor kinds, including those with a wristband, chest strap and finger-based device.

  The security and privacy issues related to the usage of these devices must be addressed, though, as they capture private health information. We can provide the secure and responsible use of heart rate monitors by adopting strong security measures, data encryption, secure communication protocols, and stringent access controls(Pradhan, Bhattacharyya and Pal, 2021b). This will therefore make it possible for both patients and healthcare workers to take use of the devices' potential to advance better health outcomes, increased fitness, and a proactive approach to wellbeing.

  In this section, we discuss the selection of healthcare IoT devices and the test environment for implementing the advanced security framework. The chosen devices should represent a diverse range of use cases and functionality to ensure comprehensive evaluation.

- **Blood pressure monitors:** Blood pressure monitors are crucial instruments for controlling and monitoring cardiovascular health, especially for people with hypertension or other heart diseases. Users may select the device that suits them most from upper arm monitors, which give the most precise readings, and wrist monitors, which provide convenience and accessibility.

  The sensitive health information gathered by blood pressure monitors raises security and privacy problems, which must be addressed. We can make sure that these technologies are used safely and responsibly by installing strong security measures, data encryption, secure communication protocols, and stringent access restrictions(Pradhan, Bhattacharyya and Pal, 2021b). Adopting security and privacy first in blood pressure monitoring will help both patients and medical professionals manage cardiovascular health more successfully, improve medical results, and support a proactive approach to wellness.

- **Sleep monitors:** A person's entire sleep health can be better understood with the use of sleep monitors, which are tools for tracking sleep quality, duration, and patterns(Pradhan, Bhattacharyya

and Pal, 2021b). For someone's physical and mental health, getting enough sleep is essential, and keeping track of someone's sleep patterns can help spot problems before they become serious.

To monitor sleep quality and patterns, a variety of sleep monitors are available. They comprise contactless monitors, wearable monitors, bedside monitors, and monitors that are attached to the bed. Each of these monitors uses a different technology and approach to evaluate sleep. While some gadgets need to be near the user, others offer non-intrusive surveillance for a peaceful sleep. Patient may select the sleep monitor that best satisfies their tastes and requirements to learn important details about the quality of their sleep.

5.1.2 Implementation of Security Framework using Python:

5.1.2.1 Encryption and Decryption Algorithms:

For IoT healthcare devices, implementing encryption and decryption methods like AES and RSA is essential for ensuring data security and privacy. Sensitive patient data sent between IoT devices and healthcare systems remains secure by these algorithms.

- **AES (Advanced Encryption Standard):**

The National Institute of Standards and Technology (NIST) developed the Advanced Encryption Standard (AES), a symmetric encryption algorithm that utilises the same key for both encryption and decryption(Alabdullah, Beloff and White, 2021). It has gained widespread acceptance as a worldwide standard, providing a high level of security and great performance on a variety of hardware and software, making it the best option for real-time data transmission in Internet of Things healthcare devices(Alabdullah, Beloff and White, 2021). Due to its resilience to well-known cryptographic attacks and its huge key sizes, which offer strong protection against brute-force assaults, AES is highly secure. Due to its symmetric design, which enables quick encryption and decryption, it is ideally suited for Internet of Things (IoT) devices with limited power consumption. AES may be used to encrypt data on a broad range of devices, including powerful servers and IoT devices, and its wide availability assures uncomplicated data transfer across different systems(Yahaya and Ajibola, 2019). It is essential to use secure key management techniques when utilising AES for IoT healthcare equipment, such as creating strong random keys and securely storing and exchanging them. The security of IoT healthcare systems may also be increased by adopting authorised encryption techniques like AES-GCM or AES-CCM, which can provide both secrecy and data integrity(Magdum, 2023).

Galois/Counter Mode (GCM) was used by the Advanced Encryption Standard (AES) for both encryption and decryption. AES-GCM is the specific algorithm employed. For block cyphers like AES, GCM is an authorised encryption mode that offers both data integrity and confidentiality(Menezes and Stebila, 2021). Due to its effectiveness and effective security features, it is frequently used. NIST (National Institute of Standards and Technology) advises using AES-GCM to protect sensitive data.(Menezes and Stebila, 2021) The key derivation algorithm known as PBKDF2 applies a predetermined number of iterations and a pseudorandom function (in this case, HMAC-SHA256) to the input password and salt. This procedure aids in producing a derived key that is challenging for an adversary to decipher.

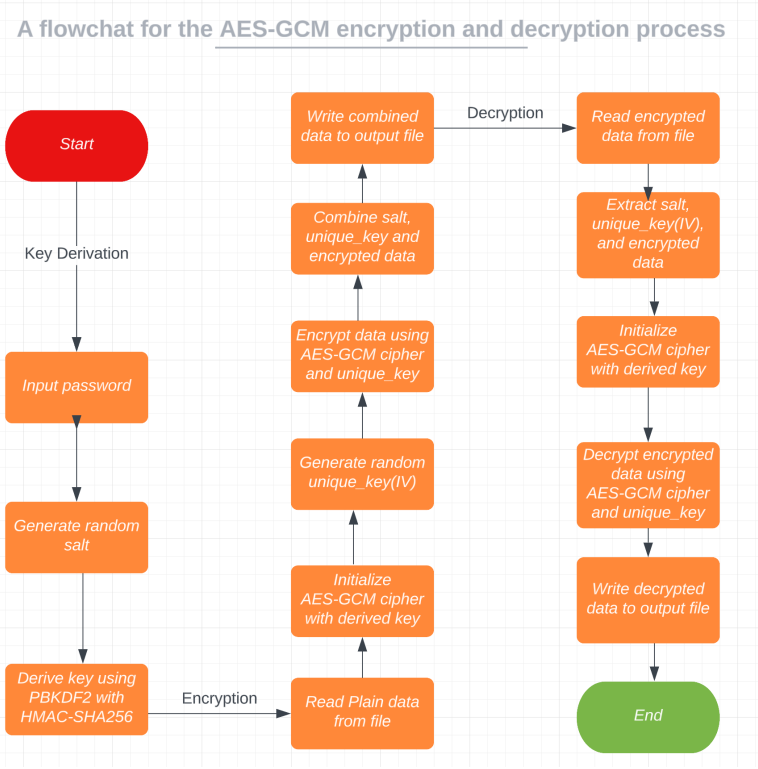


Figure2: Flowchart of Advanced Encryption Standard (AES)

Data security is crucial in the context of IoT healthcare devices since these gadgets deal with private patient information. AES-GCM was selected as the preferred encryption method because it provides a high degree of security and performance, making it suited for securing healthcare data.

Secure key management is necessary for healthcare IoT devices to protect sensitive information from unauthorised access. Its excellent resistance to brute-force and dictionary attacks led to the selection of PBKDF2-HMAC-SHA256, a key derivation function that is well-known and frequently advised(Choi and Seo, 2021). Due to the potentially serious effects of unauthorised access to patient information, this resilience is especially crucial for protecting healthcare data. Utilising PBKDF2-HMAC-SHA256 will guarantee that the obtained keys are safe and appropriate for use in encryption and decryption procedures.

- **RSA (Rivest-Shamir-Adleman):**

Asymmetric encryption, such as the Rivest-Shamir-Adleman (RSA) method, which employs a public key for encryption and a private key for decryption, offers a high level of security but is slower than symmetric algorithms like AES(Bansal, Gupta and Mathur, 2021). The security of the public-private key pair, which is the basis of the 1977-developed RSA algorithm, is predicated on the mathematical complexity of factoring large prime numbers(Pathirage *et al.*, 2021). Digital signatures for data integrity and authenticity, as well as scalability for key management in big networks, are just a few benefits that RSA offers. However, RSA has several drawbacks when employed in IoT healthcare devices, such as its computationally demanding nature, which causes poorer performance when compared to AES, and limitations on the amount of the encryption. To overcome these difficulties, a hybrid strategy is often employed, in which RSA is used to safely exchange AES keys and then AES is used to encrypt and decode the real data(Bharathi *et al.*, 2021). With this approach, a complete encryption solution for IoT healthcare equipment is provided, combining the efficiency of AES with the security advantages of RSA.

```
function generate_rsa_key_pair():
    private_key = generate_private_key()
    public_key = get_public_key(private_key)

    private_pem = serialize_private_key(private_key)
    public_pem = serialize_public_key(public_key)

    save_to_file(private_pem, "private_key.pem")
    save_to_file(public_pem, "public_key.pem")
```

Figure 3: Pseudo-code RSA key Generation

```
function encryption_rsa(file_path, public_key_file):
    data = read_data(file_path)
    public_key = load_public_key(public_key_file)

    key_aes = generate_aes_key()
    data_encrypted, unique_key = encrypt_data_aes(data, key_aes)

    aes_encrypted_key = encrypt_aes_key_rsa(key_aes, public_key)

    save_encrypted_data(encrypted_file_path, unique_key, aes_encrypted_key, data_encrypted)
```

Figure 4:Pseudo-code RSA Encryption (Hybrid with AES-GCM)

```
function rsa_decrypt(file_path, private_key_file):
    unique_key, encrypted_aes_key, data_encrypted = read_encrypted_data(file_path)
    private_key = load_private_key(private_key_file)

    decrypted_aes_key = decrypt_aes_key_rsa(encrypted_aes_key, private_key)
    data_decrypted = decrypt_data_aes(unique_key, data_encrypted, decrypted_aes_key)

    save_decrypted_data(decrypted_file_path, data_decrypted)
```

