© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214

Development of a Cloud Based Security Risk Assessment Framework for IoT-Based Health Care System: A Review

TAYAPITI E.[1], SARJIYUS O.[2], NATHAN N.[3]
[1,2,3]*Computer Science Department, Adamawa State University, Mubi*

Abstract- ***The use of Internet of Things (IoT) technology in healthcare has changed how medical services are provided. IoT devices like wearable sensors, implantable tools, and smart diagnostic machines allow doctors to watch patients' health as it happens and help make better decisions about their care. These devices help doctors talk to patients from a distance and give them tailored care, which makes healthcare faster and better for patients. Even though there are many advantages, the way IoT devices are connected creates big security problems because the medical data being sent over networks is very sensitive. Healthcare organizations have to deal with two main problems: keeping patient information safe and making sure that healthcare services keep running without any interruptions. The growing number of IoT devices, which have different amounts of computing power and security features, has made traditional security methods not enough anymore. Many devices don't have enough power to use strong encryption or detect threats as they happen, which makes them easier targets for attacks like man-in-the-middle, malware insertion, and unwanted access. Even though more people are aware of these problems, healthcare organizations still have a hard time finding a complete and flexible security risk assessment system that covers both IoT devices and cloud-based systems. Current solutions are usually broken, slow to act, or only cover certain kinds of threats. They don't look at all the weaknesses, dangers, and possible problems in a complete way. The design science approach works well because the research is about making a tool (a security risk assessment framework) to deal with a real-world issue. The method will go through these steps: first, identifying and looking at the security issues in IoT healthcare systems, then figuring out what the security framework needs, next creating a cloud-based system to assess risks, followed by building and putting the framework into use, and finally testing and checking how well the framework works. This way, the framework is made to properly handle the security problems in IoT healthcare settings.***

Keywords: Cyber Security Threats, Data Protection, HealthCare System, Internet of Things (IoT) Device and e Security Risk Assessment Framework.

I. INTRODUCTION

The use of Internet of Things (IoT) technology in healthcare has changed how medical services are provided. IoT devices like wearable sensors, implanted devices, and smart diagnostic tools help track patients' health in real time and make healthcare decisions better. These devices allow doctors to consult with patients from a distance and offer tailored care, which makes healthcare more efficient and improves patient results. Even though there are many good things about IoT devices, their ability to connect with each other creates big security problems. This is because the medical information being sent over networks is very private and important (Zhang et al., 2023).

Healthcare IoT systems include many different types of devices that have different abilities to process information, and a lot of them don't have strong security features. Using weak ways to check who is allowed to access and not keeping communications safe can make these systems vulnerable to problems like hackers getting in, people listening in on conversations, and others getting unwanted access. Because healthcare information is very private and protected by laws, losing access to it can cause serious problems. This makes it very important to keep IoT devices secure (Alrawashdeh et al., 2023).

Cloud computing has become an important foundation for healthcare IoT systems, providing flexible storage, strong processing ability, and a single place to manage data. Cloud services help with real-time data analysis, allow access from anywhere, and support team-based healthcare solutions. However, using the cloud also brings more risks, like problems with shared environments and the chance of someone gaining unwanted access, which need to be handled along with keeping IoT devices safe

(ISO/IEC, 2020). Traditional risk management approaches don't work well for cloud-connected IoT healthcare systems because they handle risks from IoT devices and the cloud separately. A good security risk assessment needs a system that looks at everything from the IoT devices at the edge to the cloud where data is stored and analyzed. Without a unified strategy, healthcare groups are still at risk from both existing and new dangers (Alqahtani et al., 2020).

New research has introduced security plans and risk tools designed specifically for cloud-based IoT systems used in healthcare. These frameworks focus on identifying threats, regularly checking for risks, and working with established cyber security guidelines. Even so, there is still a need for a complete and flexible system that can handle the risks from IoT devices and cloud systems, making sure patient information stays private and the system works reliably (Sultan et al., 2021).

It is very important to create a cloud-based framework for assessing security risks in IoT healthcare systems. This framework can spot weaknesses in devices and the cloud, measure how risky they are, and help create plans to fix them. By combining cloud security measures with IoT threat modeling, the framework helps healthcare providers stay compliant, keep patient data safe, and keep their services running smoothly (Bokhari et al., 2022). In short, combining IoT with cloud computing in healthcare offers big benefits but also brings important security issues. A strong, complete system for checking security risks helps healthcare groups deal with cyber dangers before they happen, keep patient data safe, and use new technology in a secure way to make healthcare better (ScienceIJSAR, 2022). This study is about creating a cloud-based framework to assess security risks in an IoT-based healthcare system, to help protect patient information safely.

This study looks at previous events that show how weaknesses in medical IoT devices can be used to harm patients, change how the devices work, or take sensitive information. These attacks show how important it is to manage security risks actively in healthcare systems that use the Internet of Things, as mentioned in Rashid et al.'s 2023 study. The possible dangers go beyond just privacy issues; they can actually harm patients' health if the devices stop working or get altered. The fast increase in the number of IoT devices is making it harder for old security methods to keep up. Standard security measures like encryption or ongoing user verification are usually not possible for IoT devices that have limited resources. Interoperability problems and the absence of common standards make risk management harder, creating weaknesses that hackers can take advantage of (Mekky et al., 2023). Find and group the risks related to patient data, look at the security dangers and weaknesses in healthcare IoT devices, check how likely these threats and weaknesses are to happen and how much damage they could cause, review the current security steps and strategies being used to keep the IoT healthcare system safe, and create a full plan that gives a clear and practical way to find, examine, and handle risks, making sure the system stays secure, accurate, and available. This study is about creating a cloud-based framework to assess security risks in an IoT-based healthcare system. Healthcare organizations deal with a big problem: they need to protect very sensitive patient information while also making sure that healthcare services are always available and working properly. The growing number of IoT devices, which have different amounts of computing power and security protections, has made traditional security methods not enough anymore. Many devices don't have enough power to use strong encryption or detect threats as they happen, which makes them easy targets for attacks like man-in-the-middle, malware being added, and unwanted access. Also, because IoT networks are connected, a threat at one device can spread through the system, possibly impacting many devices and harming patient results (Mekky et al., 2023).

Adding cloud computing to IoT-based healthcare systems helps manage data better and makes the system more flexible, but it also brings more challenges when it comes to handling risks. Cloud platforms hold and manage huge amounts of private patient information, which makes them a big target for hackers. Security breaches in cloud environments can lead to the wide spread sharing of sensitive

patient data, cause service interruptions, and result in breaking compliance rules. Traditional risk assessment methods usually look at IoT devices or cloud systems separately, but they don't consider the bigger risks that come from how these systems are connected to each other (ISO/IEC, 2020).