Figure 5:pseudo-code RSA Decryption (Hybrid with AES-GCM

In a hybrid approach, AES and RSA algorithms are merged to improve the framework's security and effectiveness. Contribution to the security architecture: The hybrid encryption solution uses AES-GCM to encrypt and decode the data. The security framework achieves a compromise between the security advantages of public-key cryptography and the performance advantages of symmetric encryption by integrating RSA for public-key encryption and AES-GCM for effective symmetric encryption. Although RSA offers public-key encryption, it cannot be used to encrypt huge databases. The advantages of both methods are combined by encrypting data with AES-GCM and the AES key with RSA, resulting in a more effective and secure method of securing sensitive data in a healthcare IoT environment.

```
# ==================================================AES methods=========================
def encryption_aes(self):
    print("AES Encrypt method called") # method called check
    time_start = time.time()  # performance time start

    file_path = filedialog.askopenfilename(initialdir = "/",title = "Select file",
                                           filetypes = (("csv files","*.csv"),("all files","*.*")))


    password = "your_password_here"  # password input from the user
    salt = os.urandom(16) #Generates a random 16-byte salt (cryptography value)
    key = self.aes_hash_key(password, salt)
    with open(file_path, "rb") as file:
        data = file.read()

    aes_gcm = AESGCM(key)
    unique_key = os.urandom(12) #Encrypts the data with the AES-GCM cipher
    ct = aes_gcm.encrypt(unique_key, data, None)
    data_encrypted = salt + unique_key + ct

    with open(file_path + ".enc", "wb") as file:
        file.write(data_encrypted)
    # performance
    time_end = time.time()
    time_elapsed = time_end - time_start
    self.performance_data["AES"]["encrypt"].append(time_elapsed)

def decryption_aes(self):
    time_start = time.time()  # Performance time start
    file_path = filedialog.askopenfilename(title="Choose a file to decrypt")
    password = "your_password_here"  # Replace with a proper password input from the user
    with open(file_path, "rb") as file:
        encrypted_data = file.read()

    salt = encrypted_data[:16]
    unique_key = encrypted_data[16:28]
    ct = encrypted_data[28:]
    key = self.aes_hash_key(password, salt)

    aes_gcm = AESGCM(key)
    data = aes_gcm.decrypt(unique_key, ct, None)

    output_file_path = filedialog.asksaveasfilename(title="Save decrypted file")
    with open(output_file_path, "wb") as file:
        file.write(data)
    # performance
    time_end = time.time()
    time_elapsed = time_end - time_start
    self.performance_data["AES"]["decrypt"].append(time_elapsed)
```

Figure 6: Implementation of AES encryption and decryption

The ‘encryption_aes’ function, which was developed to provide safe encryption for a file's contents, encrypts files using the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM), as seen in Figure 2 above. The user is then given the option of selecting a CSV file or another file type and is then prompted to choose a file for encryption using a file dialogue. The data in the chosen file is then read and encrypted with an AES-GCM cypher and derived key.

The key is created using an encoded password and a 16-byte salt (cryptography value) that is produced randomly in order to protect against cyber - physical attacks and support the password-derived key. The aes_hash_key function is in responsible for generating the AES key from the password and salt. To provide semantic security, the same plaintext encrypted with the same key produces distinct ciphertexts,

which is ensured by a 12-byte random key. Without additional linked information, the data is encrypted with the derived key, created unique key generator, and AES-GCM cypher. In order to ensure that the salt and cryptographic nonce can be retrieved during decryption in order to rebuild the AES key and properly decode the data, the salt and cryptographic nonce are combined with the ciphertext to form the encrypted data.

Finally, a new file with the same directory as the original file and the ".enc" extension is created and contains the encrypted data. The contents of the original file are encrypted in this file. The function also calculates the length of time needed for encryption and stores that information in the 'self.performance_data' dictionary, which may be used to evaluate how well the encryption process performed.

```python
def encryption_rsa(self):
    print("RSA Encrypt method called") # method called check
    start_time = time.time()  # Performance time start
    if not self.public_key:
        print("Please select a public key.")
        return
    file_path = filedialog.askopenfilename(initialdir = "/",title = "Select file",
                                           filetypes = (("csv files","*.csv"),("all files","*.*")))


    with open(file_path, "rb") as file:
        data = file.read()

    with open(self.public_key, "rb") as key_file:
        public_key = serialization.load_pem_public_key(
            key_file.read(),
            backend=default_backend()
        )

    # Generate a random AES key
    key_aes = os.urandom(32)

    # Encrypt the data using the AES key
    aesgcm = AESGCM(key_aes)
    unique_key = os.urandom(12)
    data_encrypted = aesgcm.encrypt(unique_key, data, None)

    # Encrypt the AES key using the RSA public key
    aes_encrypted_key = public_key.encrypt(
        key_aes,
        padding.OAEP(
            mgf=padding.MGF1(algorithm=hashes.SHA256()),
            algorithm=hashes.SHA256(),
            label=None
        )
    )

    # Save the encrypted AES key, nonce, and encrypted data to a file
    encrypted_file_path = file_path + ".enc"
    with open(encrypted_file_path, "wb") as encrypted_file:
        encrypted_file.write(unique_key)
        encrypted_file.write(aes_encrypted_key)
        encrypted_file.write(data_encrypted)

    print(f"Encrypted file saved to: {encrypted_file_path}")

    end_time = time.time()
    elapsed_time = end_time - start_time
    self.performance_data["RSA"]["encrypt"].append(elapsed_time)
```

Figure 7: Implementation of RSA encryption

```python
def rsa_decrypt(self):
    start_time = time.time()
    if not self.private_key:
        print("Please select a private key.")
        return

    file_path = filedialog.askopenfilename(title="Choose an encrypted file to decrypt")

    with open(file_path, "rb") as file:
        unique_key = file.read(12)  # Read the key (12 bytes)
        encrypted_aes_key = file.read(256)  # Read the encrypted AES key (assuming a 2048-bit RSA key)
        data_encrypted = file.read()  # Read the remaining encrypted data

    with open(self.private_key, "rb") as key_file:
        private_key = serialization.load_pem_private_key(
            key_file.read(),
            password=None,
            backend=default_backend()
        )

    # Decrypt the AES key using the RSA private key
    decrypted_aes_key = private_key.decrypt(
        encrypted_aes_key,
        padding.OAEP(
            mgf=padding.MGF1(algorithm=hashes.SHA256()),
            algorithm=hashes.SHA256(),
            label=None
        )
    )

    # Decrypt the data using the decrypted AES key
    aesgcm = AESGCM(decrypted_aes_key)
    data_decrypted = aesgcm.decrypt(unique_key, data_encrypted, None)

    # Save the decrypted data to a file
    decrypted_file_path = file_path.rstrip(".enc") + "_decrypted"
    with open(decrypted_file_path, "wb") as decrypted_file:
        decrypted_file.write(data_decrypted)

    print(f"Decrypted file saved to: {decrypted_file_path}")

    end_time = time.time()
    elapsed_time = end_time - start_time
    self.performance_data["RSA"]["decrypt"].append(elapsed_time)
```

Figure 8: Implementation of RSA decryption

```python
def rsa_key_generate(self):
    private_key = rsa.generate_private_key(
        public_exponent=65537,
        key_size=2048,
        backend=default_backend()
    )

    public_key = private_key.public_key()

    private_pem = private_key.private_bytes(
        encoding=serialization.Encoding.PEM,
        format=serialization.PrivateFormat.PKCS8,
        encryption_algorithm=serialization.NoEncryption()
    )

    public_pem = public_key.public_bytes(
        encoding=serialization.Encoding.PEM,
        format=serialization.PublicFormat.SubjectPublicKeyInfo
    )

    with open("private_key.pem", "wb") as private_key_file:
        private_key_file.write(private_pem)

    with open("public_key.pem", "wb") as public_key_file:
        public_key_file.write(public_pem)
```

Figure 9: Public key and Private key for RSA

The function in figure 7 & 8 above uses a hybrid RSA-AES encryption method to encrypt a chosen file by user. A public key needs to first be sure to be accessible. The user is then presented with a file dialogue to

choose a file for encryption. The data is then encrypted using AES-GCM using a random AES key. Using the RSA public key and OAEP padding, the produced AES key is encrypted. Finally, a new file with the ".enc" extension is created and saved with the cryptographic nonce (unique_key), encrypted AES key, and encrypted data. Additionally, the function calculates the length of time required for encryption and puts the result in the self.performance_data dictionary.

Figure 7 above using the ‘encryption_rsa’ function, this function decrypts a file that has been encrypted. The user is prompted to choose an encrypted file for decryption when the programme determines whether a private key is available. The file is read to obtain the cryptographic nonce (unique_key), encrypted AES key, and encrypted contents. The AES key is decrypted using the private key, and the data is then decrypted using AES-GCM. The encrypted information is stored to a new file with the prefix "_decrypted" after the file name. The function also calculates and maintains the length of time required for the decryption ‘self.performance_data’ dictionary.

Figure 9 above shows a method for creating an RSA key pair, which consists of a private key and a public key. The key pair is produced using a 2048-bit key size and a public exponent of 65537(Patgiri and Singh, 2022). The public key is recorded in the PEM format using the SubjectPublicKeyInfo encoding, while the private key is saved in the PEM format using PKCS8 encoding without encryption(Patgiri and Singh, 2022). The files "private_key.pem" and "public_key.pem" provide the keys' respective locations of storage in the operating system.

5.1.2.2 Anomaly Detection System:

Every security architecture for IoT devices used in healthcare must include anomaly detection. An unexpected or suspicious behaviour on the device, such as data theft, unauthorised access, or other possible security risks, can be found with the use of anomaly detection. The Isolation Forest algorithm is one useful method for anomaly identification(Carletti, Terzi and Susto, 2020).

A machine learning approach that works well for tasks requiring anomaly detection is the isolation forest algorithm. By building a series of decision trees, the algorithm divides the data into progressively smaller subgroups until each subset includes just one instance. The programme then evaluates each instance's anomaly according to how many splits are necessary to separate it from the rest of the data. High anomaly score instances are considered as anomalies(Carletti, Terzi and Susto, 2020).

```
def data_load(self):
    options = QFileDialog.Options()
    file_name, _ = QFileDialog.getOpenFileName(self, "Load Data", "", "CSV Files (*.csv);;All Files (*)",
                                               options=options)
    if file_name:
        self.data = pd.read_csv(file_name)
        self.label_status.setText(f"Data loaded: {file_name}")

def analyze_data(self):
    if not hasattr(self, 'data'):
        self.label_status.setText("Error: No data loaded")
        return

    # Split data into train and test sets
    train_data, test_data, train_labels, test_labels = self.split_data(self.data)

    # Preprocess data
    preprocessed_train_data = self.data_preprocessing(train_data)

    # Train the model
    model = self.model_train(preprocessed_train_data, train_labels)

    # Evaluate the model
    self.evaluate_model(model, test_data, test_labels)

    # Visualize the results
    preprocessed_data = self.data_preprocessing(self.data.iloc[:, :-1])
    self.visualize_results(preprocessed_data, model)

def split_data(self, data):
    X = data.iloc[:, :-1]
    y = data.iloc[:, -1]
    X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42, stratify=y)
    return X_train, X_test, y_train, y_test

def model_train(self, preprocessed_data, labels):
    # Applying the Logistic Regression model
    model = LogisticRegression(random_state=42)

    # Fit the model to the preprocessed dataset
    model.fit(preprocessed_data, labels)
    return model
```

Figure 10: Anomaly Detection System for Dataset in python

Python tools like Scikit-Learn or PyOD may be used to create the model and apply the Isolation Forest technique for anomaly detection in healthcare IoT device data. Preparing the data from the healthcare IoT device for analysis is the first step. This might entail picking pertinent characteristics for the model as well as cleaning and processing the data(Lin, Lin and Yeh, 2021). The pertinent characteristics are chosen from the pre-processed data and used as inputs for the Isolation Forest algorithm. This stage could entail reducing the number of features using dimensionality reduction methods like Principal Component Analysis (PCA).

The Logistic Regression model can be trained on the pre-processed and chosen characteristics of the healthcare IoT device data after feature selection(Hasan *et al.*, 2019). The number of splits necessary to separate an instance from the rest of the data should be used to train the model to detect anomalies. A test dataset containing data from healthcare IoT devices is used to assess the model's performance once it has been trained. To evaluate the effectiveness of the model, this stage could entail employing measures like accuracy, false positive/negative rates, and response time. Following testing Logistic Regression model can be implemented on the healthcare IoT device to evaluate incoming data in real-time and classify it as normal or abnormal based on how many splits are necessary to isolate an instance from the rest of the data(Hasan *et al.*, 2019).

5.1.2.3 IDS/IPS with Machine Learning:

The IoT healthcare device can be protected against security threats with the use of cybersecurity technologies like an intrusion detection system (IDS) and intrusion prevention system (IPS) with the use of machine learning.

- **Intrusion Detection System (IDS):**
  A security system called an intrusion detection system (IDS) monitors network traffic for indications of unauthorised access, hostile activity, or other security breaches. It operates by

looking for patterns in network traffic that correspond to well-known attack signatures or unusual behaviour(Saranya *et al.*, 2020). An IDS will send out an alert to security staff when it discovers a possible security concern.

The primary objective of an IDS is to quickly identify potential security risks so that necessary measures may be taken to either avoid or mitigate them. An IDS generally operates by continuously observing network traffic and comparing it to a database of known attack signatures or anomalous behaviour patterns. The IDS model has utilized the machine learning method called Random Forest for intrusion detection. Numerous feature selection algorithms are used in Random Forest, an ensemble learning technique, to increase accuracy overall and minimise overfitting(Saranya *et al.*, 2020). Since it can handle huge datasets and high-dimensional characteristics, which are prevalent in the IoT area, Random Forest Classifier was selected for the security framework. Additionally, the algorithm is accurate and strong, making it appropriate for spotting intrusions in IoT devices used in healthcare, where false positives or false negatives might have detrimental effects.
The Random Forest algorithm may be trained on a specific dataset of network traffic data to uncover patterns that point to possible security vulnerabilities in the context of intrusion detection. The technique may then be used to classify malicious form regular healthcare network data in real-time(Choubisa *et al.*, 2022).

```
# ==================================Intrusion Detection System(IDS) model====================================

class IDSModel:
    def __init__(self):
        # RandomForestClassifier with 100 trees and a random state of 42.
        self.model = RandomForestClassifier(n_estimators=100, random_state=42)

    def train(self, X_train, y_train):  # fit the model on the training data
        self.model.fit(X_train, y_train)

    def predict(self, X_test):  # to make predictions on the test data.
        return self.model.predict(X_test)

    def evaluate(self, y_test,
                 y_pred):  # method to calculate the accuracy, confusion matrix, and classification report.
        accuracy = accuracy_score(y_test, y_pred)
        conf_mat = confusion_matrix(y_test, y_pred)
        class_report = classification_report(y_test, y_pred)

        return accuracy, conf_mat, class_report


# Initializing the IDSModel class
ids_model = IDSModel()

# Training the model using the preprocessed training dataset
ids_model.train(train_x, train_y)

# Predictions on the preprocessed testing dataset
y_pred = ids_model.predict(test_x)

# Evaluate the model's performance
accuracy, conf_mat, class_report = ids_model.evaluate(test_y, y_pred)

# Display the evaluation metrics
print("Accuracy:", accuracy)
print("Confusion Matrix:\n", conf_mat)
print("Classification Report:\n", class_report)
```

Figure 11: IDS model implementation in python

The network traffic data must be pre-processed to make it suitable for analysis when using the Random Forest method for an IDS model. It is possible to choose pertinent characteristics from the pre-processed data to include in the Random Forest model. Then, using the chosen characteristics, the model is trained on a labelled dataset of network traffic data to classify incoming traffic as normal or malicious(Choubisa *et al.*, 2022). Metrics including accuracy, precision, recall, and F1 score are used to assess the model's performance(Guia, Silva and Bernardino, 2019). Once implemented, the Random Forest model may rapidly and precisely identify possible security vulnerabilities, enhancing the IoT healthcare device's overall security.

As the main method for the Intrusion Detection System (IDS), the Random Forest Classifier is used. By identifying them as attack or normal incidents, the IDS model seeks to identify network intrusions. The method is tested using multiple metrics, including accuracy, confusion matrix, and classification report, after it has been trained on a pre-processed dataset.

- **Intrusion Prevention System(IPS):**

An Intrusion Prevention System (IPS) is a more efficient security system that actively works to prevent possible security attacks in addition to the detection capabilities of an IDS. By evaluating network traffic and comparing it to a list of established security policies, an IPS analyses network activity. If any of the policies are broken by the traffic, the IPS can immediately take action to either block or lessen the threat(Disha and Waheed, 2022).

A very effective security technique to protect an IoT healthcare equipment from potential security risks is an IPS system with IP address blocking and alerting capabilities. Such a system operates through real-time network traffic analysis and notify administrators. An IPS system can take action to block the offending IP address when it discovers possible security issues, stopping additional assaults or data espionage(Disha and Waheed, 2022). Administrators can get warnings from the IPS system informing them of attempted attacks and giving them details like the source IP address, attack type, and time of attack.

```python
class IPSModel:
    def __init__(self):
        self.model = RandomForestClassifier(n_estimators=100, random_state=42)

    def train(self, X_train, y_train):
        self.model.fit(X_train, y_train)

    def predict(self, X_test):
        return self.model.predict(X_test)

    def evaluate(self, y_test, y_pred):
        accuracy = accuracy_score(y_test, y_pred)
        conf_mat = confusion_matrix(y_test, y_pred)
        class_report = classification_report(y_test, y_pred)

        return accuracy, conf_mat, class_report

    def prevent(self, input_data):
        # Make predictions using the model
        predictions = self.predict(input_data)

        # Iterate over the input_data and corresponding predictions
        for i, (data, prediction) in enumerate(zip(input_data, predictions)):
            if prediction == 1:  # If the model predicts an attack
                print(f"Potential DDOS attack detected for data entry {i}")

                # Extract the IP address from the input data
                # Note: replace 'ip_address' with the correct column name in your dataset
                ip_address = data['ip_address']

                # Block the IP address and alert the administrator
                block_ip_address(ip_address)
                alert_administrator(ip_address)

            else:
                print(f"No attack detected for data entry {i}")

# Initialize the IPSModel
ips_model = IPSModel()
# Train the model using the preprocessed training dataset
ips_model.train(train_x, train_y)
# Make predictions on the preprocessed testing dataset
y_pred = ips_model.predict(test_x)
# Evaluate the model's performance
accuracy, conf_mat, class_report = ips_model.evaluate(test_y, y_pred)
# Display the evaluation metrics
print("Accuracy:", accuracy)
print("Confusion Matrix:\n", conf_mat)
print("Classification Report:\n", class_report)
```