Alqahtani et al., (2020) Mention in his work that even though more people are becoming aware of these problems, healthcare companies still have a hard time finding a complete and flexible way to check security risks that covers both internet-connected devices and cloud systems. Right now, many existing solutions are broken up, only deal with problems after they happen, or don't cover everything. They usually look at just one kind of threat instead of checking all possible weaknesses, dangers, and how bad things could get. Because of this, healthcare workers face ongoing cyber-attacks that can damage the accuracy of information, put private data at risk, and harm patients.

Sultan et al., (2021) Moreover, there are no standard steps in place for spotting, measuring, and handling security risks in healthcare systems that use cloud-connected IoT devices, which makes it harder to manage risks before they become serious problems. Without a clear structure in place, companies depend a lot on temporary security steps, which can be uneven, missing parts, or no longer useful. This gap shows how important it is to have a cloud-based security risk assessment framework specifically for healthcare IoT systems. Such a framework would help in clearly identifying threats, properly evaluating risks, and making solid plans to reduce them.

Bokhari et al., (2022) State that besides problems with technology, following rules and regulations also makes things more complicated. Healthcare companies need to follow strict rules about protecting and keeping patient information private, like HIPAA, GDPR, and other national laws that govern how health data is gathered, kept safe, and shared. Not having a clear system to assess risks makes it more likely that rules are broken, which can lead to fines, harm to the organization's reputation, and loss of trust from patients.

II. REVIEW OF RELATED LITERATURE

The last chapter talked about the main subject of this thesis. This chapter will discuss the topic in detail and highlight the key ideas that are important for protecting IoT environments. In this literature review, I look at what experts currently say about the key ideas, and I explain them in a general way.

Almahdi (2019), proposed stated that patients who are treated indoors and outdoors are responsible for keeping their data safe by being more aware of cyber-attacks and how to protect themselves from them. Meanwhile, the people who work at the facility and the companies that provide services are responsible for making sure better hardware is used to protect patient information both inside and outside the building. Since IoT is still in the early stages of development, it doesn't have strong security standards yet.

Shah et al., (2019) made a statement that the information shared between the patient's real-time health monitoring systems would be protected to ensure it is genuine, accurate, and kept private. Right now, the safety issues in telemedicine and real-time health monitoring systems need academics to work together to solve the security problems.

IoT combines various technologies, and data is shared between devices through different communication methods. Each communication level requires different security activities. Many scientists have suggested using biometric safety measures because they use people's unique behaviors to create security solutions that can work for a large number of users. Biometric systems are gaining a lot of popularity among people because they are used to confirm someone's identity and verify who they really are. However, these systems are facing several challenges, including high costs, difficulty in working in real time, needing regular hardware upkeep, and threats like cyber-attacks such as Denial of Service (Rahmani et al., 2015), eavesdropping, and tampering with data. Certain types of attacks, like man-in-the-middle attacks, spoofing, and brute force attacks, happen on the perception layer of biometric systems. This is the part where people enter their

biometric data into the system. These attacks cause issues within the system that make it harder to make decisions.

A framework was created to handle important problems in the layered structure of an IoT-based health system, which gathers all patient data and sends it to the cloud, making it available both locally and worldwide (Nanayakkara et al., 2019). The model was tested with the Contiki real-time operating system. The model had three layers, and each layer was meant to do a certain job; but the system didn't have the security setup needed to handle the existing administrative tasks.

The Mobicare plan was suggested for use in mobile healthcare apps. This system allows patients to access a nursing and tracking system that provides up-to-date and accurate information about their health condition. The system allows healthcare workers to review the patient's health details when the patient is not there, as found in Mohammed et al., 2019. Technological changes happen all the time, so Mobicare faces some tough research challenges.These include keeping body sensor networks safe, making sure sensor code updates are reliable and secure, and exploring possible new opportunities. Some solutions provide important examples for use in e-health applications. This study has offered a solid approach for merging secret sharing methods and linking identities to create groups of patients with the same illness (Sun, 2019).
The groups are split into different blocks, and the block department assists the block director in gathering detailed information from patients' mobile devices. Even though the system doesn't stop bad people from entering, those people aren't actually harming the patients.Instead, the system helps patients in difficult situations by sharing some private info about their safety (Selvaraj, 2019).

Wireless body area networks (WBANs) systems now use technologies that help overcome challenges like power limits, processing speed, scalability issues, management difficulties, and computing constraints by incorporating cloud computing technology. Combining WBANs with cloud computing as a sensor cloud infrastructure helps in healthcare by allowing real-time tracking of patients and early detection of diseases (Masood et al., 2018). However, this does not include standard architecture, policy compliance, usual data collection, patient behavior management, medically coded passwords, data sharing, data disclosure, data management, and various ways to organize data (Masood et al., 2018). Similarly, the SC-I should focus closely on friendly applications, network security, real-time implementation, access control, and improved access to higher-quality patient data (Choi et al., 2018).

Reliable data communication is very important in IoT because it helps with combining data, finding useful information, offering services that know the user's situation, and keeping user information safe (Yan et al., 2014). One way to handle these issues is to imagine a virtual version of the IoT setup in the cloud, called the Cloud-of-Things (CoT).In this setup, each device can be linked to one or more cloud agents, as mentioned by Fortino in 2018.These agents use a method called CoTAG, which groups them together based on how reliable and trustworthy they are. They perform the tests in a made-up situation to see how reliable and effective the algorithm is. The results suggest that agreeing to a plan might have some positive effects.

An IoT framework and a two-dimensional IoT structure were created to ensure complete security throughout the entire system and to fix the issue of HTTP-CoAP proxies being limited. They proposed a new HTTP-CoAP security model. The simplest method was to encrypt the HTTP payload to ensure secure communication from end to end, while still supporting both HTTP and CoAP protocols (Li et al., 2011).

The Reliable IoT-based Security System Architecture is the first scholarly summary-based proposal. In summary, this study focuses on making a trusted security system for IoT work in real life. It includes parts like secure device modules, reliable sensing parts, secure user devices, dependable network parts, and advisor modules.

It's also important to look into ways to fix security issues in IoT because of how easy it is to access IoT

devices and the fact that IoT growth isn't complete yet (Yang, 2017).

A survey was done to look at IoT safety from three angles: the three-layer network structure, the security problems in each layer, and the ways to protect against those issues. Another survey was done to uncover some IoT security problems through a part of the network setup and to find answers to the issues mentioned earlier and important technologies. Safety measures include things like the ones mentioned in the climate layer. These are important parts like management and algorithm, security routing protocol, data fusion software, authentication, and access control (Yasin et al., 2018; Mohapatra et al., 2018).