Figure 12: IPS implementation

```python
# ==========Email alert of admin for (DDOS attack)  prevention==========


EMAIL_SERVER = "smtp.example.com"
EMAIL_PORT = 587  # Typically, 587 for STARTTLS or 465 for SSL
EMAIL_ADDRESS = "sk1234.@gmail.com"
EMAIL_PASSWORD = "1234abc"
ADMIN_EMAIL = "NHSadmin@gmail.com"

from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText


def alert_administrator(ip):
    # Create a message object
    msg = MIMEMultipart()

    # Set the email subject, sender, and recipient
    msg["Subject"] = "Potential DDOS attack detected"
    msg["From"] = EMAIL_ADDRESS
    msg["To"] = ADMIN_EMAIL

    # Create the email body
    body = f"Alerting administrator about a potential DDOS attack from IP address: {ip}"

    # Attach the email body to the message object
    msg.attach(MIMEText(body, "plain"))

    # Connect to the email server
    server = smtplib.SMTP(EMAIL_SERVER, EMAIL_PORT)
    server.starttls()  # Use this line for STARTTLS. Remove it if using SSL.
    server.login(EMAIL_ADDRESS, EMAIL_PASSWORD)

    # Send the email
    server.sendmail(EMAIL_ADDRESS, ADMIN_EMAIL, msg.as_string())

    # Close the connection to the email server
    server.quit()

    print(f"Alert sent to administrator about potential DDOS attack from IP address: {ip}")
```

Figure 23: Email alert system.

```python
# ==========IP blocking system for prevention==========

FIREWALL_API_URL = "https://firewall.example.com/api"


def block_ip_address(ip):
    # Define the API endpoint for adding a blocked IP address
    url = f"{FIREWALL_API_URL}/block_ip"
    # IP address to be blocked
    ip = "192.168.1.1"_# Example of hacker Ip address

    # Define the payload with the IP address
    data = {
        "ip_address": ip
    }

    # Sending a request to the firewall API to block the IP address
    response = requests.post(url, json=data)

    # Checking the request
    if response.status_code == 200:
        print(f"Blocking IP address: {ip}")
    else:
        print(f"Error blocking IP address {ip}: {response.text}")
```

Figure 14: IP blocking system.

The above framework used Python tools like Scapy or Pyshark can be applied to record and analyse network traffic in real-time to create an IPS system with IP address filtering and alerting features. The IPS system can be set up to compare network traffic to established security policies, such as those that block known malicious IP addresses or prevent types of network traffic from accessing private data on IoT medical devices. The IPS system can operate to block the offending IP address when a DDOS attack is found. Moreover, the IPS system can produce warnings to inform administrators of the attempted attack, enabling them to take additional steps to investigate and address the security event. An IPS system may be set up to perform additional measures to stop possible security concerns in addition to blocking IP addresses and sending out alerts. It might be set up to drop packets that fit a certain pattern or to change the source or destination IP address of packets to stop the DoS attack in healthcare network.

5.1.3 Integration of Security Measures

Implementing an improved security framework for IoT devices used in healthcare requires the integration of security mechanisms. Strong data encryption techniques must be used for both information in storage and information during transmission, using complex algorithms like AES or RSA, to ensure data confidentiality, integrity, and availability. To restrict access to sensitive patient data, use access control techniques like role-based or attribute-based access control. This will reduce the risk of data breaches and unauthorised access. For confirming the identities of people and devices connected to the healthcare IoT ecosystem, strong authentication techniques are necessary. They include multi-factor authentication (MFA)

and certificate-based authentication. Also, to secure data while it is being transmitted and avoid snooping or detection, secure communication protocols like HTTPS must be used(Tukade and Banakar, 2018).

Furthermore, to address any security flaws and strengthen data protection procedures, regular security upgrades, including firmware and software updates, are required. In order to assist healthcare workers, understand and successfully respond to possible risks, such as social engineering assaults and following to best practises for managing sensitive data and device management, frequent security awareness and training is essential. The advanced security framework can efficiently protect sensitive patient data and guarantee a secure and dependable IoT environment in healthcare settings by including these security measures into the design and operation of healthcare IoT devices.

5.1.4 Development of Monitoring and Management Tools

For the healthcare IoT ecosystem to successfully manage security, monitoring and management solutions must be developed. Real-time information and control over devices and their data are made possible by these technologies, which also preserve system efficiency and speed up issue response. With centralised dashboards, managers can monitor system health and spot any security risks by having a single view of the whole healthcare IoT infrastructure, which shows connected device status, security warnings, and performance data(Lee, 2020). To notify managers to suspected malicious activity or security breaches, intrusion detection systems (IDS) analyse network traffic and identify potential threats in real-time.

Moreover, Security-related events and logs are gathered and analysed by Security Information and Event Management (SIEM) technologies, which also improve incident response by spotting patterns suggestive of security concerns(*ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) EVASION AND DETECTION METHODS*, 2016). To manage IoT devices, update firmware and software, adjust security settings, and monitor device health and performance, administrators can use device management solutions. analytics tools evaluate huge volumes of data from IoT devices to produce insights into device performance, use trends, and possible security threats. These insights allow administrators to proactively solve issues and improve performance. By putting these monitoring and management technologies in place, healthcare IoT ecosystems become more secure, possible threats are quickly identified and addressed, and IoT device dependability is maintained for secure and effective healthcare IoT technology use.

5.2 Evaluation of the Advanced Security Framework

The Advanced Security Framework is a comprehensive plan for securing the availability, confidentiality, and integrity of digital assets and networks. In order to build a multi-layered defence against a variety of cyber threats, the framework implies several security technologies and approaches, such as encryption/decryption, anomaly detection, intrusion prevention systems (IPS), and intrusion detection systems (IDS). This framework's key objectives are to preserve sensitive data, keep systems reliable, and shield organisations from the disastrous effects of data breaches and cyberattacks.

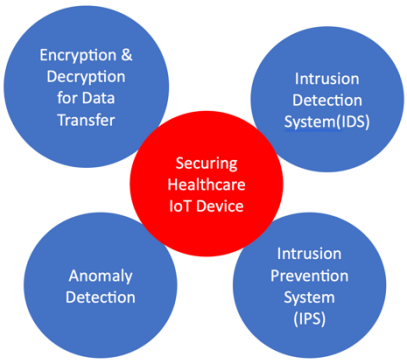
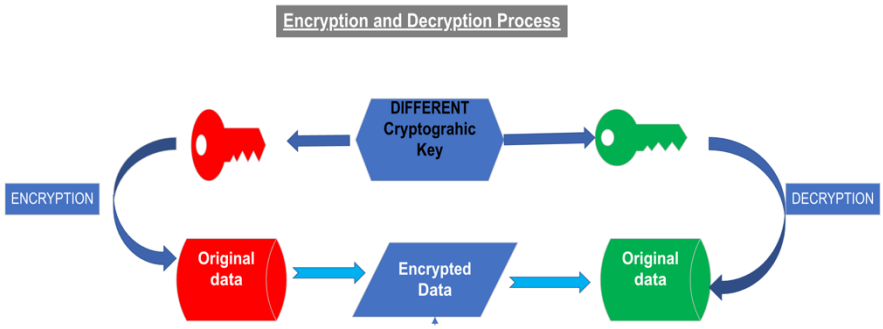


Figure 15: Advance Security Framework

The encryption/decryption algorithms, such as AES and RSA, ensure data confidentiality and privacy by securing data during transmission and storage, thereby preventing unauthorized access to sensitive information. Anomaly detection contributes to the framework by monitoring and analysing network traffic, system events, and user behaviour, detecting unusual patterns or deviations from the norm. This early identification of potential threats and attacks enables organizations to respond quickly and mitigate potential damage. The Intrusion Prevention System (IPS) actively safeguards the network by blocking malicious traffic, identifying, and thwarting exploitation attempts, and preventing the spread of malware within the network. In the meanwhile, the Intrusion Detection System (IDS) performs the role of a passive monitor, identifying and evaluating potential intrusions and attacks, assisting in determining the nature of threats, and enabling targeted actions to guarantee system availability and integrity. Organisations may get a high level of safety and protection against the constantly changing environment of cyber threats by integrating these elements into a unified architecture.

- **Encryption/Decryption (AES, RSA):**

  By transforming plaintext data into ciphertext and vice versa, respectively, encryption and decryption play a crucial part in protecting data transport and storage. With the help of this procedure, sensitive data is kept private and out of the hands of unauthorised individuals. When sending data via networks, encryption is especially important since it shields the information from snooping and tampering. Additionally, even if physical or digital security measures are violated, encrypting stored data provides protection against unauthorised access.



The Advanced Security Framework uses the popular cryptographic algorithms AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman). Both algorithms have certain advantages and disadvantages and are used for various things.

The same key is utilised for both encryption and decryption in the symmetric-key encryption method known as AES. Its quick speed and minimal resource usage make it very effective and suitable for encrypting massive amounts of data. AES is considered as being very safe and has keys that are 128, 192, and 256 bits long. Key management, which may be difficult in large-scale or dispersed situations where the symmetric key must be safely exchanged between the sender and the recipient, is its main weaknesses.

While RSA uses a private key for decryption and a public key for encryption, it is an asymmetric-key encryption method. The key management process used by RSA is simpler since only the public key needs to be shared; the private key is kept confidentially by the owner. While AES is faster and better suited for encrypting huge amounts of data, RSA requires more work than AES. Digital signatures, safe authentication, and the secure exchange of symmetric keys all frequently include RSA.

- **Anomaly Detection:**

An essential component of cybersecurity is anomaly detection, which makes potential dangers and attacks easier to spot by keeping an eye on and analysing user activity, system events, and network traffic. Organisations may proactively respond to emerging risks, reduce potential harm, and improve their overall security posture by spotting unexpected trends or departures from the norm. Finding unknown or zero-day attacks requires the use of anomaly detection.

Based on variables including accuracy, false positive/negative rates, and reaction time, the Advanced Security Framework's anomaly detection system's efficacy may be evaluated. High detection accuracy is a need for an efficient system; this means that it must be able to recognise threats with little to no false positives or negatives. False positives can result in unwanted alerts and resource loss when the system misclassifies innocuous activity as harmful. False negatives, in contrast, when real threats are missed, can lead to undiscovered attacks and severe damage. Fast reaction times are another important aspect of a strong anomaly detection system that enables organisations to respond swiftly to possible threats.

The following is a representation of the Logistic Regression mathematical equation(Daniel and Martin, 2023):

Let, samples = **m**

Features = **n**

'**X'** be the input feature matrix **(m × n)**

The weigh vectors **'W' = (n ×1)**

The bias term is represented by **b** (scalar).

The probability of an instance belonging to the positive class (P(y=1|X)) can be calculated using the sigmoid function: P(y=1|X) = σ(X * W + b)

σ(z) is the sigmoid function, defined as:

σ(z) = 1 / (1 + exp(-z))

The output probability can be thresholder (e.g., at 0.5) to determine the predicted class label.

To train the Logistic Regression model, the model learns the optimal weights W and bias b by minimizing the cost function, which is typically the cross-entropy loss function. The optimization process can be performed using gradient descent or other optimization algorithms.

However, the Logistic Regression model is trained for the anomaly detection function using the '**LogisticRegression'** class from the **'sklearn.linear_model'** module, which takes care of the training process automatically and learns the ideal weights and bias for the model.

An approach for machine learning that may be used to find anomalies is logistic regression. Generalised linear models (GLMs) of this kind use input characteristics to estimate the probability of a binary outcome(Jayawardena, Epps and Ambikairajah, 2023). The binary result in the context of anomaly detection denotes whether an observation is normal or abnormal. As a machine learning approach for anomaly detection, logistic regression has a number of benefits, including interpretability, simplicity, compatibility with feature engineering, and robustness to small departures from underlying assumptions(Kalair and Connaughton, 2021). The results are simple to grasp, which is helpful for root cause analysis and repair. Organisations may be able to identify aspects that contribute to abnormalities. It is excellent for scenarios requiring rapid initial investigations or with limited resources due to its simplicity and computational efficiency. The method also has good feature engineering performance, allowing it to capture complicated correlations between variables and enhance detection performance. However, there are also some drawbacks using logistic regression. It assumes that the binary outcome's log-odds and input attributes have a linear connection, which may not be true for all datasets, especially when relationships are very non-linear(Levy *et al.*, 2020). Other methods, such as neural networks or tree-based models, may perform better in such circumstances.

- **Intrusion Prevention System (IPS):**

The Intrusion Prevention System (IPS), which actively blocks unauthorised access and shields the system from known vulnerabilities, is essential for improving cybersecurity. It functions by

constantly monitoring network traffic, spotting possible dangers, and acting quickly to block or eliminate such threats before they can cause damage. By using a proactive approach, the network's security and integrity are preserved, lowering the possibility of data breaches and system intrusions(Bijone, 2016). Accuracy, performance, interaction with a firewall API for IP blocking, email warnings for DDoS attack prevention, and usage of Random Forest Classifier algorithms for threat identification are all features of the IPS implementation in the Advanced Security Framework.

The Random Forest Classifier algorithms, recognised for their strong prediction effectiveness and ability to handle massive datasets, can be used to increase the IPS's high detection accuracy(Alsahli *et al.*, 2021). It is essential to maintain real-time network traffic analysis without introducing delay or degrading network performance, and Random Forest Classifier algorithms' parallelization abilities help achieve this goal. For an IPS to direct the firewall to immediately block malicious IP addresses, effortless communication with a firewall API for IP blocking is necessary for efficient threat response(Kao *et al.*, no date). When possible, DDoS assaults are identified, the system should also be able to notify administrators through email. This will enable them to take immediate action to preserve network availability and reduce damage. Although it could increase computational complexity, using Random Forest Classifier methods can improve threat detection skills by capturing complicated correlations between features.

- **Intrusion Detection System (IDS):**

In order to identify and analyse possible network intrusions and attacks, the Intrusion Detection System (IDS) is a crucial element for healthcare security system. It performs the role of a passive observer, continually monitoring network activity, system events, and user behaviour to spot malicious behaviour or security policy breaches. Organisations can respond swiftly, protect the integrity of their systems, and reduce possible harm thanks to the IDS's early threat detection.

The Intrusion Detection System (IDS) using Random Forest Classifier algorithms plays a crucial role in identifying and evaluating probable intrusions and assaults by utilising the special advantages of the ensemble learning approach. To reduce false positives and negatives and enable efficient incident response, high detection accuracy is accomplished by combining the strengths of many decision trees. The IDS can continue to function well while analysing complex and varied network traffic even in the presence of noise or outliers because to the resilient performance of Random Forest classifiers.(Kongunadu College of Engineering & Technology and Institute of Electrical and Electronics Engineers, no date) Random Forest is also well suited for intrusion detection jobs that entail a variety of parameters influencing the likelihood of an assault since it can handle big, high-dimensional datasets with many attributes.

When making decisions to improve security procedures or allocate resources, the algorithm's capacity to evaluate feature importance could provide valuable information about the elements that might contribute to incursions or assaults. Additionally, Random Forest classifiers are comparatively resistant to overfitting, guaranteeing that the IDS continues to be successful in identifying real-world threats on fresh, unexplored data(Kongunadu College of Engineering & Technology and Institute of Electrical and Electronics Engineers, no date).

- **Integration and Interoperability:**

  The Advanced Security Framework must be both integrated and interoperable in order for its numerous components to work together efficiently and for the framework to be successful in a variety of contexts and systems.

  AES, RSA, anomaly detection, intrusion prevention system (IPS), intrusion detection system (IDS), and other Advanced Security Framework components should all be integrated so that they may coexist peacefully. Through this connection, the framework is able to offer complete security coverage and handle threats more effectively. The IPS can take necessary action, such as blocking suspicious IP addresses or encrypting sensitive data, when the IDS detects possible intrusions, for example.

  The Random Forest Classifier is the Intrusion Detection System (IDS)'s primary algorithm when it comes to IoT devices used in the healthcare industry. In order to protect the security and integrity of the healthcare IoT devices and their data, the IDS model attempts to identify network intrusions by classifying them as either normal or attack instances. The IDS model may help to the overall security of the healthcare IoT ecosystem by recognising and reducing possible risks.

  It is crucial to implement the Advanced Security Framework in various settings and make sure that it is compatible with other technologies and systems. Healthcare organisations may use a variety of hardware, software, and infrastructure components; therefore the framework must be versatile and flexible. Organisations may employ modular design that is simple to integrate with existing systems, industry standards and best practises, open protocols, and these strategies to assure interoperability.

  The Advanced Security Framework may not operate well with organisations using older systems, requiring time-consuming and expensive upgrades or replacements. The failure of companies to integrate the framework with current technology might also be impaired by vendor lock-in when they rely on proprietary solutions. Healthcare sector may get around this by looking for solutions that support open standards and promote interoperability. Organisations should evaluate their resource capacities and give priority to implementing crucial components in order to maximise security advantages.

5.2.1: Test Environment (DATASETS)

The test environment is made to simulate the actual healthcare IoT ecosystem, down to device connectivity, data transfer, and system interaction with other platforms including electronic health records (EHR) and hospital information systems (HIS). To make sure that the security assessment does not interfere with how healthcare facilities typically operate, the test environment should be kept separate from production networks.

- **Pima Indians Diabetes Database:** Particularly in medical and health research, the Pima Indians Diabetes Database is an extensively used dataset for machine learning and data analysis. It focuses on modelling the onset of diabetes based on multiple diagnostic markers and includes data of Pima Indian women who are above the age of 21.

  This dataset has been deployed using encryption and decryption methods, and it has also been utilised in machine learning contexts that protect user privacy or secure data analysis. Before being

used for analysis or training a model, the dataset would be encrypted to protect the sensitive personal data it contains. The findings of the analysis or training may be decrypted to acquire the final result after completion, all while maintaining the data's confidentiality and privacy.