Choi et al., (2018) stated in his study that, a study was done to make sensor-based attacks and security methods in mHealth better so that patient data stays private. A detailed classification system was used to reach the goal. About 3064 papers were gathered and then sorted into different groups. These groups included surveys about telemedicine, three common types of telemedicine systems, methods using smartphone sensors for user verification, and other related articles. They looked at the second layer of smartphone sensors to improve security in mobile health apps.

Continuous tracking of a patient's health information, updating their status, and keeping their records current requires an advanced system. A secure cloud server lets approved users view patient details instantly and talk to doctors who are not nearby. Different rules for managing policies are used to improve data privacy and security, as mentioned in Hamrioui's 2017 work.

Using IoT, multimedia helps patients and experts communicate more effectively and clearly, even from a distance. This enables remote care and brings many new ideas and improvements to the healthcare field. A study by Logambal in 2017 said that a wireless body area network (WBAN) system with three levels can help monitor health care continuously and in real time.

To make sure that private data is only used to help official services by approved providers, some solutions have been suggested. These solutions usually depend on a system known as a privacy broker. The proxy works with the user on one side and with the services on the other.

A solution was found that works well between security and practicality; using a DTH-P2P social network and a cryptographic protocol, the system met security needs without the complex parts of today's e-voting systems (Buccafurri, 2012).

Suppose a Wireless Sensor Network (WSN) is to be completely integrated into the.

IoT. In that case, there are several security issues to think about, like making sure there's a safe way for an internet-connected device to talk to a sensor node. To set up this network, it's important to have systems in place that let two devices far apart agree on special security details, like secret keys, to keep the information safe as it moves (Huang, 2017). The VICINITY framework can offer full semantic interoperability to various IoT platforms and vendors. It is designed to fix privacy and security issues and provides a strong answer to problems with IoT devices. A system with a decentralized setup made up of nodes is used to protect peer-to-peer communication by applying legal principles, as mentioned in Farooq et al., 2018.

Trust is the most important part of intelligent agent technology because it helps improve the reputation of smart objects within the community. A study suggests a secure way and a system setup for different areas of IoT in e-health that helps send and receive patient data safely, which can reduce security issues and make the most of wearable devices. This current research shows how many patients' data can be handled through IoT e-health applications (Hathaliya & Tanwar, 2020).

DTLS, which is based on certificates, uses a handshake process to ensure secure communication between users and IoT-based e-health gateways. This is necessary because the devices involved have

limited resources and cannot easily handle complex cryptographic methods (Hatzivasilis, 2019).

RSA keys, DTLS, and Clasp authentication methods are used to verify and set up this system (Ali, 2020). This offers an algorithm that uses public-key cryptography along with TSA features and modules, so the security relies on these features. After switching DTLS with this new protocol, it was found that the small difference noticed on the hardware platform is fully acceptable for IoT. This protocol ensures the SMS works properly from start to finish, uses the least amount of power, keeps your information private, and confirms who is sending the message. In the end, it was found that IoT is the right choice for using DTLS, as stated by Tewari in 2016.

The works mentioned earlier have made significant contributions to securing real-time health monitoring systems by ensuring data remains private, genuine, and accurate. Different research studies are looking into how safe real-time data is. As technology keeps getting better, more hackers are targeting it, and the number of cyber threats is rising every day (Draz, 2018). The services provided by IoT-based monitoring systems are different from the services we use on the public network, as noted by Al-Qaseemi et al., 2018.

2.1 Cyber security in the development of a cloud-based security risk assessment framework for an IoT-based healthcare system.

Cyber security does not have a single, widely accepted definition (Rossouw, 2013). To make it clear, the subject can be described as “the practice of protecting important systems and private information from online threats” (IBM, 2022). Cyber security became relevant back in the 1970s. In 1977, the US government noticed the first instances of security problems in computer systems that anyone could access (Janine, 2018). Since the 1970s, bad people have come up with many different ways to take advantage of the environment. Malicious users are people who deliberately enter a system to damage it or use it in ways that aren't allowed. Because of this, the security of computer systems had to improve a lot. Until 2013, protecting computer systems was mostly about responding after bad actors attacked. This means that the environments acted in response once an attack happened (Eric, 2013). In recent years, more active cybersecurity programs have become common (AmandaNCraig, 2015). These programs require sharing of intelligence and encourage the use of active methods to detect threats. This method offers a chance for wide and shared cooperation in protecting against cyber threats. This had a good effect on making computer systems safer. This began the present trend of actively checking for security risks within the organization and taking steps to prevent them.

Not only bad people can take advantage of the environment's security, but there's also another serious danger that's really hard to deal with, and that's everyday users. These users can enter the environment and have the proper login details to make changes. Because of this, bad people might try to get them to do something. Besides people who intentionally do bad things, other users can also be a big danger. Even if the environment is safe from harmful users, harmful users can still start attacking it by using the help of other users who have the right permissions.

This can be explained by the "weakest link" idea. The security of a system depends on its weakest point. Because bad actors just need one way in to take advantage of the system. In many situations, the people who use the environment are often the most vulnerable part (Jalkanen, 2019).

The area where cyber security experts work is changing very quickly. This happens because digital technologies are changing quickly (Borka, 2022). New technologies are being used, and attackers are creating new ways to take advantage of them. As time goes on, it's important to handle possible risks and lower the chance of them occurring. Here is the rephrased content in a simple and natural tone:

All of these attacks are impacting the CIA triad in some way. The CIA triad is a common standard used to check how well information system security is working. This benchmark is built on three main goals of every security program: keeping information secret, making sure it stays accurate, and ensuring it's accessible when needed (Kim, 2018). Confidentiality

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214

keeps certain information from being seen by people who aren't allowed to know, integrity makes sure information isn't changed in a wrong way, and availability ensures that information is always there when you need it. As mentioned before, all of the 15

Top 15 cyber threats as listed by ENISA in the report from Ifigeneia in 2021.

The attacks shown in figure 2.1 take advantage of the environment's weakness in keeping information secret, ensuring it stays correct, or making sure it is always accessible. With the help of these tricks, the bad people can gain benefits in different ways. The effects of these attacks can be different depending on the environment, the user, and the device being used.

These consequences can range from small, annoying viruses on a personal computer to issues that threaten national security. In figure 2.2, there is a common example of the CIA benchmark shown. All three borders of the benchmark are equally important and necessary to keep the information inside the triangle safe.