- **Cleveland Heart Disease Dataset:** A well-liked dataset for medical research, notably in the fields of cardiology and machine learning, is the Heart Disease Dataset, commonly known as the Cleveland Heart Disease Dataset. It was initially gathered at the Cleveland Clinic Foundation, and based on numerous diagnostic parameters, it is frequently used to forecast the existence of heart disease. Since it makes it easier to see patterns that are out of the ordinary and might potentially be signs of cardiac disease, this dataset is well-suited for anomaly detection techniques.

  There are 303 cases in the dataset, each having 13 input characteristics (also known as attributes) and a class label (target variable) indicating the existence of heart disease. The integer values for the goal variable range from 0 (no heart disease) to 4 (the most severe kind of heart disease). However, it will find odd patterns or outliers in the data that could point to the presence of heart disease by integrating the Heart Disease Dataset in anomaly detection approach. Techniques for detecting anomalies can be helpful for early diagnosis, enabling prompt intervention and treatment. Clustering, classification, and regression techniques as well as specialised algorithms like one-class support vector machines, isolation forests, or autoencoders are typical approaches for anomaly identification. Implementing the NSL-KDD dataset into IDS/IPS techniques in order to create a system that can accurately identify and stop network traffic intrusions. Decision trees, support vector machines, and ensemble techniques are examples of common machine learning algorithms for IDS/IPS.

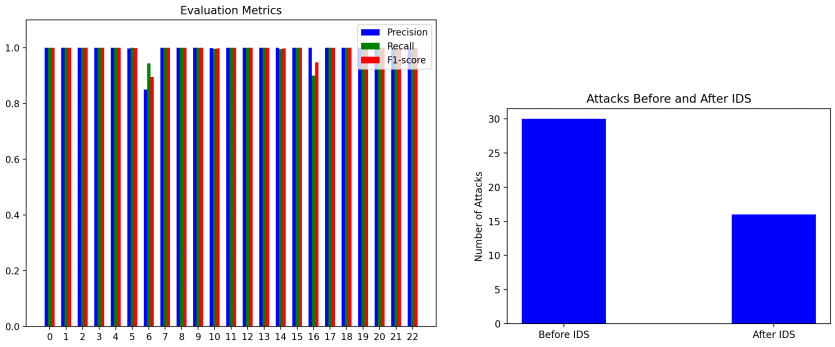
- **NSL-KDD dataset:** A popular benchmark dataset for assessing intrusion detection systems (IDS) and intrusion prevention systems (IPS) is the NSL-KDD dataset. The dataset has been improved from the original KDD Cup 1999 dataset, which was produced for the Third International Knowledge Discovery and Data Mining Tools Competition.

  The network traffic data in the NSL-KDD dataset includes both regular and attack cases. The KDDTrain+ dataset, which includes 125,973 records for training, and the KDDTest+ dataset, which contains 22,544 records for testing, are the two sections of the dataset. The dataset includes 41 input characteristics for each record as well as a class label that designates whether the traffic is legitimate or malicious.

5.2.2 Performance Indicators:

Performance indicators are quantitative measurements that are used to assess how well the advanced security architecture is working(Li *et al.*, 2019). These indicators offer insightful information on the performance of the framework and may be used to identify areas that need improvement. Performance indicators include, for example:

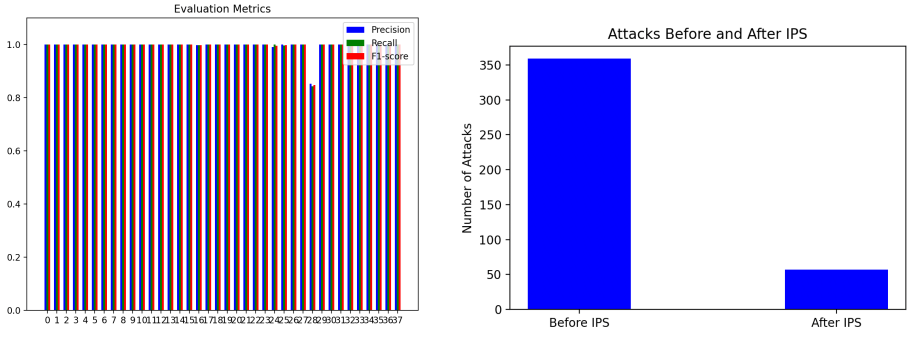
- **Performance of IDS:**



The classification report demonstrates an impressive performance of the Intrusion Detection System (IDS) across multiple classes. With an overall accuracy of 1.00, the IDS is highly effective in detecting and analyzing various types of intrusions and attacks. The macro average and weighted average for precision, recall, and f1-score also indicate a nearly perfect performance.

Looking at the individual classes, the IDS performs exceptionally well in most cases, with precision, recall, and f1-scores of 1.00. However, there are a few classes (e.g., class 6 and class 16) with slightly lower precision, recall, or f1-scores. Despite these minor discrepancies, the overall performance remains outstanding.

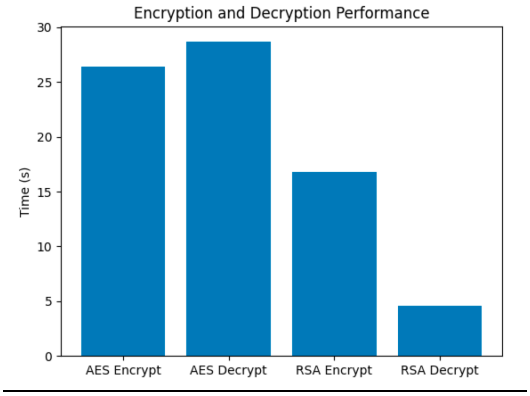
- **Performance of IPS:**



The classification report for the Intrusion Prevention System (IPS) indicates performance across multiple classes.With an overall accuracy of 1.00, the IPS is highly effective in preventing unauthorized access and protecting the system from known vulnerabilities. The macro average and weighted average for precision, recall, and f1-score are also close to perfection.Inspecting the

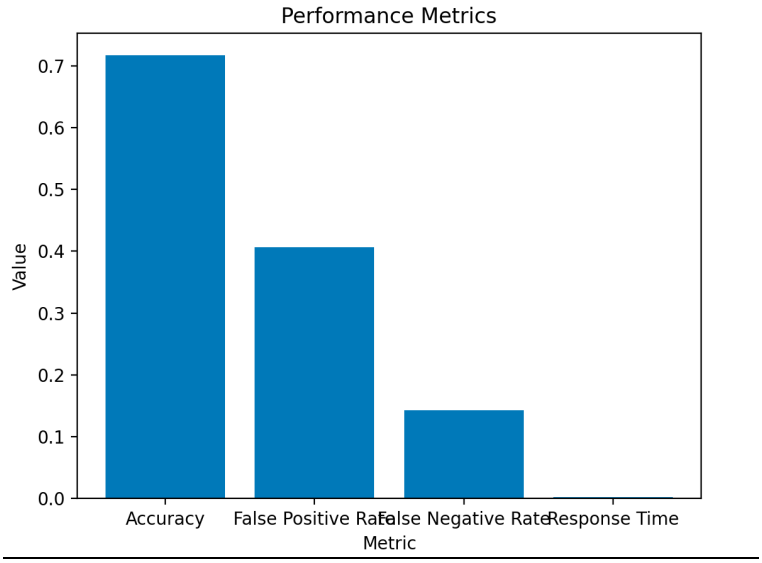
individual classes, the IPS demonstrates exceptional performance in the majority of cases, with precision, recall, and f1-scores of 1.00. Nonetheless, there are a few classes (e.g., class 24 and class 28) with slightly lower precision or f1-scores. Despite these minor discrepancies, the overall performance remains outstanding.

- **Performance of Encryption and Decryption methods:**



As you can see from the graph above, both the encryption and decryption processes for AES are quicker compared to those for RSA. This is mainly because symmetric encryption involves easier mathematical procedures than asymmetric encryption, which calls for more complicated computations. Additionally, the computational cost for RSA develops more quickly than for AES as the key size rises, exacerbating the performance disparity.

- **Performance of Anomoly Detection:**



The performance of the anomaly detection system in the Advanced Security Framework can be evaluated based on the above graph:

Accuracy: The system achieves an accuracy of 71.67%, indicating that it can correctly identify anomalies in about 71.67% of the cases. Although this is a relatively good result, there may still be room for improvement in order to minimize the number of missed anomalies or false alarms.

False Positive Rate: The false positive rate of 40.62% suggests that a significant portion of normal instances are mistakenly identified as anomalies. This may lead to unnecessary alerts and increased workload for security analysts, who must investigate these false alarms. Reducing the false positive rate should be a priority to improve the efficiency of the anomaly detection system.

False Negative Rate: With a false negative rate of 14.29%, the system misses some actual anomalies, which could potentially lead to undetected security breaches. Minimizing the false negative rate is crucial to enhance the system's ability to detect and respond to potential threats.

Response Time: The system's response time of 0.0028 seconds indicates that it can quickly analyse instances and make decisions, which is essential for real-time anomaly detection and prompt response to potential threats.

The Advanced Security Framework's anomaly detection system performs with a fair amount of accuracy and speed. The high percentages of false positive and false negative results, however, indicate that there is potential for improvement.

6. Limitations and Future Directions

Although the advanced security framework has a lot of potential to handle the security issues in healthcare IoT settings, there are several drawbacks and potential areas for future development that demand additional investigation.