CIA triad of data security (Deepak, 2018).

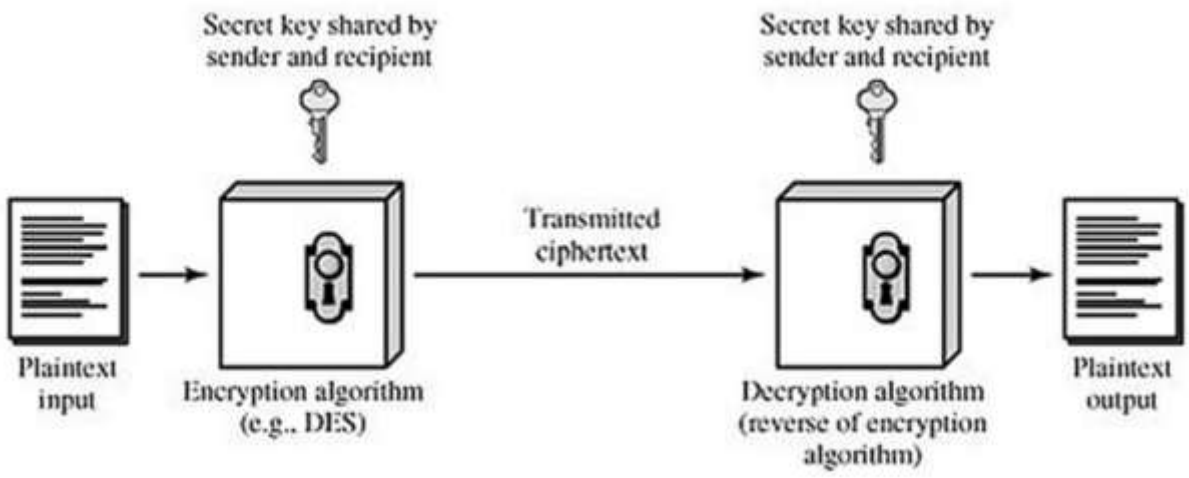
Critics have developed this standard because it has problems with non-repudiation. In the years that followed, new models were developed to explain and expand on the CIA triad. The Five Pillars of Information Assurance provide authenticity and ensure that actions cannot be denied.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214

2.2 Encryption

The third essential security measure is encryption. The two sections above talk about mistakes people make and how they watch over things. However, it's not just mistakes made by people that can cause harm to the environment. To best protect the environment from harmful actions, it's important to use the best available technology. Many different methods are used to help keep the environment safe. These methods aim to protect the three main values of the CIA triad from being damaged. One of these techniques is cryptography. Cryptography solves the issues of keeping information secret, ensuring it comes from a real source, and making sure it hasn't been changed by using methods called encryption. Encryption methods change data so that people who aren't allowed to see it can't read or use the information in the data. This means that only people who are allowed can access the information that is kept in the data (Pooja, 2018). Cryptography is the study of methods used to protect digital information, transactions, and shared computations, Jonathan (2020).

However, this is not possible for the malicious actors.



Conventional encryption (Pooja, 2018).

In figure 2.4, there's an example that shows how encryption works while data is being transmitted. Data can be found in different states: data that is not moving, data that is being transferred, and data that is currently being used (Laura, 2019). All three states must be thought about and protected carefully.

In the case of EIT, data that is moving is considered. This means that the data being sent from one place to another is kept safe with a code (Kevin, 2012). In this change, the entire process is seen as safe. So, it's only fair to say that the transition is safe as long as the data is encrypted before it leaves the computer and decrypted once it gets to the receiver's computer. This phenomenon is called end-to-end encryption. In today's digital world, protocols such as SSL, TLS, and HTTPS are used to support end-to-end encryption across a wide range of applications.

Another key area that needs to be protected is Encryption at Rest (EAR). This handles data that is stored and ensures all stored data is encrypted to protect against harmful individuals. In this way, bad people can't get information from the data (Kevin, 2011). This process is like the one shown in figure

2.4. However, in this case, the encrypted text is sent to the database. Once the sender wants to get the data back, it is decrypted.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214

Table 2: Summary of Related Literature Review

S/No	Author(s)	Title of the Work	Methodology	Result	Limitation
1	Khan et al. (2025)	*IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019*	Qualitative, non-empirical study using systematic literature review (2002–2023).	99.96% literature exclusion rate (390,995–167); 100% of identified risks concentrated on data security, privacy, confidentiality across all IoT architectural layers.	Non-empirical (no primary data collection); did not evaluate technical programming/design of IoT devices; focused only on wearable and implantable IoT devices; control implementation not empirically tested.
2	Obidallah (2025)	*A Unified Computational Model for Assessing Security Risks in Internet of Transportation Things-Based Healthcare Applications*	Hybrid Fuzzy ANP–TOPSIS model; 60 expert evaluations; 3 Level-1 factors, 9 Level-2 factors, 27 Level-3 sub-factors.	71.8% reduction in cyber-physical risk exposure through integrated control measures.	Expert-driven dataset may limit generalizability; no real-world live deployment validation; model depends on subjective fuzzy judgments; limited scalability testing across diverse IoTT infrastructures.
3	Akinbi et al. (2025)	*A Systematic Security Analysis of Medical Internet of Things (MIoT) Ecosystems in Threat Modeling Scenarios*	Systematic Literature Review (574 papers identified → 34 selected; 94.1% exclusion rate); 48 threats identified.	94.1% literature exclusion rate; 75% of MIoT threats applicable to ECG systems (36/48).	Excluded cloud/server-side and side-channel attacks; limited to three ECG devices; consumer-grade tools used; no live clinical deployment validation; firmware encryption prevented full internal analysis.
4	Sun et al. (2024)	*A Survey on Security Issues in IoT Operating Systems*	Survey of security and privacy challenges in IoT operating systems.	Identified critical need for robust data security mechanisms like lightweight encryption and access control.	Highlighted a lack of privacy data usage standards and public awareness regarding data leakage.
5	Bariro (2019/2026)	*IEEE Internet Computing (implied publication) / arXiv preprint*	Proposed Health Guard, a machine learning framework that correlates vital signs from multiple medical devices (e.g., ANN, DT, RF, KNN).	Achieved an overall accuracy of 91% and an F1 score of 90% in detecting malicious activities in an SHS.	Passive attacks like eavesdropping or information leakage via packet capture are considered out of scope. The study assumes the data collected from the SHS are not compromised.
6	Si-Ahmed et	*arXiv:2202.09657v4*	Comprehensive	Identified advantages	The literature survey may