Emerging technologies like blockchain, edge computing, and 5G networks are providing new options for enhancing security, privacy, and data integrity as the healthcare IoT environment continues to change(Razdan and Sharma, 2022). To further increase the advanced security framework's efficacy in securing healthcare IoT settings, future study should look at how it may be combined with these new technologies.

It is crucial to consider user-centric security and privacy problems as healthcare IoT devices grow more prevalent and incorporated into daily life(Attia, no date). The development of user-friendly user interfaces, raising user knowledge of security threats, and putting in place security measures without compromising user experience or delaying the adoption of healthcare IoT solutions should be the main areas of future study.

The creation of automated security management solutions is necessary given the complexity of healthcare IoT ecosystems and the rise in connected devices(Ge *et al.*, 2017). Future studies should investigate how automated security management tools, such automated threat intelligence collecting, vulnerability assessment, and patch management, might improve the advanced security framework. In healthcare IoT contexts, integrating these capabilities into the framework may enhance efficiency, reduce the workload on security professionals, and promote a more proactive security posture.

The intrusion detection algorithms must be continuously improved and adjusted because of the constantly changing threat approach. To maintain a high level of safety, the framework must be capable of recognising

and mitigating risks as they arise, and current threats change. Future studies should investigate cutting-edge methods and tools, such deep learning to improve the intrusion detection system's capacity to recognise and take action to address future threats.

Healthcare IoT security is significantly hampered by Advanced Persistent Threats (APTs), which entail highly experienced and resourceful adversaries that launch persistent and precise cyberattacks(Yaacoub *et al.*, 2020). To successfully identify and stop APTs, the advanced security architecture has to be improved. Future study should look into methods for enhancing the framework's capacity to recognise and respond to complex and covert attacks, such as those utilising supply chain attacks, insider threats, and zero-day vulnerabilities.

Further thorough testing is necessary to determine the framework's performance and scalability in large-scale IoT implementations. When implementing the framework across many linked devices, resource limitations such the restricted processing and memory in IoT devices may provide problems(Zikria *et al.*, 2018). Also, it could be challenging to adopt consistent security measures due to the variety of devices and their diverse capabilities. To enable smooth deployment and scalability, future research should concentrate on refining the framework to support resource-constrained situations and a wide range of devices.

Finally, the advanced security framework may further enhance its efficiency in defending healthcare IoT settings by tackling these new study areas, ensuring the safety, privacy, and integrity of sensitive medical data while encouraging the responsible use of IoT technology in healthcare.

7. Conclusion:

A notable improvement in resolving the complex security issues found in healthcare IoT ecosystems is the advanced security architecture for IoT devices. The framework provides a thorough and adaptable solution that includes authentication, encryption, intrusion detection, access control, and security policy enforcement due to its flexible, multi-layered design. The framework efficiently secures sensitive medical data and ensures patient privacy and regulatory compliance by including cutting-edge encryption algorithms, machine learning-based intrusion detection systems, and privacy-preserving strategies.

The evaluation and comparative study of the advanced security framework showed that it outperformed existing security solutions in terms of performance, security, and flexibility. Its adoption by healthcare organizations is made more simpler by its compliance to well recognized security standards and protocols, which also encourage interoperability within the healthcare IoT environment. Although the results are encouraging, there is still progressed to be made, including improving intrusion detection methods, scalability, and performance in installations.

Future research should be focused on addressing these problems and exploring having to cut methods to improve the efficiency of the advanced security framework in protecting healthcare IoT ecosystems. By doing this, the framework will continue to develop and adapt to the changing needs of healthcare IoT ecosystems, ultimately enhancing the resilience of these infrastructures.

Healthcare IoT ecosystems can completely change way security is controlled because to the advanced security framework for IoT devices. The development and implementation of good security frameworks, like this one, will be important to ensuring the safety, privacy, and integrity of sensitive medical data and encouraging the responsible use of IoT technologies in healthcare as the usage of IoT devices increases.

8. Bibliography

Abdul-Ghani, H.A. and Konstantas, D. (2019) 'A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective', *Journal of Sensor and Actuator Networks*. MDPI AG. Available at: https://doi.org/10.3390/jsan8020022.

Ahmadi, H. *et al.* (2019) 'The application of internet of things in healthcare: a systematic literature review and classification', *Universal Access in the Information Society*. Springer Verlag, pp. 837–869. Available at: https://doi.org/10.1007/s10209-018-0618-4.

Akkaş, M.A., SOKULLU, R. and Ertürk Çetin, H. (2020) 'Healthcare and patient monitoring using IoT', *Internet of Things (Netherlands)*, 11. Available at: https://doi.org/10.1016/j.iot.2020.100173.

Alabdullah, B., Beloff, N. and White, M. (2021) 'E-art: A new encryption algorithm based on the reflection of binary search tree', *Cryptography*, 5(1), pp. 1–15. Available at: https://doi.org/10.3390/cryptography5010004.

Aldeer, M. *et al.* (2021) 'Unobtrusive patient identification using smart pill-bottle systems', *Internet of Things (Netherlands)*, 14. Available at: https://doi.org/10.1016/j.iot.2021.100389.

Aleisa, M.A., Abuhussein, A. and Sheldon, F.T. (2020) 'Access Control in Fog Computing: Challenges and Research Agenda', *IEEE Access*, 8, pp. 83986–83999. Available at: https://doi.org/10.1109/ACCESS.2020.2992460.

Alsahli, M.S. *et al.* (2021) 'Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN', *International Journal of Advanced Computer Science and Applications*, 12(5), pp. 617–626. Available at: https://doi.org/10.14569/IJACSA.2021.0120574.

ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) EVASION AND DETECTION METHODS (2016).

Assiri, A. and Almagwashi, H. (2018) 'IoT Security and Privacy Issues', in *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/CAIS.2018.8442002.

Attia, T.M. (no date) *Attia, Tarek M. Standard-Nutzungsbedingungen: Challenges and Opportunities in the Future Applications of IoT Technology*. Available at: http://hdl.handle.net/10419/201752.

Azzawi, M.A. *et al.* (2016a) *A Review on Internet of Things (IoT) in Healthcare Location Based Authentication System View project Remote Consultation of Envenomation Case with Mobile Application View project*, *Article in International Journal of Applied Engineering Research*. Available at: https://www.researchgate.net/publication/309718253.

Azzawi, M.A. *et al.* (2016b) *A Review on Internet of Things (IoT) in Healthcare Location Based Authentication System View project Remote Consultation of Envenomation Case with Mobile Application View project*, *Article in International Journal of Applied Engineering Research*. Available at: https://www.researchgate.net/publication/309718253.

Bansal, M., Gupta, S. and Mathur, S. (2021) 'Comparison of ECC and RSA Algorithm with DNA Encoding for IoT Security', in *Proceedings of the 6th International Conference on Inventive Computation*

Technologies, ICICT 2021. Institute of Electrical and Electronics Engineers Inc., pp. 1340–1343. Available at: https://doi.org/10.1109/ICICT50816.2021.9358591.

Bharathi, P. *et al.* (2021) 'Secure File Storage using Hybrid Cryptography', in *Proceedings of the 6th International Conference on Communication and Electronics Systems, ICCES 2021*. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/ICCES51350.2021.9489026.

Bijone, M. (2016) 'A Survey on Secure Network: Intrusion Detection & Prevention Approaches', *American Journal of Information Systems*, 4(3), pp. 69–88. Available at: https://doi.org/10.12691/ajis-4-3-2.

Bokefode, J.D. *et al.* (2016) 'Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption', in *Procedia Computer Science*. Elsevier B.V., pp. 43–50. Available at: https://doi.org/10.1016/j.procs.2016.06.007.

Breivold, H.P. and Sandstrom, K. (2015) 'Internet of Things for Industrial Automation -- Challenges and Technical Solutions', in *2015 IEEE International Conference on Data Science and Data Intensive Systems*. IEEE, pp. 532–539. Available at: https://doi.org/10.1109/DSDIS.2015.11.

Butt, S.A. *et al.* (2019) 'IoT Smart Health Security Threats', in *Proceedings - 2019 19th International Conference on Computational Science and Its Applications, ICCSA 2019*. Institute of Electrical and Electronics Engineers Inc., pp. 26–31. Available at: https://doi.org/10.1109/ICCSA.2019.000-8.

Carletti, M., Terzi, M. and Susto, G.A. (2020) 'Interpretable Anomaly Detection with DIFFI: Depth-based Isolation Forest Feature Importance'. Available at: http://arxiv.org/abs/2007.11117.

Castiglione, A. *et al.* (2021) 'The Role of Internet of Things to Control the Outbreak of COVID-19 Pandemic', *IEEE Internet of Things Journal*, 8(21), pp. 16072–16082. Available at: https://doi.org/10.1109/JIOT.2021.3070306.

Choi, H. and Seo, S.C. (2021) 'Optimization of PBKDF2 Using HMAC-SHA2 and HMAC-LSH Families in CPU Environment', *IEEE Access*, 9, pp. 40165–40177. Available at: https://doi.org/10.1109/ACCESS.2021.3065082.

Choubisa, M. *et al.* (2022) 'A Simple and Robust Approach of Random Forest for Intrusion Detection System in Cyber Security', in *2022 International Conference on IoT and Blockchain Technology, ICIBT 2022*. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/ICIBT52874.2022.9807766.