S/No	Author(s)	Title of the Work	Methodology	Result	Limitation
	al. (2023)	*(cs.CR) (Preprint submitted to Elsevier)*	survey/review of existing literature using Machine Learning (ML) for Intrusion Detection Systems (IDS) in IoMT.	and disadvantages of various ML methods (SVM, DT, RF, NN, etc.) and highlighted the main challenges in applying ML-based IDS to IoMT systems.	have unintentionally left out non-scientific or very current unpublished works; recommendations are subjective.
7	ElSayed et al. (2024)	*SoutheastCon 2024 (Proceedings) / arXiv:2401.07368 (Preprint)*	Proposed a novel green architecture using a convolutional ML autoencoder model for network security monitoring and intrusion prediction in healthcare IoT.	Achieved an accuracy of up to 93.6% in predicting various attacks and demonstrated zero-day detection capabilities.	The system performs at 93.6% mean accuracy with an 82.1% worst-case scenario; a more extensive dataset is needed.
8	Azaliah et al. (July 2019)	*Indonesian Journal of Electrical Engineering and Computer Science*	Used Hospital Kuala Lumpur (HKL) as a case study to develop a risk model plan based on ISO/IEC 27005:2018.	Proposed an iterative IoT Security Risk Model for Healthcare addressing five layers of risk technology (authentication, encryption, secure boot, IPS/firewall, education).	Preliminary/design stage; requires feedback from IT and business personnel before implementation; limited by the HKL case study.
9	Jasour et al. (2022)	*Autonomous Robots*	Used profile justification, risk assessment model selection, security monitoring, and machine learning techniques for dynamic risk evaluation.	Achieved dynamic risk evaluation capabilities using ML for connected autonomous vehicles.	Did not account for the number of IoT devices in the risk evaluation and was validated only on a vehicle network.
10	Abbass et al. (2018)	*2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*	Comparative study of deep learning algorithms (CNNs, RNNs, RBMs, DSNs) for intelligent security risk assessment.	CNNs improved performance, classifying threats faster and learning features from unlabeled data efficiently.	Requires extensive training data and does not guarantee absolute prediction accuracy.
11	Jaidi et al. (2025)	*An Internet of Medical Things Cyber Security*	Comparative analysis of existing	Developed the IoMT-CySAM	General risk management processes are complex and

S/No	Author(s)	Title of the Work	Methodology	Result	Limitation
		Assessment Model (IoMT-CySAM)	risk management frameworks and ML solutions (DT, RF, GB) using the BoTNeT-IoT dataset.	framework; DT, RF, and GB achieved 100% anomaly detection accuracy during testing.	prone to errors; real-world deployment testing is still needed.
12	Mohammad (2023)	*Cybersecurity Approach in Internet of Healthcare Things (IoHTs)*	Review of current cybersecurity challenges in IoHTs and secure service solutions across five security layers.	Described security measures for 5G, mMTC, and Network Slicing, including access control, encryption, and IDPS.	Lack of publicly available IoHT cyberattack datasets limits further research.
13	Sfar et al. (2018)	*A Roadmap for Security Challenges in the Internet of Things*	Literature review categorizing risks into secured technology, human privacy, and trustable process/data.	Identified five major healthcare IoT risks, including privacy exposure, cyberattacks, and location privacy.	Security and privacy are often overlooked because of the emphasis on new IoT features and capabilities.
14	Khan et al. (2025)	*IoT Medical Device Risks: Data Security, Privacy, Confidentiality and Compliance*	Qualitative, non-empirical systematic literature review applying HIPAA and COBIT 2019 governance frameworks.	Developed a comprehensive risk-technology matrix identifying data-related risks across six IoT architecture layers.	Limited to non-technical analysis; did not discuss the design, development, or programming of IoT devices.
15	Waeal (2025)	*A Unified Computational Model for Assessing Security Risks in Internet of Transportation Things-Based Healthcare Applications*	Used a hybrid Fuzzy ANP–TOPSIS model and surveyed 60 experts to prioritize security risks across healthcare applications.	MediXcel EMR was identified as the most viable solution for IoTT security, while Caresoft was the least effective among seven alternatives.	Limited by a small expert-driven dataset, affecting generalizability to broader real-world scenarios.
16	Grispos et al. (2024)	*A Digital Forensic Analysis of an Electrocardiogram Medical Device: A First Look*	Conducted a digital forensic analysis of a physical ECG device after an incident to recover forensic evidence.	Identified a methodology for recovering forensic artifacts from ECG devices.	Did not identify actual security vulnerabilities or conduct pre-incident security analysis or penetration testing.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214

III. METHODOLOGY

This chapter explains the approach that will be used to create a cloud-based framework for assessing security risks in healthcare systems that use the Internet of Things. It describes the plan for the research, how the system is built, the ways data will be collected, the model for assessing risks, the tools that will be used for development, and the methods for evaluating the results. The method will focus on finding security risks in IoT healthcare devices and creating a cloud-based system that can check for these risks and help reduce them.

3.1 Research Design

The study will use a design science research approach along with system development methods. The design science approach works well because the research is about making a tool (a security risk assessment framework) to address a real-world issue. The methodology will involves the following phases:

1. Understanding and looking into the security risks and dangers that exist in internet of things (IoT) systems used in healthcare.
2. Requirement analysis for the security framework
3. Design of the cloud-based risk assessment framework
4. Development and implementation of the framework
5. Testing and evaluation of the framework

This method makes sure the framework properly handles the security issues in IoT healthcare settings.

Study Environment

The study will look at healthcare systems that use the Internet of Things, where medical tools like wearable sensors, smart monitors, and devices that track patients from a distance send information through networks and save data on cloud-based platforms. Typical components of the environment will include:

i. IoT medical devices include wearable sensors and smart monitoring devices.
ii. Healthcare network infrastructure
iii. Cloud storage and computing platform
iv. Security risk assessment module

The cloud environment is used because it allows things to grow as needed, makes it easier to watch over everything from one place, and helps find security issues quickly.

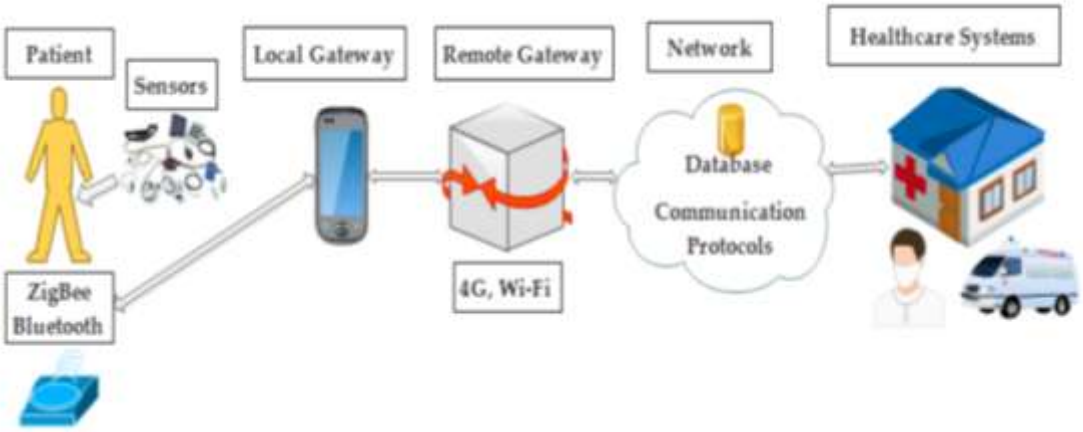
3.2 Data Collection Methods

The data needed for this study will be gathered through a review of existing literature. Information about IoT security threats, cloud security frameworks, and how to protect healthcare data will be collected from sources like academic journals, conference papers, cyber security reports, and healthcare IT security standards.

3.3 Existing system

Many studies say that the IoT has three main layers: the perception layer, the network layer, and the application layer. The flow of data through these layers. Each layer has some security issues such as keeping information secret, making sure it stays unchanged, and proving it is real, because people are involved. Because people are involved, the system becomes more sensitive. That's why the data collected from individuals and patients' needs the system's permission to access their records. This privacy issue stops users from fully benefiting from the system. Protecting healthcare data is very important. To make sure the data is real, accurate, and private, we need to create a security system for the real-time health monitoring system. Many security tools and systems are already being used by health technicians and paramedics. These systems, however, become absurd over time. Moreover, our earlier work in this area also backs up what we are saying.

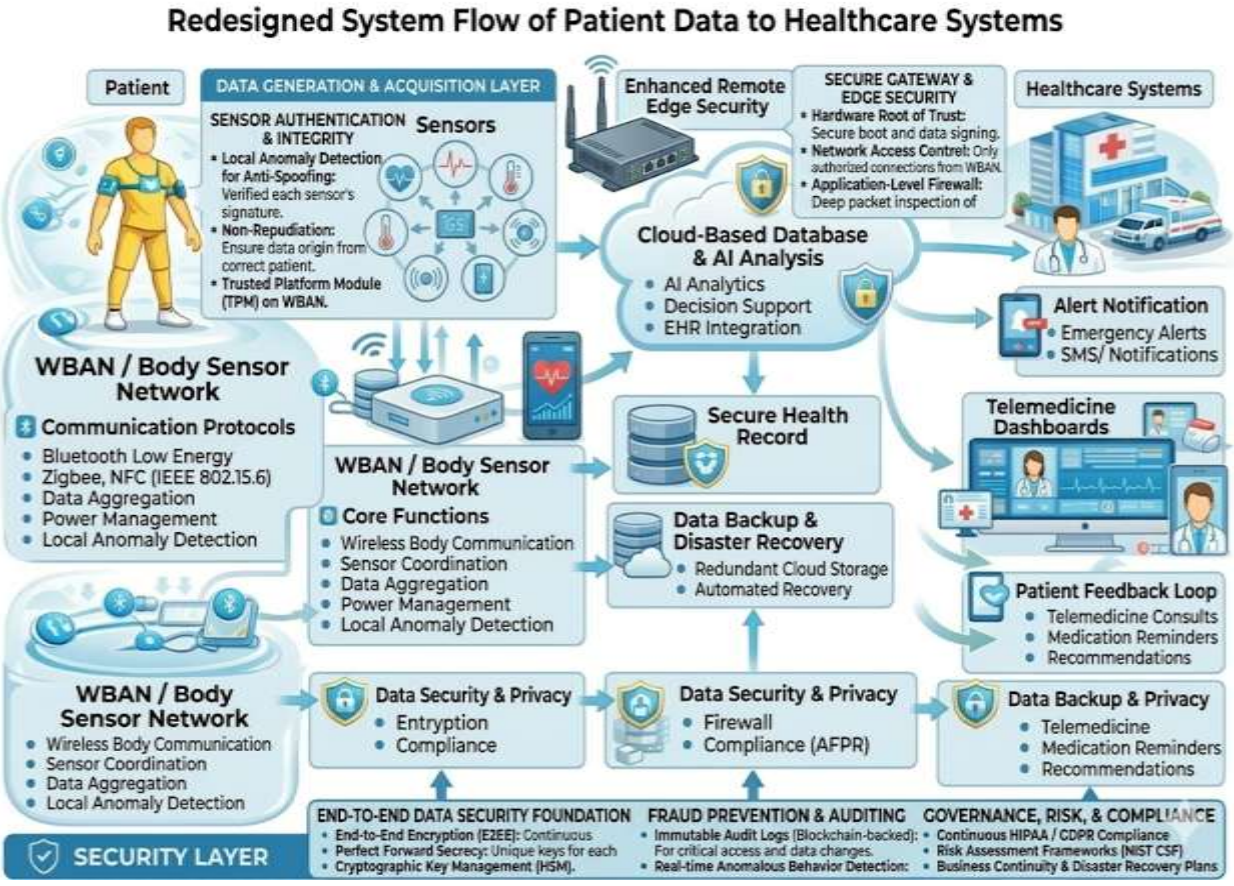
© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214



The current system shows how data flows from the patient to the healthcare systems (Yueyang, 2025).

As mentioned before, IoT operates in layers, and each layer has security issues that need to be fixed to address major security problems. The first layer is called the physical layer, and it's also known as the perception layer. Information about the environment, like temperature, humidity, and where something is, is picked up by sensors. These sensors send the data to a network layer.

3.4 Proposed Model



Shows the overview of the proposed model

The Data Generation & Acquisition Layer acts as the main connection between the patient's biological information and the digital systems used in healthcare. At this outer edge, the architecture uses a complex set of Wireless Body Area Network (WBAN) sensors, which are grouped according to how they interact with the body. These include devices you wear on your body without needing surgery, like PPG sensors that measure heart rate and oxygen levels in the blood, and devices that are placed inside the body, such as continuous glucose monitors or subcutaneous cardiac loop recorders. The main problem with this layer is called "Transduction Fidelity," which means the ability to turn analog signals from biology or electrical activity into clear digital data without losing important medical information. To do this, the system uses high-bit-depth Analog-to-Digital Converters (ADCs) that sample at frequencies matching the needs of each vital sign being tracked.