Daniel, J. and Martin, J.H. (2023) *Speech and Language Processing*.

Ding, X. *et al.* (2021) 'Wearable Sensing and Telehealth Technology with Potential Applications in the Coronavirus Pandemic', *IEEE Reviews in Biomedical Engineering*, 14, pp. 48–70. Available at: https://doi.org/10.1109/RBME.2020.2992838.

Disha, R.A. and Waheed, S. (2022) 'Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique', *Cybersecurity*, 5(1). Available at: https://doi.org/10.1186/s42400-021-00103-8.

Ge, M. *et al.* (2017) 'A framework for automating security analysis of the internet of things', *Journal of Network and Computer Applications*, 83, pp. 12–27. Available at: https://doi.org/10.1016/j.jnca.2017.01.033.

Guia, M., Silva, R.R. and Bernardino, J. (2019) 'Comparison of Naive Bayes, support vector machine, decision trees and random forest on sentiment analysis', in *IC3K 2019 - Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. SciTePress, pp. 525–531. Available at: https://doi.org/10.5220/0008364105250531.

Hady, A.A. *et al.* (2020) 'Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study', *IEEE Access*, 8, pp. 106576–106584. Available at: https://doi.org/10.1109/ACCESS.2020.3000421.

Hamza, A. and Kumar, B. (2020) 'A Review Paper on DES, AES, RSA Encryption Standards', in *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*. Institute of Electrical and Electronics Engineers Inc., pp. 333–338. Available at: https://doi.org/10.1109/SMART50582.2020.9336800.

Hasan, M. *et al.* (2019) 'Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches'. Available at: https://doi.org/10.1016/j.iot.2019.10.

Hussain, I. *et al.* (2022) 'Health Monitoring System Using Internet of Things (IoT) Sensing for Elderly People', in *14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics, MACS 2022*. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/MACS56771.2022.10023026.

'ITRC_2022-Data-Breach-Report_Final-1' (no date).

Jayawardena, S., Epps, J. and Ambikairajah, E. (2023) 'Ordinal Logistic Regression With Partial Proportional Odds for Depression Prediction', *IEEE Transactions on Affective Computing*, 14(1), pp. 563–577. Available at: https://doi.org/10.1109/TAFFC.2020.3031300.

Kalair, K. and Connaughton, C. (2021) 'Anomaly detection and classification in traffic flow data from fluctuations in the flow–density relationship', *Transportation Research Part C: Emerging Technologies*, 127. Available at: https://doi.org/10.1016/j.trc.2021.103178.

Kandasamy, K. *et al.* (2020) 'IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process', *Eurasip Journal on Information Security*, 2020(1). Available at: https://doi.org/10.1186/s13635-020-00111-0.

Kao, Y.-C. *et al.* (no date) *Automatic Blocking Mechanism for Information Security with SDN*.

Karunarathne, S.M., Saxena, N. and Khan, M.K. (2021) 'Security and Privacy in IoT Smart Healthcare', *IEEE Internet Computing*, 25(4), pp. 37–48. Available at: https://doi.org/10.1109/MIC.2021.3051675.

Kongunadu College of Engineering & Technology and Institute of Electrical and Electronics Engineers (no date) *Proceedings, International Conference on Smart Electronics and Communication (ICOSEC 2020) : 10-12, September 2020*.

Lee, I. (2020) 'Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management', *Future Internet*. MDPI AG. Available at: https://doi.org/10.3390/FI12090157.

Levy, J.J. *et al.* (2020) 'Don't dismiss logistic regression: The case for sensible extraction of interactions in the era of machine learning', *BMC Medical Research Methodology*, 20(1). Available at: https://doi.org/10.1186/s12874-020-01046-3.

Li, F. *et al.* (2019) 'Enhanced cyber-physical security in internet of things through energy auditing', *IEEE Internet of Things Journal*, 6(3), pp. 5224–5231. Available at: https://doi.org/10.1109/JIOT.2019.2899492.

Lin, X.X., Lin, P. and Yeh, E.H. (2021) 'Anomaly Detection/Prediction for the Internet of Things: State of the Art and the Future', *IEEE Network*, 35(1), pp. 212–218. Available at: https://doi.org/10.1109/MNET.001.1800552.

Magdum, N. (2023) 'Hybrid Encryption using Symmetric Block and Stream Cipher', *International Journal of Engineering and Management Research*, 13(1), pp. 35–39. Available at: https://doi.org/10.31033/ijemr.13.1.4.

Menezes, A. and Stebila, D. (2021) 'The Advanced Encryption Standard: 20 Years Later', *IEEE Security and Privacy*, 19(6), pp. 98–102. Available at: https://doi.org/10.1109/MSEC.2021.3107078.

Moustafa, H. *et al.* (2016) 'Remote monitoring and medical devices control in eHealth', in *International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE Computer Society. Available at: https://doi.org/10.1109/WiMOB.2016.7763177.

Nasiri, S. *et al.* (2019) 'Security requirements of internet of things-based healthcare system: A survey study', *Acta Informatica Medica*, 27(4), pp. 253–258. Available at: https://doi.org/10.5455/aim.2019.27.253-258.

Patgiri, R. and Singh, L.D. (2022) 'An Analysis on the Variants of the RSA Cryptography', in *International Conference on Information Networking*. IEEE Computer Society, pp. 40–45. Available at: https://doi.org/10.1109/ICOIN53446.2022.9687262.

Pathirage, T.D. *et al.* (2021) 'Multi-Prime RSA Verilog Implementation Using 4-Primes', in *2021 10th International Conference on Information and Automation for Sustainability, ICIAfS 2021*. Institute of Electrical and Electronics Engineers Inc., pp. 60–65. Available at: https://doi.org/10.1109/ICIAfS52090.2021.9605975.

Pradhan, B., Bhattacharyya, S. and Pal, K. (2021a) 'IoT-Based Applications in Healthcare Devices', *Journal of Healthcare Engineering*. Hindawi Limited. Available at: https://doi.org/10.1155/2021/6632599.

Pradhan, B., Bhattacharyya, S. and Pal, K. (2021b) 'IoT-Based Applications in Healthcare Devices', *Journal of Healthcare Engineering*. Hindawi Limited. Available at: https://doi.org/10.1155/2021/6632599.

Prantl, T. *et al.* (2021) 'Performance Impact Analysis of Securing MQTT Using TLS'. Available at: https://doi.org/10.1145/3427921.

Razdan, S. and Sharma, S. (2022) 'Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies', *IETE Technical Review (Institution of Electronics and Telecommunication Engineers,*

India). Taylor and Francis Ltd., pp. 775–788. Available at: https://doi.org/10.1080/02564602.2021.1927863.

Saranya, T. *et al.* (2020) 'Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review', in *Procedia Computer Science*. Elsevier B.V., pp. 1251–1260. Available at: https://doi.org/10.1016/j.procs.2020.04.133.

Security of Cyber-Physical Systems (2020) *Security of Cyber-Physical Systems*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-45541-5.

Serror, M. *et al.* (2021) 'Challenges and Opportunities in Securing the Industrial Internet of Things', *IEEE Transactions on Industrial Informatics*, 17(5), pp. 2985–2996. Available at: https://doi.org/10.1109/TII.2020.3023507.

Tukade, T.M. and Banakar, R.M. (2018) *Data Transfer Protocols in IoT-An Overview*. Available at: http://www.ijpam.eu.

Vegh, L. (2018) 'Cyber-physical systems security through multi-factor authentication and data analytics', in *Proceedings of the IEEE International Conference on Industrial Technology*. Institute of Electrical and Electronics Engineers Inc., pp. 1369–1374. Available at: https://doi.org/10.1109/ICIT.2018.8352379.

White, G., Nallur, V. and Clarke, S. (2017) 'Quality of service approaches in IoT: A systematic mapping', *Journal of Systems and Software*, 132, pp. 186–203. Available at: https://doi.org/10.1016/j.jss.2017.05.125.

Xiao, L. *et al.* (2018) 'IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?', *IEEE Signal Processing Magazine*, 35(5), pp. 41–49. Available at: https://doi.org/10.1109/MSP.2018.2825478.

Yaacoub, J.P.A. *et al.* (2020) 'Cyber-physical systems security: Limitations, issues and future trends', *Microprocessors and Microsystems*, 77. Available at: https://doi.org/10.1016/j.micpro.2020.103201.

Yahaya, Musa.M. and Ajibola, A. (2019) 'Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 317–322. Available at: https://doi.org/10.32628/cseit195659.

Yu, L., Lu, Y. and Zhu, X.J. (2012) 'Smart hospital based on internet of things', *Journal of Networks*, 7(10), pp. 1654–1661. Available at: https://doi.org/10.4304/jnw.7.10.1654-1661.

Zheng, G. *et al.* (2019) 'A Critical Analysis of ECG-Based Key Distribution for Securing Wearable and Implantable Medical Devices', *IEEE Sensors Journal*, 19(3), pp. 1186–1198. Available at: https://doi.org/10.1109/JSEN.2018.2879929.

Zikria, Y. Bin *et al.* (2018) 'Internet of Things (IoT): Operating System, Applications and Protocols Design, and Validation Techniques', *Future Generation Computer Systems*. Elsevier B.V., pp. 699–706. Available at: https://doi.org/10.1016/j.future.2018.07.058.