From a project implementation point of view, these sensors do more than just collect data—they are smart devices that can process information and clean up unwanted noise before sending it on. In a real-world setting, the body's signals can be mixed up or messed with by "artifacts" that happen because of the patient moving, their muscles tightening, or outside electrical noise from the environment. The sensors in this new design use digital signal processing units that apply band-pass filters and wavelet transforms right at the source. This makes sure that only good-quality data moves ahead, which helps reduce the work needed by the later AI analysis steps. These sensors are made to work according to strict rules for managing power. Since many of these devices run on batteries, the acquisition layer uses a "Trigger-Based" sampling method. This means the sensor stays in a low-power sleep mode until it detects a change in the body's signals, which helps the device last much longer—sometimes from days to months.

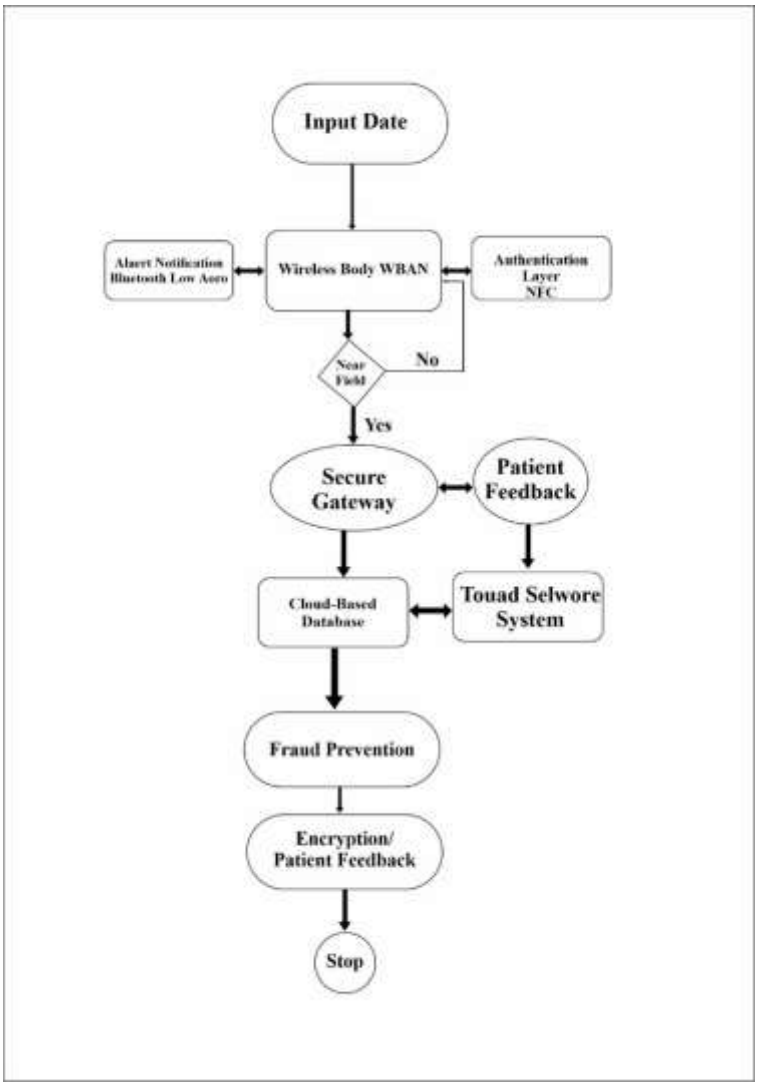
Putting these sensors together in one WBAN helps sync data from different sources. In clinical diagnostics, a single piece of data, like a sudden increase in heart rate, is usually unclear on its own. When the system works with information about oxygen levels in the blood and movement data from a device that measures motion in three directions, it can tell the difference between a person who is exercising and someone who is having a problem with their heart. This synchronization is handled through a local hub, usually a special wearable device or a smartphone, which serves as the "Orchestrator" for the body-worn network. This hub makes sure every data packet has a very precise time mark, down to a millionth of a second, so the Cloud-Based Database can create an exact timeline of the patient's health condition. This careful way of creating data sets the foundation, or "Source of Truth," that all medical decisions are based on.

The Foundation Layer includes a strict Identity and Access Control (IAM) system. In a setting where many people like patients, nurses, doctors, and insurance companies use the system, it's important to follow the "Principle of Least Privilege." This means each person should only have the access they need to do their job, nothing more. The model uses Multi-Factor Authentication (MFA) for all healthcare provider logins, which means users have to provide both a password and either a biometric scan or a hardware token to log in. For the patient, IAM is managed through the Hardware Root of Trust in their gateway device, making sure that the "Identity" of the data source is just as secure as the identity of the human clinician looking at it.

To make security even better, the system uses Attribute-Based Access Control (ABAC), which takes into account the "Context" of the access request. For example, a doctor might have full access to a patient's records while working at the hospital during their shift, but their access could be limited if they log in from a public Wi-Fi network or a place that isn't recognized. This "context-aware" security is important for stopping unauthorized data leaks. By including IAM as part of the End-to-End Data Security Foundation, the model makes sure that the human part, which is usually the weakest point in security, is better protected with technical measures. This last part of the Foundation Layer connects the cryptographic, auditing, and regulatory parts into one strong shield that lets medical data move safely and with proper clinical standards.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720214

3.5 System Flowchart



Shows the System Flowchart

IV. CONCLUSION

Healthcare organizations have to deal with two main problems: protecting very private patient information and making sure that healthcare services keep running without any stoppages. The growing number of IoT devices, which have different amounts of computing power and security protections, has made traditional security methods not enough anymore. Many devices don't have enough power to use strong encryption or detect threats as they happen, which makes them easy targets for attacks like man-in-the-middle, malware being added, and unwanted access. Even though more people are becoming aware of these issues, healthcare organizations still find it hard to deal with the absence of a complete and flexible security risk assessment system that covers both IoT devices and cloud-based systems. Current solutions are usually broken up, slow to respond, or only cover a small part of the problem. They tend to focus on certain types of threats rather than looking at all possible weaknesses, dangers, and the bigger effects they could have. The frame work to be develop will help the Healthcare System to secure a patients information and other data. The design science approach works well because the research is about

making a tool (a security risk assessment framework) to address a real-world issue. In the future, more research should focus on creating better cloud-based security risk assessments using other methods to develop a framework for IoT-based healthcare systems.

REFERENCES

[1] Abbass, A., et al. (2018). Intelligent security risk assessment using deep learning algorithms in IoT. Proceedings of the 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM).

[2] Akinbi, A., et al. (2025). A systematic security analysis of medical internet of things (MIoT) ecosystems in threat modeling scenarios. Frontiers in the Internet of Things.

[3] Al-Qaseemi, S. A., et al. (2018). Security challenges in IoT-based monitoring systems.

[4] Ali, M. (2020). DTLS and Clasp authentication methods for IoT systems.

[5] Almahdi, M. (2019). Patient data safety and awareness against cyber-attacks in IoT environments.

[6] Alqahtani, H., et al. (2020). Security risk management in cloud-connected IoT healthcare systems.

[7] Alrawashdeh, M., et al. (2023). Access control and communication security in healthcare IoT.

[8] AmandaNCraig. (2015). Active cybersecurity programs and threat intelligence sharing.

[9] Azaliah, et al. (2019). An iterative IoT security risk model for healthcare. Indonesian Journal of Electrical Engineering and Computer Science.

[10] Bariro. (2019/2026). Health Guard: A machine learning framework for detecting malicious activities in smart healthcare systems. IEEE Internet Computing / arXiv preprint.

[11] Bokhari, M. U., et al. (2022). Cloud-based security risk assessment and compliance in healthcare IoT.

[12] Borka. (2022). Changing paradigms in digital technology and cybersecurity.

[13] Buccafurri, A. (2012). DTH-P2P social networks and cryptographic protocols for secure systems.

[14] Choi, J., et al. (2018). Sensor-based attacks and security classification methods in mHealth.

[15] Deepak, S. (2018). The CIA triad of data security.

[16] Draz, U. (2018). Cyber threats and real-time data security in technology.

[17] ElSayed, et al. (2024). Network security monitoring and intrusion prediction in healthcare IoT using a convolutional ML autoencoder model. Proceedings of IEEE SoutheastCon 2024 / arXiv preprint.

[18] Eric, P. (2013). Reactive computer system security and incident response history.

[19] Farooq, M. U., et al. (2018). The VICINITY framework for semantic interoperability, privacy, and security in IoT.

[20] Fortino, G. (2018). CoTAG: Cloud-of-Things virtualization and device reliability grouping.

[21] Grispos, et al. (2024). A digital forensic analysis of an electrocardiogram medical device: A first look.

[22] Hamrioui, S. (2017). Policy management rules for secure cloud servers in continuous patient tracking.

[23] Hathaliya, J. J., & Tanwar, S. (2020). Trust management and secure agent technology in IoT e-health.

[24] Hatzivasilis, G. (2019). Certificate-based DTLS handshake mechanisms for resource-constrained e-health gateways.

[25] Huang, X. (2017). Key agreement and cryptographic setup in wireless sensor networks for IoT.

[26] IBM. (2022). What is cybersecurity? IBM.

[27] Ifigeneia. (2021). ENISA threat landscape report: Top 15 cyber threats.

[28] ISO/IEC. (2020). Information technology — Security techniques — Risk management. ISO/IEC 27005 standard.

[29] Jaidi, et al. (2025). An Internet of Medical Things Cyber Security Assessment Model (IoMT-CySAM). Cureus.

[30] Jalkanen, A. (2019). Human factors and the weakest link concept in information security.

[31] Janine, S. (2018). History of early security problems in multi-user computer systems (1970s–1977).

[32] Jasour, et al. (2022). Dynamic risk evaluation using machine learning techniques. Autonomous Robots.

[33] Jonathan, K. (2020). Fundamentals of digital cryptography and secure computations.

[34] Kevin, M. (2011). Encryption at rest (EAR) strategies for database security.

[35] Kevin, M. (2012). Encryption in transit and end-to-end security protocols.

[36] Khan, et al. (2025). IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019. South African Journal of Business Management.

[37] Kim, L. (2018). Information system security standards and the CIA triad benchmark.

[38] Laura, P. (2019). Data states: Data at rest, data in transit, and data in use.

[39] Li, X., et al. (2011). HTTP-CoAP security model and payload encryption for two-dimensional IoT structures.

[40] Logambal, R. (2017). Three-level wireless body area networks (WBAN) for real-time healthcare monitoring.

[41] Masood, A., et al. (2018). Integrating wireless body area networks with sensor cloud infrastructures.

[42] Mekky, A., et al. (2023). Vulnerability factors, interoperability issues, and attack propagation in medical IoT devices.

[43] Mohammad. (2023). Cybersecurity approach in Internet of Healthcare Things (IoHTs).

[44] Mohammed, B., et al. (2019). Mobicare: Mobile healthcare tracking and body sensor security.

[45] Mohapatra, S., et al. (2018). Security routing protocols and data fusion in IoT network layers.

[46] Nanayakkara, C., et al. (2019). Three-layered IoT health framework under Contiki real-time operating system.

[47] Obidallah, W. J. (2025). A unified computational model for assessing security risks in internet of transportation things-based healthcare applications. Electronics, 14(24), 4894.

[48] Pooja, R. (2018). Conventional encryption techniques and data protection.

[49] Rahmani, A. M., et al. (2015). Biometric safety measures and vulnerability to Denial of Service in IoT perception layers.

[50] Rashid, M., et al. (2023). Managing active security risks and medical IoT device weaknesses.

[51] Rossouw, V. (2013). Definitions and conceptual frameworks in cybersecurity.

[52] ScienceIJSAR. (2022). Risk assessment frameworks for cloud and IoT integration.

[53] Selvaraj, K. (2019). Secret sharing schemes and privacy preservation in patient data blocks.

[54] Sfar, et al. (2018). A roadmap for security challenges in the Internet of Things.

[55] Shah, S. A., et al. (2019). Data authenticity, accuracy, and privacy in real-time health monitoring and telemedicine.

[56] Sultan, A., et al. (2021). Threat identification and continuous risk evaluation in cloud-based IoT healthcare.

[57] Sun, Y. (2019). Identity linking and group secret management in e-health applications.

[58] Sun, et al. (2024). A survey on security issues in IoT operating systems.

[59] Tewari, A. (2016). Evaluation of lightweight DTLS protocols for low-power IoT hardware platforms.

[60] Waeal. (2025). A unified computational model for assessing security risks in internet of transportation things-based healthcare applications.

[61] Yan, Z., et al. (2014). Reliable data communication and situation-aware trust management in IoT.

[62] Yang, K. (2017). Addressing security vulnerabilities in evolving IoT ecosystems.

[63] Yasin, A., et al. (2018). A three-layer network security analysis and access control in IoT.

[64] Yueyang, Z. (2025). Data flow security architecture from patient sensors to healthcare systems.

[65] Zhang, Y., et al. (2023). Privacy concerns and data transmission security in healthcare Internet of Things.